On-road enforcement for automated vehicles

July 2022

Discussion paper

National Transport Commission

Report outline

Title	On-road enforcement for automated vehicles
Type of report	Discussion paper
Purpose	For public consultation
Abstract	This discussion paper examines whether state and territory law enforcement officers have sufficient powers to interact with and respond to the road safety risks of automated vehicles. It also considers practical aspects of interacting with automated vehicles and proposes options to address any identified gaps. The findings and recommendations from this work will support development of nationally consistent approaches to on-road enforcement that will assist states and territories to implement regulatory and policy changes as well as changes to procedures, training needs and system requirements.
Submission details	The NTC will accept submissions until 5 September, 2022 online at **www.ntc.gov.au** or by mail to: National Transport Commission Public submission – On-road enforcement for automated vehicles Level 3, 600 Bourke Street Melbourne VIC 3000
Attribution	This work should be attributed as follows, Source: National Transport Commission 2022, *On-road enforcement for automated vehicles: discussion paper*, NTC, Melbourne. If you have adapted, modified or transformed this work in anyway, please use the following, Source: based on National Transport Commission 2022, *On-road enforcement for automated vehicles: discussion paper*, NTC, Melbourne.
Key words	automated vehicle, automated driving system, automated driving system entity, in-service, first supply, general safety duty, in-service regulator, law enforcement
Contact	National Transport Commission Level 3/600 Bourke Street Melbourne VIC 3000 Ph: (03) 9236 5000 Email: **enquiries@ntc.gov.au** **www.ntc.gov.au**

Have your say

What to submit

The NTC is seeking your views on the consultation questions in this discussion paper and any other relevant views you have on the on-road enforcement of automated vehicles. The NTC would like to hear in particular from Commonwealth and state and territory road transport and enforcement agencies, regulators and the automated technology providers and transport industry bodies in Australia.

When to submit

We are seeking submissions on this discussion paper by Monday 5 September 2022.

How to submit

Any individual or organisation can make a submission to the NTC.

Making a submission

- Visit **www.ntc.gov.au** and select 'Have your say' on the homepage.
- Send a hard copy to:

  National Transport Commission
  Public submission – On-road enforcement for automated vehicles
  Level 3, 600 Bourke Street
  Melbourne VIC 3000

Where possible, you should provide evidence, such as data and documents, to support the views in your submission.

Publishing your submission

Unless you clearly ask us not to, we publish all the submissions we receive online. We will not publish submissions that contain defamatory or offensive content.

The *Freedom of Information Act 1982* (Cwlth) applies to the NTC.

Contents

Executive summary

The operation of automated vehicles on Australian roads will create unique challenges for enforcement. This discussion paper details these challenges and proposes options to address them. It focuses on how law enforcement will interact with automated vehicles on the road. It does not cover broader enforcement issues such as criminal investigations.

The National Transport Commission (NTC) consulted with industry and government stakeholders to develop the information in this paper. We conducted topic-based workshops as well as targeted sessions.

We will use the findings from this work to develop policy positions that are nationally consistent and outcomes based. This will help states and territories when they put in place regulatory and policy changes. It will also help them with changes to procedures, training needs and system requirements.

Context

This paper is part of the on-road enforcement for automated vehicles project. The goal of the project is to develop a nationally consistent approach that allows state and territory law enforcement officers to:

- interact with automated vehicles
- respond to the road safety risks of automated vehicles.

The on-road enforcement work is part of a broader reform program. Its aim is to create end-to-end regulation to support the safe commercial deployment and operation of automated vehicles at all levels of automation. The NTC is collaborating with Austroads and the Commonwealth, state and territory governments on the reform program. We are seeking consensus on policy positions and final outputs so we can achieve national consistency.

States and territories want to be prepared for enforcing automated vehicles when they begin operating on our roads. At the same time, there is uncertainty over the future capability of automated vehicle technology. The ongoing tension between these two themes states is a common theme running through this paper. In response, most of the proposed options in the paper do not seek to define prescriptive solutions. Instead, they focus on making sure enabling powers and provisions are available.

This approach aims to balance the following considerations:

- reform principles of legal certainty
- flexibility to accommodate future developments in technology
- advice from law enforcement about their operational requirements.

This discussion paper examines the powers of state and territory law enforcement officers. It aims to encourage discussion about whether current powers are sufficient for officers to interact with and respond to the road safety risks of automated vehicles. The paper explores practical aspects of interacting with automated vehicles. Where there are gaps, the paper considers options to address them. The focus is on how industry is considering these issues, and how existing or proposed mechanisms may be used to address them.

The key areas covered are:

- Powers and practices of state and territory law enforcement officers. These include powers to interact with, intercept or disable, and to ensure the safe on-road operation of automated vehicles.
- Access to data (powers and privacy protections) by state and territory law enforcement agencies. This includes data to identify automated vehicles and respond to their road safety risks (for example, data on factors causing or contributing to a breach of a road traffic law or crash).
- Enforcement agencies sharing data with relevant parties, particularly the in-service safety regulator.

The NTC is a national land transport reform body with a mandate focused on transport laws. For this reason, any matters relating to the powers and practices of police officers beyond road safety, such as criminal investigations, are not covered in this paper.

We acknowledge the potential operational impacts of automated vehicles on law enforcement. This paper does not attempt to comprehensively assess these impacts. It is only intended to support states and territories in considering potential operational impacts within their jurisdiction.

Providing on-road directions to automated vehicles

Consideration is given to how enforcement officers can provide directions to automated vehicles at the roadside. We propose to include the automated driving system (ADS) as a system to which enforcement officers can provide an on-road direction.

Two options to assist automated driving system entities (ADSEs) to develop the capacity of their ADS to interact with enforcement officers and act on directions are proposed.

Disabling an automated driving system

Considers how enforcement officers could disable an ADS at the roadside and remotely, and relevant processes once an ADS is disabled. Proposes that there may be multiple scenarios where police may need additional powers to disable a vehicle as well as remove an automated vehicle from the road once its ADS has been disabled.

Data needs and overview of enforcement access to automated vehicle data

Recognises that enforcement officers will need to access data to respond to automated vehicle road safety risks. This includes timely access to data for crash investigation and reporting, and in relation to road rule infringements.

Considers relevant data needs and provides and overview of some of the issues around enforcement access to automated vehicle data.

Access to data at the roadside and more broadly

Considers issues relating to the availability and accessibility of ADS operational data at the roadside and more broadly. The paper outlines the range of existing mechanisms, such as the first supply requirements, for ongoing data recording and sharing capability that are relevant for law enforcement access to vehicle data.

Proposes that states and territories include new data collection/access powers that would allow enforcement officers to collect or access ADS data at the roadside.

Additional data availability and access considerations

Outlines additional issues around enforcement access to automated vehicle data, such as visual indicators, in-vehicle cameras and information from vehicle occupants, as well as retention and admissibility of automated vehicle data.

Interactions with the in-service regulator, ADSEs and registered owners

Sets out the interactions between law enforcement and the in-service regulator, automated driving system entities (ADSEs) and automated vehicles registered owners. Considers whether states and territories need new powers to allow enforcement officers to disclose relevant data and information to the in-service regulators and ADSEs.

Operational impacts on enforcement roles, responsibilities and resources

In the final chapters we consider the operational impacts of automated vehicles on enforcement roles, responsibilities and resources.

We conclude that it is difficult to quantify the scope of the impact until more is known about automated vehicles and how they will operate in the Australian environment. States and territories need to consider the potential operational impacts within their jurisdictions to allow for adequate training and investment in infrastructure.

A case study of a camera-detected rule breach is used to illustrate the modified role of enforcement officers in dealing with automated vehicles.

Next steps

We are seeking views on the options discussed in this paper. We want our work to support states and territories as they implement regulatory, policy, procedure and system changes. Ideally, the advice we receive will be framed around practical considerations to help us achieve this.

We welcome written submissions, as well as feedback through to 5 September, 2022. During the consultation period we will also consult with stakeholders through meetings. We will use the findings from our work to develop a policy paper and updated guidelines. We will then submit these to Commonwealth, state and territory infrastructure and transport ministers for approval.

Questions

The NTC will consult on the following questions until 5 September, 2022.

1 About this project

Key points

- The purpose of this project is to develop a nationally consistent approach that allows state and territory law enforcement officers to interact with automated vehicles and respond to their road safety risks.
- While the focus of this project is on enforcement powers, some practical issues are also explored.
- The issues and options in this paper were developed by the National Transport Commission (NTC) and our stakeholders.
- The NTC will continue to consult with government stakeholders, industry, other regulators and the wider public about the issues raised in this discussion paper.
- We will analyse feedback to this paper to develop a final policy paper and recommendations.

1.1 Project objectives

1.1.1 Purpose

The purpose of this project is to develop a nationally consistent approach that allows state and territory law enforcement officers[1] to:

- interact with automated vehicles
- respond to the road safety risks of automated vehicles.

1.1.2 Problem statement

As with conventional vehicles on the road, law enforcement officers will continue to play an integral role in addressing road safety issues of automated vehicles. Officers will need to monitor automated vehicles' compliance with road traffic laws and their safe interaction with other road users. They will need to interact with automated vehicles on the road, at the roadside and after a crash, and intervene, in real time, in cases of road traffic law breaches.

The on-road operation of automated vehicles will create unique challenges for enforcement. These include:

- safely intervening and interacting with automated vehicles on the road when required
- identifying an automated vehicle's level of automation and whether it is under automated driving system (ADS) or driver control
- communicating with automated vehicles
- applying road rules to automated vehicles

[1] 'State and territory law enforcement officers' for road safety purposes include police officers, relevant officers of state and territory road transport agencies and authorised officers under the Heavy Vehicle National Law. We generally refer to 'state and territory law enforcement officers' as 'enforcement officers' throughout this discussion paper.

- accessing data for crash investigation and reporting, including at the roadside where possible.[2]

Current powers and practices of state and territory law enforcement officers are insufficient or ineffective to allow officers to interact with and respond to the road safety risks of automated vehicles in all scenarios.

1.1.3 Project objectives

The objectives of this project are to:

- Examine whether powers currently available to state and territory law enforcement officers (including authorised officers under the Heavy Vehicle National Law) are suitable for ensuring the safe operation of automated vehicles on the road and identify gaps.
- Establish what data law enforcement officers need to respond to the road safety risks posed by automated vehicles.
- Develop a nationally consistent approach for law enforcement officers to ensure the safe operation of automated vehicles on the road, including legal powers to:
  - interact with automated vehicles
  - access data to respond to automated vehicle road safety risks
  - share data with relevant parties, particularly the in-service regulator, as part of interacting with other parties.
- Identify further legislative or operational changes required by states and territories.

1.1.4 Project mandate

This project derived from recommendations agreed at the Infrastructure and Transport Ministers Meeting in May 2021 that:

> *The NTC work with state and territory governments to develop enforcement practices for automated vehicles and establish data requirements and data access protocols for enforcement officers, and report back to ministers in November 2022.*[3]

[2] The NTC previously identified key areas that would need to be addressed so enforcement officers can undertake their safety and enforcement roles when automated vehicles start operating on our roads (National Transport Commission, 2021, pp. 104-105).

[3] There was also agreement that states and territories will undertake a review of existing powers by an agreed date.

1.2 Key terms

The following concepts are central to the end-to-end framework described in this paper:

Automated driving system (ADS): the hardware and software collectively capable of performing the entire dynamic driving task (defined below) on a sustained basis without human input.

Automated driving system – dedicated vehicle (ADS-DV): a vehicle designed to operate exclusively by a level 4 or 5 ADS within the given operational design domain limitations of the ADS.

Automated driving system entity (ADSE): the party that will self-certify the safety of the ADS and take responsibility for it over its life. The ADSE will self-nominate at first supply when applying for type approval or when applying to take responsibility for an ADS in service.

Automated vehicle: a vehicle that has an ADS. It is distinct from a vehicle with advanced driver-assistance systems such as lane-keep assist.

Automated Vehicle Safety Law (AVSL): a new national law agreed by ministers to regulate the in-service safety of automated vehicles. The AVSL will regulate ADSEs, their executive officers and remote drivers, and operate in conjunction with existing road transport laws. It will also establish an in-service regulator for automated vehicles.

Control: ministers have agreed that when an automated vehicle's ADS is engaged, the ADS is in control and the ADSE is responsible for complying with dynamic driving task obligations.

Dynamic driving task (DDT): all the operational and tactical functions required to operate a vehicle in on-road traffic. This includes steering, acceleration and deceleration, object and event detection and response, manoeuvre planning and enhancing visibility through lighting, signalling and so on. The DDT excludes strategic functions such as trip planning.

Enforcement officers: officers of the law that perform investigations, confiscations or other law enforcement functions.

Fallback-ready user: a human in a level 3 vehicle who can operate the vehicle, and who is receptive to requests from the ADS to intervene and to respond to emergency vehicles. The fallback-ready user is expected to respond by taking control of the vehicle.

First supply: the point at which vehicles enter the Australian market for the first time. Ministers have agreed a safety assurance approach for the first supply of automated vehicles consisting of ADSEs self-certifying the safety of their ADS against safety criteria and obligations under the existing type-approval process.

First-supply regulator: the Commonwealth Department of Infrastructure, Transport, Regional Development and Communication administers the regulation of road vehicles up to the point of first supply in Australia. The enabling legislation for this framework is the *Road Vehicle Standards Act 2018* (Cwlth).

General safety duty: an overarching and positive obligation on the ADSE to ensure the safe operation of its ADS so far as is reasonably practicable. This type of duty is used in other transport sectors in Australia including heavy vehicles, commercial passenger vehicles, rail and domestic commercial marine vessels. What is 'reasonably practicable' will vary over time as technologies and practices evolve.

In service: when vehicles have entered the Australian market and can be operated on the road. Ministers have agreed the key elements of the in-service framework for automated vehicles – a new national in-service safety law for automated vehicles (the AVSL), a new in-service regulator, a general safety duty on ADSEs and due diligence obligations on ADSE executive officers.

In-service regulator: the new regulator for the in-service safety of automated vehicles. The regulator will be established once the AVSL is passed. The regulator is expected to begin operations by the end of 2026. The office of the regulator is expected to be small to begin, scaling up as the automated vehicle market grows.

Levels 3, 4 and 5 vehicles: vehicle automation levels, as defined by Society of Automotive Engineers International. Automated vehicles have level 3 or above automation (while advanced driver assistance systems vehicles have levels 1 or 2 automation). Levels 3 to 5 are defined as:

- **Level 3 vehicles:** the ADS undertakes the entire DDT within its operational design domain. When the ADS is driving, the human operator does not have to monitor the driving environment or the driving task but must respond to ADS requests to intervene.
- **Level 4 vehicles:** the ADS undertakes the entire DDT within its operational design domain. When the ADS is driving, the human operator is not required to monitor the driving environment or the driving task, nor are they required to intervene because the ADS can bring the vehicle to a safe stop unassisted.
- **Level 5 vehicles:** the ADS undertakes all aspects of the DDT and monitoring of the driving environment. The ADS can operate on all roads at all times. No human operator is required.

Operational design domain: the specific conditions under which an ADS or feature is designed to function (for example, location, weather conditions, driving modes).

1.3 Background

1.3.1 This project is part of the national reform program for automated vehicles

Australia's laws do not currently support the deployment of automated vehicles. Our laws are designed for vehicles with human drivers. A review in 2016 found more than 700 barriers to deploying automated vehicles in state, territory and Commonwealth laws.

Automated vehicles are expected to deliver safety, productivity, mobility and environmental benefits. Without reforms, Australians will not be able to gain these benefits. In 2016, infrastructure and transport ministers agreed to developing an end-to-end regulatory framework for the commercial deployment of automated vehicles. Since then, the NTC has been working with government and industry to develop this framework. This work has led to ministers' decisions on:

- regulated parties
- determining control of an automated vehicle
- safety assurance for automated vehicles at first supply
- a new national AVSL and new regulator for the in-service safety of automated vehicles (the in-service regulator)
- the approach to motor accident injury insurance for automated vehicles
- regulating government access to automated vehicle data.

Elements of the regulatory framework for automated vehicles in Australia agreed by ministers that are particularly relevant to this on-road enforcement work are that:

- The ADSE will be responsible for the driving task when the ADS is engaged.
- There will be a new regulated party (the fallback-ready user) under state and territory legislation who would have obligations to remain attentive to certain factors (for example, transition of control demands) and be fit to drive.
- The ADSE must self-certify to show how its ADS meets 11 safety criteria and three corporate obligations before supplying its ADS to the market. The safety criteria are being incorporated into the existing framework for the first supply of vehicles under the Road Vehicle Standards Act.
- In service, the ADSE will be subject to a general safety duty and prescriptive duties and requirements (including to develop and maintain a law enforcement interaction protocol).
- The in-service regulator will have compliance and enforcement powers including information access, collection and sharing powers.

Some of these elements are discussed in more detail, along with more specific relevant elements of the regulatory framework, in the chapters that follow.

1.3.2 Relevant Australian developments

Current draft Australian Design Rule 90/01

The Department of Infrastructure, Transport, Regional Development and Communications is incorporating the first supply safety criteria into the Australian Design Rules (ADRs) (National Transport Commission, 2022, pp. 18, 22-23). Specifically, Appendix B of ADR 90/01 outlines ADS design requirements at first supply. ADR 90/01 is currently in draft form.[4]

Law enforcement interaction protocol

In February 2022, infrastructure and transport ministers agreed recommendations relating to the in-service framework for automated vehicles. They included recommendations that:

- the AVSL will provide that the ADSE must develop and maintain a law enforcement interaction protocol to be shared with the in-service regulator
- the in-service regulator should, once it is set up, publish guidance on the areas to be covered in Law Enforcement Interaction Protocols (LEIPs), in conjunction with state and territory enforcement agencies (National Transport Commission, 2022, pp. 77, 79).

The in-service regulator would forward interaction protocols received from ADSEs to road transport and enforcement agencies.

[4] Draft ADR90/01 can be found online at: **https://www.infrastructure.gov.au/sites/default/files/migrated/vehicles/design/files/adr-90-01-consultation-draft.pdf**

These interaction protocols will provide clarity to enforcement and emergency services on how to interact safely with a particular automated vehicle type. In conjunction with state and territory enforcement agencies, the in-service regulator will develop guidance on the areas to be covered in interaction protocols.[5]

The interaction protocols could cover:

- how officers can intercept and safely stop an automated vehicle
- how officers can access ADS data at the roadside or during investigation
- how officers can disable an ADS (for example, after a crash)
- how the automated vehicle will recognise enforcement and emergency services on the road or at the roadside
- how first responders can safely interact with an automated vehicle at a crash scene.

Design principles for managing government access to automated vehicle data

In August 2019, the then Transport and Infrastructure Council noted:

> *… design principles for managing government access to, and addressing new privacy challenges of,* [cooperative intelligent transport systems] *and automated vehicle data, which will guide further work by the NTC and Austroads (National Transport Commission, 2019, p. 56)*.

The design principles are provided in the Appendix . Because this project considers legal powers to access automated vehicle data by government agencies, the design principles are a relevant consideration. This is because any legal powers to access data may require additional privacy protections.

Data requirements for automated and electric vehicle registration

Austroads is looking at data requirements for automated and electric vehicle registration. In a previous phase of this work, Austroads noted that to:

> *… support the registration of automated and electric vehicles, changes may be required to jurisdictional registration systems. Specifically, additional data may be required that is unique to both automated and electric vehicles* (Austroads, 2020).

The project recommended 'a small additional data set for automated vehicles and electric vehicles and draft data definitions for further development' (Austroads, 2020).

Austroads has a current project that is further progressing this work, *FDI6338 Addition of electric, hybrid and automated vehicle attributes in the National Exchange of Vehicle and Driver Information System (NEVDIS)*. This project is defining the requirements for the next NEVDIS[6] implementation project, a technical project to add the new data attributes to NEVDIS and to support the jurisdictional registration process for automated vehicles and electric vehicles.

---

[5] A recent NTC policy paper describes how an ADSEs first-supply requirements will likely flow through to the in-service law enforcement interaction protocol requirements. See: National Transport Commission, *The regulatory framework for automated vehicles in Australia*, February 2022, pp 45–46.

[6] NEVDIS is the 'National Exchange of Vehicle and Driver Information System'.

1.3.3 Relevant international developments

Development of the Data Storage System for Automated Driving

The Data Storage System for Automated Driving (DSSAD) records and stores vehicle data for significant interactions between the driver and the ADS to identify who or what was controlling the vehicle at a given time or whether the driver was requested to take over the control of the vehicle.

Working Party 29 (WP.29)[7] (including the subgroup on DSSAD) is developing international requirements for the DSSAD for an ADS. Requirements for a DSSAD are already included as part of UN Regulation No. 157, which relates to automated lane-keeping systems.[8] The regulation covers matters such as:

- requiring that a DSSAD be fitted
- when the DSSAD must record data and the data elements it must record
- the availability and accessibility of DSSAD data
- retrieving data after a crash.

The DSSAD requirements for automated lane-keeping systems provide some insights into how the DSSAD for ADSs more broadly may be developed.

The DSSAD is discussed in more detail in chapter 6.

Automated Vehicle Safety Consortium

The Automated Vehicle Safety Consortium is an invitation-only consortium made up of industry participants (potential ADSEs). It develops best practice recommendations with the intent that these would inform industry-wide standards for safely deploying ADSs. In the past, the Society of Automotive Engineers[9] standards have been developed or amended based on the Automated Vehicle Safety Consortium's recommendations. Companies within the consortium would follow the recommendations when developing their automated vehicles. Companies outside the consortium have indicated some support for also adopting the recommendations.

The consortium has developed best practice recommendations for first responder interactions with fleet-managed dedicated automated vehicles (ADS-DVs). These recommend:

> *… a common approach for describing the interactions and associated protocols for incorporating vital information regarding first responder interactions with Society of Automotive Engineers level 4 and level 5 fleet operated vehicles into on-going development and deployment plans* (Automated Vehicle Safety Consortium, 2020, p. 3).

[7] WP.29 is the World Forum for the Harmonization of Vehicle Regulations, a permanent working party of the United Nations.

[8] See: UNECE (4 March 2021), *UN Regulation No. 157 – Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems*. The official text is contained in ECE/TRANS/WP.29/2020/81, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/087/82/PDF/G2008782.pdf?OpenElement.

[9] The Society of Automotive Engineers is a global professional association and standards-developing organisation for engineering professionals. It established the levels of vehicle automation in its technical document J3016.

Requirements for a law enforcement interaction plan in California

California's Department of Motor Vehicles' regulations require ADSEs (described as 'the manufacturer') to provide a law enforcement interaction plan to enforcement agencies and other first responders that will instruct those agencies on how to interact with the automated vehicle in emergency and traffic enforcement situations.[10]

Some of the matters the manufacturer must cover in its law enforcement interaction plan are:[11]

- how to communicate with a remote operator
- where to obtain information about the owner, vehicle registration and insurance if there is a crash or traffic infringement
- how to safely remove the vehicle from the road
- how to recognise whether the ADS is engaged and, if possible, how to disengage the ADS
- how to detect and ensure the ADS has been deactivated.

Working Party 1[12] work on optical and audible signals

WP.1[13] is considering the issue of optical and audible signals on automated vehicles. WP.1's consideration is from the perspective of other road users, rather than enforcement officers. While no resolution has been reached, discussions and proposals have generally highlighted the risks to other road users of automated vehicles using optical and audible signals to indicate whether they are operating in automated mode. An informal paper submitted by Germany at a recent WP.1 meeting noted that such signals should not be used as a general rule but only in very specific scenarios as a temporary solution.[14]

1.4 What is covered by this paper?

1.4.1 Project scope

The scope of this project is to examine whether state and territory law enforcement officers have sufficient powers to interact with and respond to the road safety risks of automated vehicles, and to consider options to address any identified gaps. While the focus is on powers, some practical issues are also explored, with the focus less on developing new reform options and more on how industry is considering these issues and how existing or proposed mechanisms could be used to address them. The reference to 'existing or proposed mechanisms' throughout is a reference to first-supply ADSE requirements in draft ADR 90/01, the ADSE duties and in-service regulator enforcement powers in the AVSL, and other mechanisms agreed or under development in Australia and internationally.

[10] California Department of Motor Vehicles regulations, Article 3.8, cl 228.06(c)(3) and Article 3.7, cl 227.38(e).

[11] Ibid., (e)(1).

[12] WP.1 is the Global Forum for Road Traffic Safety, a permanent working party of the United Nations.

[13] WP.1 focuses on improving road safety. Its primary function is to serve as guardian of the United Nations legal instruments aimed at harmonising traffic rules.

[14] See: Global Forum for Road Traffic Safety, *Position statement on optical and/or audible signals in the context of driver assistance systems, advanced driver assistance systems and automated vehicles – submitted by Germany*, 83rd session, Geneva, 20–24 September 2021.

Key areas in scope:

- Powers and practices of state and territory law enforcement officers to interact with, intercept and ensure the safe on-road operation of automated vehicles. This includes some consideration of the relevance of the law enforcement interaction protocol (discussed in section 1.3.2).
- Access to data by state and territory law enforcement agencies to identify automated vehicles and respond to their road safety risks. This includes data on factors causing or contributing to a breach of a road traffic law or crash. This includes some consideration of practical issues that may arise, such as technical tools to access data.[15]
- Enforcement agencies sharing data with relevant parties, particularly the in-service regulator.

The project will consider international developments, including international data standards, as they evolve over the course of the project (including, if relevant, how these standards could apply domestically).

Key areas out of scope:

- Police powers and practices beyond those relating to road safety and road transport are outside scope. The focus for this work is on road safety and road transport laws, rather than on broader law enforcement issues that may relate to automated vehicles. For example, the following are not considered:
  - powers to stop an automated vehicle other than for a road safety purpose (for example, because the vehicle is suspected of carrying drugs)
  - the impact of criminal misuse of automated vehicles on police operations
  - data that might apply to criminal law investigations, missing persons enquiries and offences that may be committed in or near an automated vehicle.
- The NTC is a national land transport reform body, and our mandate focuses on transport laws rather than criminal law matters. Broader criminal law matters would likely need to be considered by law enforcement agencies together with other agencies that have a role in criminal law. The outcomes from this project could, however, guide how states, territories and the Commonwealth amend other relevant laws.
- We have not included a detailed consideration of operational impacts on enforcement roles, responsibilities and resources. This project will collate some potential operational impacts of automated vehicles on enforcement roles, responsibilities and resources. This is intended to support states and territories in considering potential operational impacts within their jurisdiction. Jurisdictions will need to consider:
  - potential changes to policies, procedures, training needs and system requirements
  - the resource, timing and cost implications of these changes.

[15] This includes accessing data through existing systems such as automatic number-plate recognition.

1.4.2 Topics we cover in this paper

The remaining sections of this chapter introduce the key issues. Each issue is considered in more detail in the chapters that follow.

- Chapter 2 considers issues around enforcement officers providing on-road directions to automated vehicles, including options to address gaps.
- Chapter 3 considers how enforcement officers could disable an ADS, and relevant processes once an ADS is disabled, including options to address gaps.
- Chapters 4, 5 and 6 consider issues around enforcement access to automated vehicle data, such as data needs, availability, access and admissibility, including options to address gaps.
- Chapter 7 considers how enforcement officers may interact with the in-service regulator, ADSEs and registered owners, focusing on timeliness, process and data sharing.
- Chapter 8 considers the potential operational impacts of automated vehicles on enforcement roles, responsibilities and resources.
- Chapter 9 outlines any conclusions reached and next steps.

We have developed the key issues this discussion paper examines through workshops and targeted consultation sessions with stakeholders.

1.4.3 Previous relevant work – Queensland University of Technology report

In early May 2021, the NTC engaged Queensland University of Technology (QUT) to provide legal research and advice on the powers currently available to state and territory law enforcement officers to ensure safe operation of automated vehicles on Australian roads and to identify any gaps.

Some key findings from QUT's report, *Applicability of state and territory roadside enforcement powers to automated vehicles* (the QUT report),[16] are that:

- Most roadside enforcement powers focus on a driver, making the application of roadside enforcement powers to an ADS uncertain.
- There is considerable diversity in state and territory roadside enforcement powers. For example, some jurisdictions have multiple pathways to stop a vehicle, while other jurisdictions have relatively few powers to do so.
- There are differences in roadside enforcement powers for light and heavy vehicles (QUT, 2021).

While QUT's research and analysis are used throughout, this discussion paper does not reference the QUT report except when directly quoting from the report or referring the reader to further detail contained in the report on a specific issue.

[16] See: https://www.ntc.gov.au/sites/default/files/assets/files/QUT%20report%20-%20Applicability%20of%20state%20and%20territory%20roadside%20enforcement%20powers%20to%20automated%20vehicles%20-%20July%202021.pdf

1.4.4 Project milestones

1. Development of key issues and options

From July 2021, the NTC, in consultation with Commonwealth and state and territory road transport agencies and law enforcement agencies, has refined the scope, issues and options for this project. The NTC also engaged with:

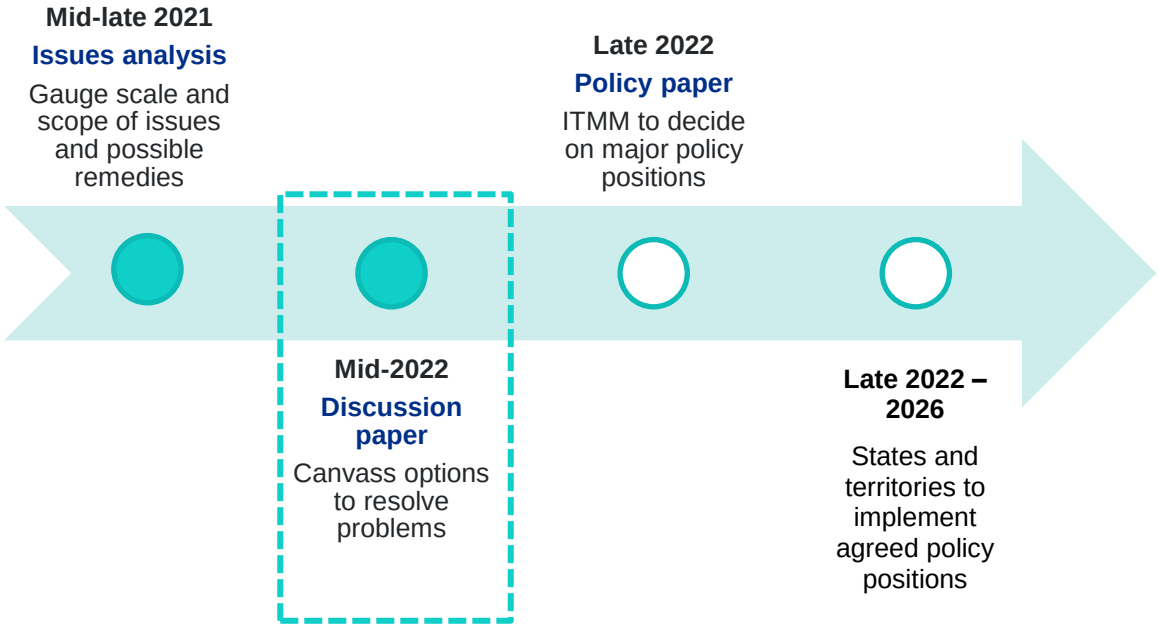
- industry stakeholders, to understand how potential ADSEs were considering law enforcement interaction from a practical perspective and to explore the practical implications of possible approaches and options
- our international counterparts, to share ideas about enforcement in anticipation of the arrival of automated vehicles on the roads.

2. Discussion paper and next steps

This discussion paper consolidates the issues and options developed during workshops and targeted consultation. After the publication of this discussion paper the NTC will continue to consult broadly with government stakeholders, industry, other regulators and the wider public. Feedback will be analysed to develop a final policy paper and recommendations. These will be delivered to the Infrastructure and Transport Ministers' Meeting (date to be announced).

The timeline for these activities is presented in Figure 1.

Figure 1. Project milestones and timelines



2 Providing directions to automated vehicles on road

Key points

- Enforcement officers may need additional powers to stop, intervene and give directions to an ADS, remotely or at the roadside.
- The technical capability of automated vehicles to respond to directions is still being developed.
- Enforcement officers may not have the powers to stop an automated vehicle remotely under current state and territory laws.

2.1 Directing an ADS

In this section we discuss powers of enforcement officers to direct an ADS, including directing it to stop, under current state and territory laws. We also discuss the practical considerations of directing an ADS and propose options to address identified gaps.

2.1.1 Powers to direct an ADS

Enforcement officers' powers under state and territory laws to direct road traffic are essential in supporting a range of other powers designed to maintain road safety. They broadly include:

- interacting with vehicles in an emergency or where occupants' future safety is at risk
- gathering information related to offences under road, traffic or vehicle laws.

An ADS is not the 'driver'

Many enforcement powers relating to directing road traffic in state and territory laws refer to the 'driver' of a vehicle, with 'driver' defined as a person (QUT, 2021, p. 62). Under state and territory interpretation Acts, a 'person' is defined as a natural person or a corporation.

The ADS is neither a natural person, nor a corporation. The ADS cannot be the 'driver' as understood by state and territory laws because the ADS does not fall within the current definitions of 'driver'.

Therefore, when the ADS is engaged at levels 3, 4 and 5 automation it is performing the driving task and is in control of the vehicle, but it is not the 'driver' of the vehicle. When the ADS is engaged, existing police powers for directing road traffic may not apply.

Heavy Vehicle National Law

The potential gap in enforcement powers also arises under the HVNL in relation to the power to stop heavy vehicles. This is because directions to stop a vehicle are similarly focused on a 'driver'. The definition of 'driver' under the HVNL, which 'includes a reference to a person in, on or in the vicinity of the vehicle who an authorised officer present at the scene reasonably believes is the vehicle's driver',[17] is potentially broader than the definition under general state and territory powers (QUT, 2021, p. 50). However, there is still no clear application to an ADS.

In addition, stopping powers under the HVNL are provided to allow enforcement officers to exercise other powers under the HVNL,[18] rather than an ability to provide on-road directions to heavy vehicles more broadly (Brady, et al., 2021, p. 52).

Responsibility for non-dynamic driving task obligations

The ADSE is responsible for complying with dynamic driving task (DDT) obligations when the ADS is engaged. (National Transport Commisssion, 2018).

There are also a range of existing driver obligations that do not relate to the DDT and that cannot or may not be able to be included in the design and programming of the ADS. We refer to these as non-DDT obligations. Generally, an ADSE should not be responsible for these obligations – but there are some exceptions to this.

One such example of a non-DDT obligation that was identified in the Changing driving laws policy paper was that of Australian Road Rule 304, a non-DDT obligation that is essential for road safety and closely linked to the DDT (National Transport Commisssion, 2018, pp. 43-44). Australian Road Rule 304 requires that a person obeys any reasonable direction for the safe and efficient regulation of traffic given to the person by a police officer or authorised person, whether or not the person may contravene another provision of the Australian Road Rules by obeying the direction. We suggested that, at least in a dedicated automated vehicle (that is, a vehicle with no manual controls enabling it to be driven by a human driver), the ADS would need to follow police directions.

In a non-dedicated automated vehicle, it may be possible to assign obligations to the fallback-ready user.[19] It may also be possible to assign obligations to an occupant in a level 4 or 5 vehicle. Responsibility for non-DDT obligations will be considered separately to this on-road enforcement project, and there is a separate piece of work being led by the NTC in conjunction with states and territories that is currently underway. Discussions about these issues are ongoing throughout 2022.

2.1.2 Automated vehicles recognising and responding to directions

Powers of enforcement officers to direct automated vehicles is closely linked to the types of directions, the methods by which directions are given, and the technical capacity of automated vehicles to respond to enforcement officer directions.

---

[17] Heavy Vehicle National Law, s 512.

[18] Heavy Vehicle National Law, s 513(a).

[19] The fallback-ready user is a human in a level 3 vehicle who can operate the vehicle, and who can receive requests from the ADS to intervene and evident DDT performance-relevant system failures. The fallback-ready user is expected to respond by taking control of the vehicle.

Direction types and methods – enforcement powers

The types of directions and the methods for giving those directions are generally contained in current state and territory laws. Types of directions could include directions to stop and where to stop.

Automated heavy vehicles will most likely need to respond to a more diverse range of directions than light vehicles. For example, they may need to follow enforcement officer directions to enter checking stations or inspection sites. They may also need to follow various directions for moving heavy vehicles during an inspection. There are a variety of methods by which directions can be communicated, including hand signals, visually, orally, via audible alarm signals or by some other means (QUT, 2021, p. 26).

The method for giving directions is relatively broad in most jurisdictions, with some having wide-ranging definitions. For example:

- *Road Safety Act 1986* (Vic), s 64A(5): *direction to stop* means "any action … to indicate to a driver of a motor vehicle that he or she must stop the motor vehicle, including but not limited to the following … [hand signals, display of signs, flashing lights, sounding of alarms and sirens]".
- Police Powers and Responsibilities Regulation 2012 (Qld) s 17(1): for s 59 of the Act, "a police officer may, by giving a direction or by signalling in a way stated in schedule 7".
- (in relation to requiring a vehicle to be moved) – *Transport Operations (Road Use Management) Act 1995* (Qld), s 33(3A): "… may be made orally or in any other way".
- *Road Traffic (Administration) Act 2008* (WA), s 43(1): a direction "… may be given … orally or by means of a sign or signal (electronic or otherwise), or in any other manner".

Other jurisdictions simply refer to signals or directions without specifically noting any methods for providing a direction.

If the methods for giving directions to drivers are sufficiently broad and inclusive in existing laws (which they appear to be), these laws could cover methods for giving directions to automated vehicles without requiring amendment.

Capability of ADS technology to follow enforcement officer directions

Stakeholders suggested it is important to consider the capability of ADS technology to follow specific directions of enforcement officers in tandem with the necessary powers of enforcement officers to direct an ADS. They noted some key considerations are whether automated vehicles can:

- respond to sirens and lights
- identify and follow hand signals and the intention of such signals (stop, move to a different lane, pull into a breath testing site)
- differentiate authorised officers from others attempting to direct traffic
- respond to unmanned roadblocks
- respond to directions in unusual situations or where the ADS is malfunctioning.[20]

[20] This point is linked to the on-road behavioural competency requirement in the current draft ADR 90/01, and we won't be specifically considering it further. See: Vehicle Standard (Australian Design Rule 90/01 – Steering System) 2021, Appendix B, clauses 3.2.36 and 4.2.26.

Stakeholders noted that there could be a benefit derived from standardising the methods by which directions are given if such an international standard exists. Bringing direction protocols in line with international practice, if and when it is established for automated vehicles, may help to encourage automated vehicles access to the Australian market.

Potential ADSEs (including those the NTC consulted with) are considering how their automated vehicles will interact with enforcement officers on the road in a variety of ways. Some examples include:

- An automated vehicle using sensors to detect police vehicles through their appearance, sirens and emergency lights and pulling over when a police or emergency vehicle is detected flashing its lights.
- An ADS making contact with its ADSE when it recognises it cannot follow the direction, rather than requiring police to make that contact.
- Training the ADS (through trials) to respond to traditional police directions. These trials will assist the ADS developer to determine how it would validate that the ADS can comply with police directions.
- That it may be possible for an automated vehicle to interpret hand signals and other relevant methods giving directions. However, where an automated vehicle sees an obstacle or cannot comply with a manual direction, it would stop.

Some potential ADSEs also noted that they would work closely with law enforcement to ensure officers are aware of how to interact with their automated vehicles. It is very important for industry to be provided with guidance around what they need to show to validate that they can interact with enforcement.

The Automated Vehicle Safety Consortium has developed best practice recommendations for first responder interactions with fleet-managed dedicated automated vehicles (ADS-DVs). These recommendations provide that: (Automated Vehicle Safety Consortium, 2020, p. 10)

- the ADS should be able to follow a direction independently or through communications with a fleet operator
- the ADS should be capable of detecting and reacting to emergency vehicles where they are identifiable by features such as flashing lights and sirens
- ADSEs should ‘document instructions for communicating with an ADS-DV and contacting fleet operators in interaction plans’.

Existing or proposed mechanisms

Enforcement interaction requirements in ADR 90/01

ADR 90/01 outlines ADS safety requirements at first supply. The current draft of ADR 90/01 provides that ‘the ADSE must provide a description of the functionality of the ADS relating to its interaction with enforcement agencies and emergency services as well as provision of information in real time at the roadside’.[21]

While this requirement is formulated in broad terms, it is a starting foundation for an ADSE to address the issue of following enforcement officer directions.

[21] Vehicle Standard (Australian Design Rule 90/01 – Steering System) 2021, Appendix B, clause 4.2.25

Law enforcement interaction protocol

As mentioned in section 1.3.2, infrastructure and transport ministers have agreed the in-service framework for automated vehicles, including that the in-service regulator should publish guidance on the areas to be covered in LEIPs, in conjunction with state and territory enforcement agencies.

The purpose of LEIPs is to ensure enforcement officers have clarity about how they can safely interact with automated vehicles. They could cover:

- how officers can intercept and safely stop an automated vehicle
- how the automated vehicle will recognise enforcement and emergency services on the road or at the roadside.

2.1.3 Proposed approach and options

The power to provide an on-road direction to an automated vehicle needs to be accompanied by a corresponding obligation on the entity performing the dynamic driving task to comply with the direction. This is because, as we noted in 2.1.1, the automated vehicle could be under the control of a human driver as the fallback-ready user or the ADS.

There is also considerable ambiguity about the technological capability of the ADS to follow the variety of directions that a human driver encounters and navigates at any given time. The requirement in ADR 90/01 and future guidance on what ADSEs should include in LEIPs described above could go some way to ensuring that ADS technology can follow specific directions of enforcement officers. However, as the ADR is designed to be technology neutral, it is left deliberately broad at this stage because ADSEs should indicate how they will meet the required criteria. As such the ADR may not provide sufficient guidance to ADSEs to ensure that their ADS can interact with enforcement.

Noting the above, we propose a broad approach to amend enforcement powers to incorporate all parties that may be required to comply with enforcement officer directions once automated vehicles are operating on the road, while retaining flexibility in how such directions might work or evolve in practice. We also propose several options to address the ambiguity around the technological capability of the ADS. These are considered below.

Amend enforcement powers to incorporate all responsible parties

We propose that enforcement powers should be amended to ensure enforcement officers can legally provide directions for relevant circumstances and obligations to:

- a person (such as the driver, fallback-ready user, passenger or other type of person)
- the ADS.

For example, if the ADSE is required to comply with Australian Road Rule 304 (even if just in certain circumstances), then enforcement powers should be amended to include the ADS as a system to which enforcement officers can provide an on-road direction.

Capability of an ADS to follow enforcement officer directions – options

As noted above, it appears that the methods for enforcement officers to give directions in current state and territory laws are sufficiently broad to capture any new methods for providing directions that may be required for automated vehicles. It is relevant to consider the types of directions and methods for providing those directions that an ADS can follow in practice.

As mentioned in section 2.1.2, potential ADSEs are considering how their ADSs will interact with enforcement officers, including recognising and following directions; however, some have suggested that they need further guidance to ensure that what they are developing will be fit-for-purpose. We need to bring together the capability of an ADS to follow enforcement officer directions with the practicalities of how officers will provide directions to automated vehicles. We also recognise that there may need to be greater consistency and clarity of the way directions are made by enforcement officers so ADS' can be trained to follow certain directions and that the diversity of officers' signals makes this process more technically challenging.

We suggest two options that could be adopted to help ADSEs develop the capacity of their ADS to interact with enforcement officers and act on directions. We acknowledge the two options are not mutually exclusive and can both be actioned, if desired.

Option 1: Guidance documentation on ADR 90/01 requirement

Additional guidance documentation, separate to an enforcement interaction protocol, could be drafted. This would accompany ADR 90/01 and explain how ADSEs can meet the 'interaction with enforcement' requirement in ADR 90/01. This could include the types of directions and the methods for providing those directions that an ADS would generally need to follow to interact with enforcement on Australian roads. The guidance could differ for light and heavy vehicles to capture some of the additional considerations that are generally only relevant for heavy automated vehicles.

It seems preferable to include this detail in guidance material rather than in ADR 90/01 itself to ensure it can be updated relatively quickly and to ensure the ADR is not overly prescriptive. Keeping this further detail together with the first supply requirements would ensure that if greater detail on this topic is agreed internationally, the internationally agreed requirements could replace (fully or in part) the requirement in ADR 90/01 and the associated guidance material.

While the guidance material would assist ADSEs to plan and validate how their ADS is to interact with enforcement, we note that this option has several potential shortcomings:

- There is no agreed place to publish this guidance documentation.
- Once a vehicle has been supplied to the market, there is no requirement to make technical updates to vehicles in service if an ADR or additional guidance has been updated, making compliance with guidance difficult to ensure.
- If the guidance documentation is attached or associated with the ADR, having the requirements for enforcement directions in ADR 90/01 means that when updates are made, only new vehicles need to comply with them, resulting in inconsistent responses to enforcement directions.
- Updates to the ADR guidance documentation have long lead times as increases in regulatory stringency must go through a regulation impact assessment process and harmonisation with international automated vehicle regulations will be hampered.

Option 2: Specify the type and method for giving directions in road rules

The types of directions to automated vehicles and the methods for giving those directions could be specified in the road rules. Under the public version of ADR 90/01, when an ADS is engaged it is required to operate in compliance with all applicable Australian state and territory road traffic laws and, where there is no contradiction, the Australian road rules.

The chief benefit of this option is that the ADSE is obliged to ensure continued compliance with any amendments to relevant road traffic laws when they come into force, overcoming the in-service compliance issue noted in option 1.

A challenge of this option is that the lengthy development and consultation process of establishing or changing road rules could preclude jurisdictions from making timely alterations to complement a change in procedure or technology.

Another challenge to this option is that it remains unclear how enforcement officers will determine whether a vehicle is an automated vehicle or not. If the types of directions to be given to automated vehicles are different from the directions for conventional vehicles, this increases the risk that enforcement officers may make errors in critical moments.

Should there be difficulties with providing directions to an automated vehicle, it was noted from stakeholder feedback that there is a desire for law enforcement to have a direct point of contact for a resolution. The timeliness of communication between law enforcement and ultimately the party responsible for the automated vehicle is of great importance.

2.2 Using intervention and pursuit tactics

Powers to stop are often connected with powers to use intervention and pursuit tactics, such as powers to immobilise a vehicle and powers to erect roadblocks.

In this section we consider whether enforcement officers have powers to use intervention and pursuit tactics in relation to automated vehicles under current state and territory laws and propose an approach to address identified gaps.

2.2.1 Current powers to use intervention and pursuit tactics

There appear to be two different categories of powers to use intervention and pursuit tactics in the context of road safety and road transport laws:

- Category 1 powers are those that are not directed at human driver behaviour and therefore do not raise issues or gaps for automated vehicles. These include powers in Victoria's Road Safety Act[22] and the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW),[23] which are either directed at vehicles (Victoria) or the existence of road safety risks (New South Wales) rather than at human driver behaviour.

[22] See *Road Safety Act 1986* (Vic), s 63B(1)(b): The Chief Commissioner of Police may authorise the use by police officers of a vehicle immobilising device[22]… to stop or assist in stopping a vehicle in connection with the pursuit of the vehicle by police officers. (emphasis added)

[23] See *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 37(2)(b): A senior police officer may authorise another police officer to exercise any or all of the vehicle roadblock powers[23]… if the senior police officer suspects on reasonable grounds that … circumstances exist on or in the vicinity of that road, road related area, place or school that are likely to give rise to a serious risk to public safety and the exercise of the powers may lessen the risk. (emphasis added)

- Category 2 powers are directed at human driver behaviour. These include powers such as those in the *Summary Offences Act 1953* (SA),[24] which cover the driver disobeying a request to stop. The South Australian provision specifically relates to a driver failing to follow a police direction. This raises the issue discussed above at section 2.1.1 (that is, that the ADS does not fall within the current definition of 'driver').

Vehicles used to commit criminal offences

Powers to immobilise vehicles often arise in relation to suspicion of criminal offences. While criminal law matters beyond road safety and road transport laws are out of scope for this project, it is relevant to note that powers to immobilise a vehicle and powers to erect roadblocks for these offences tend not to be directed at controlling human driver behaviour and therefore may not raise issues or gaps for automated vehicles.[25]

2.2.2 Proposed approach to using intervention tactics on automated vehicles

Category 1 powers

Category 1 powers do not appear to raise issues or gaps for automated vehicles because they can be exercised without reference to a human driver. We are not proposing any changes to these powers.

While the category 1 powers themselves do not raise any specific issues, some issues may arise once the intervention and pursuit tactic power has been exercised. For example, if a vehicle has been immobilised by use of road spikes, enforcement officers may need to provide further directions to ensure the automated vehicle continues to be restrained from being driven. For conventional vehicles, such a direction would likely be provided to the driver. For automated vehicles, this direction may need to be provided to another person or system (such as the ADS or fallback-ready user). The powers and proposed approach discussed in section 2.1 above, including amending the definitions of 'driver', may be relevant here, but states and territories would need to consider whether there are additional powers that may need to be amended.

Category 2 powers

Enforcement powers to use intervention and pursuit tactics that are linked to direct actions by a driver should be amended to ensure they can apply where the driving task is performed by another person or system (where it is that person or system that enforcement officers would have provided a direction to). This would resolve the issue that an ADS does not fall within the current definition of 'driver' and allow other parties (such as the fallback-ready user) to be captured, if relevant.

[24] See *Summary Offences Act 1953* (SA), s 74BAA(1)(a)(i): if an authorised officer believes on reasonable grounds that the driver of a motor vehicle has disobeyed, or is likely to disobey, a request or signal to stop given under this or any other Act … the officer may use a vehicle immobilisation device. (emphasis added)

[25] See, for example, *Summary Offences Act 1953* (SA), s 74BAA(1)(a)(ii)(A); *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 37(2)(a).

2.3 Stopping an automated vehicle remotely

Stakeholders have raised that the best safety outcome would be if enforcement officers have the authority and ability to stop an automated vehicle remotely, and that a technological solution to enable this is preferred.

In this section we consider whether enforcement officers have the powers to stop an automated vehicle remotely under current state and territory laws and whether such powers are necessary from a practical perspective.

2.3.1 Powers to stop a vehicle remotely

It is relevant to note that stopping a vehicle remotely is a subset of vehicle immobilisation powers,[26] and so issues discussed in section 3.2 would also apply here.

Therefore, the focus of this section is whether stopping a vehicle remotely is contemplated by existing enforcement powers – in particular, by the definition of a vehicle immobilising device (or similar). Some examples include:

- Victoria's Road Safety Act, s 63B(3): *vehicle immobilising device* means a device capable of causing a vehicle to stop or preventing a vehicle from moving and includes a device designed for, or capable of, deflating tyres.
- SA's Summary Offences Act, s 74BAA(4): *vehicle immobilisation device* means a device declared by regulation to be a vehicle immobilisation device.
- SA's Summary Offences Regulations 2016 (under the Summary Offences Act), cl 34 provides that 'the Stinger Spike System', 'the Stop Stick' and 'the Scorpion Rat Trap' are declared vehicle immobilisation devices.

The Victorian and South Australian examples highlight the variation in the definitions of a vehicle immobilising device (or similar) in current state and territory laws. The Victorian definition is relatively inclusive and refers to a device capable of stopping a vehicle from moving. This could be broad enough to capture a remote engine immobilisation device. Conversely, the South Australian definition is dependent on devices declared by regulations, which currently do not appear to include remote engine immobilisers.

Despite these differences in definitions, whether there is an issue or gap in current enforcement powers is closely linked to practical considerations around the availability of remote engine immobilisation technology and its safety risks. That is, even if current laws do not include powers to use remote engine immobilisers, there is only an issue or gap if such powers are necessary from a practical perspective. We consider this directly below in section 2.3.2.

We note that current methods for stopping a conventional vehicle which are practiced by law enforcement, such as spike strips, can also be used on automated vehicles.

[26] Stopping a vehicle remotely would likely require some form of engine immobilisation. Generally, fixed engine immobilisers prevent an engine from starting whereas remote engine immobilisers could operate on a moving vehicle (See: 57th Queensland Parliament Transport and Resource Committee, *Inquiry into vehicle safety, standards and technology, including engine immobiliser technology,* September 2021, p. 32).

2.3.2 Practical considerations for stopping a vehicle remotely

As noted in section 2.3, some stakeholders raised that the best safety outcome would be if enforcement officers can stop an automated vehicle remotely. However, this was not a consensus view because other stakeholders suggested this creates safety and cybersecurity risks.

A recent Queensland Parliamentary inquiry report noted that 'while remote immobilisation technology is progressing it had not yet sufficiently developed to be useful in assisting police' (57th Queensland Parliament Transport and Resource Committee, 2021, p. 188). The report referred to 2019 findings from the Australia New Zealand Policing Advisory Agency (ANZPAA) suggesting that little had changed since that report.

Some findings from the ANZPAA report included the following:

- there could be unintended safety consequences from deploying a remote engine immobiliser (REI) on a moving vehicle.
- while REIs exist, they operate on a much smaller scale than envisaged for policing
- mandated REIs have not been successfully implemented across the vehicle fleet anywhere in the world
- adopting REIs through ADRs is not feasible, with one reason being that there isn't a clearly defined and tested safety benefit of REIs.

Remote engine immobilisation is also not an issue specific to automated vehicles, so the inability of enforcement officers to stop an automated vehicle remotely is not in itself a gap. We propose that it should be considered as part of any broader work on remote engine immobilisation, rather than through the automated vehicle reform program.

We consider this issue in a more automated vehicle-specific context in the next chapter, where we consider the potential for remotely disabling an ADS.

Question 1: Do you support amending enforcement powers to ensure enforcement officers can legally provide directions?

Question 2: Will either of the options proposed – that is, the provision of guidance documentation or the addition of directions to the road rules – best offer a pathway for giving ADSEs information on how to build the capability of their technology?

Question 3: If guidance documentation is preferred, where would the guidance documentation be best placed?

Question 4: Are there any powers not covered in this paper that may need to be amended to ensure enforcement officers have sufficient powers to use intervention or pursuit tactics?

3 Disabling an automated driving system

Key points

- Enforcement officers may need additional powers to be able to disable an ADS at the roadside. These powers could apply only where there is an immediate safety risk or for broader reasons.
- There may be safety risks associated with disabling an ADS remotely.
- Enforcement officers may need additional powers to be able to tow or remove an automated vehicle from the road after the ADS has been disabled. There is scope for these powers to be worded to apply in all circumstances or only in those circumstances where there is an occupant that cannot drive the vehicle.

3.1 Disabling an ADS at the roadside and remotely

3.1.1 Powers to disable an ADS

In the previous chapter we discussed powers to direct an ADS, including directions to stop a vehicle. When a conventional vehicle has stopped, there is generally no longer an immediate safety risk presented by the vehicle itself. However, for an automated vehicle, even where the vehicle has stopped, there may still be a safety risk remaining if the ADS is not disabled. By disable, we mean the ADS has been disengaged so it is no longer in automated mode. For example, though a malfunctioning ADS may have brought the vehicle to a stop in response to police warnings, it may still subsequently take unsafe action.

In some automated vehicles, there may be a human user inside who can disable the ADS themselves, but this may not always be the case – either because the vehicle has no human occupants, or because the occupants cannot or will not disable the ADS. In these circumstances, it may be necessary for enforcement officers to disable an ADS themselves to prevent any immediate safety risks.

There may also be broader circumstances where it may also be desirable for officers to disable an ADS themselves. For example, officers at the scene of an incident may consider it necessary for the ADS to be disabled if there is concern about the ADS driving away prior to preliminary investigations or information exchange being complete.

In initial consultation, there were differing views on whether an ADS that has brought itself to a stop would ever present a residual safety risk, and whether enforcement officers would need the ability to disable the ADS themselves.

Existing and proposed mechanisms

Current enforcement powers allow enforcement officers to immobilise a vehicle in certain circumstances (as discussed in section 2.2.1). However, there are no specific powers in state and territory laws addressing the power to disable an ADS.[27]

[27] Disabling an ADS and immobilising a vehicle are different concepts; however, we note that in a dedicated automated vehicle, disabling the ADS will in effect immobilise the vehicle due to the lack of manual controls.

Under the proposed AVSL, the in-service regulator will have the power to suspend the operation of an ADS until a safety issue is resolved, or even permanently suspend an ADSE. These powers would require the ADSE to disable its ADS to stop it from operating, and this power could extend to disabling a whole ADS fleet. However, these powers rest with the in-service regulator and would be used only after it has undertaken its own investigations under the AVSL. These powers would therefore not be sufficient to address an immediate safety risk encountered on the road or at the roadside.

The NTC therefore considers that existing and proposed enforcement powers are insufficient to deal with the potential safety risks or other scenarios. In the following sections, we explore whether enforcement officers require a power to disable an ADS to mitigate potential safety risks in particular, or to deal with other scenarios where disabling an ADS may be appropriate.

3.1.2 Practical considerations for disabling an ADS

Before considering a proposed approach to powers, it is necessary to consider the capabilities of ADS technology to let enforcement officers disable an ADS. In our initial consultation, government stakeholders stated it was important to consider disabling an ADS both at the roadside and remotely. These scenarios present different practical considerations.

At the roadside

Some automated vehicle companies are already preparing for disabling the ADS at the roadside. For example:

- Enforcement officers can disable automated driving mode in Waymo vehicles by contacting Waymo at the roadside, requesting that the vehicle is authorised for manual mode and following instructions that will include pressing buttons on the steering wheel (Waymo, 2021, p. 16).
- In its *Driverless deployment program guidance for first responders*, Cruise notes that enforcement officers can contact its Incident Expert team to disengage the vehicle from automated mode and immobilise the vehicle (Cruise, 2021, p. 21).
- Another company explained that while they have not specifically considered the ADS being disabled at the roadside, it is important to ensure enforcement officers can reach the ADSE with 24/7 connectivity.

These examples highlight that the current focus is on enforcement officers contacting the ADSE to disable the ADS – that is, the focus is on the ADSE intervening. However, in Waymo's example, while enforcement officers would contact Waymo for instructions and authorisation, it is still the enforcement officer who disables the ADS.

The Automated Vehicle Safety Consortium's best practice guidance for first responder interactions also provides recommendations around disabling and ADS-dedicated vehicle (ADS-DV). It provides that (Automated Vehicle Safety Consortium, 2020, p. 9):

- ADS-DVs should be capable of being kept from moving.
- ADSEs should provide instructions in interaction plans about how to safely disengage the ADS to ensure it will not 'self-drive'.

Existing and proposed mechanisms

The 'interaction with enforcement' requirement in ADR 90/01 (outlined in section 1.3.2) may not currently extend to disabling an ADS, but the requirement for ADSEs to develop and maintain an enforcement interaction protocol could potentially address this issue. We previously noted that the protocols could cover how enforcement officers can disable an ADS.[28]

Remotely

In initial consultation, there was some interest from government stakeholders in having the ability to disable the ADS remotely. This action could be as substantial as a 'kill-switch', or through a non-destructive pursuit tactic such as sending a remote direction or command to the ADS to bring the vehicle to a minimal risk condition or to perform a minimum risk manoeuvre.[29] However, unlike for disabling the ADS at the roadside, industry stakeholders we consulted indicated they are not considering or planning for enforcement officers to be able to disable the ADS remotely. One company noted the cybersecurity risks that could arise from allowing the ADS to be remotely controlled by enforcement officers.

Existing and proposed mechanisms

Because the above regulation potentially applies to enforcement officers disabling an ADS at the roadside, the 'interaction with enforcement' requirement in ADR 90/01 may not extend to disabling an ADS remotely, but the requirement for ADSEs to develop and maintain a LEIP could potentially address this issue.

3.1.3 Disabling an ADS – proposed options and approach

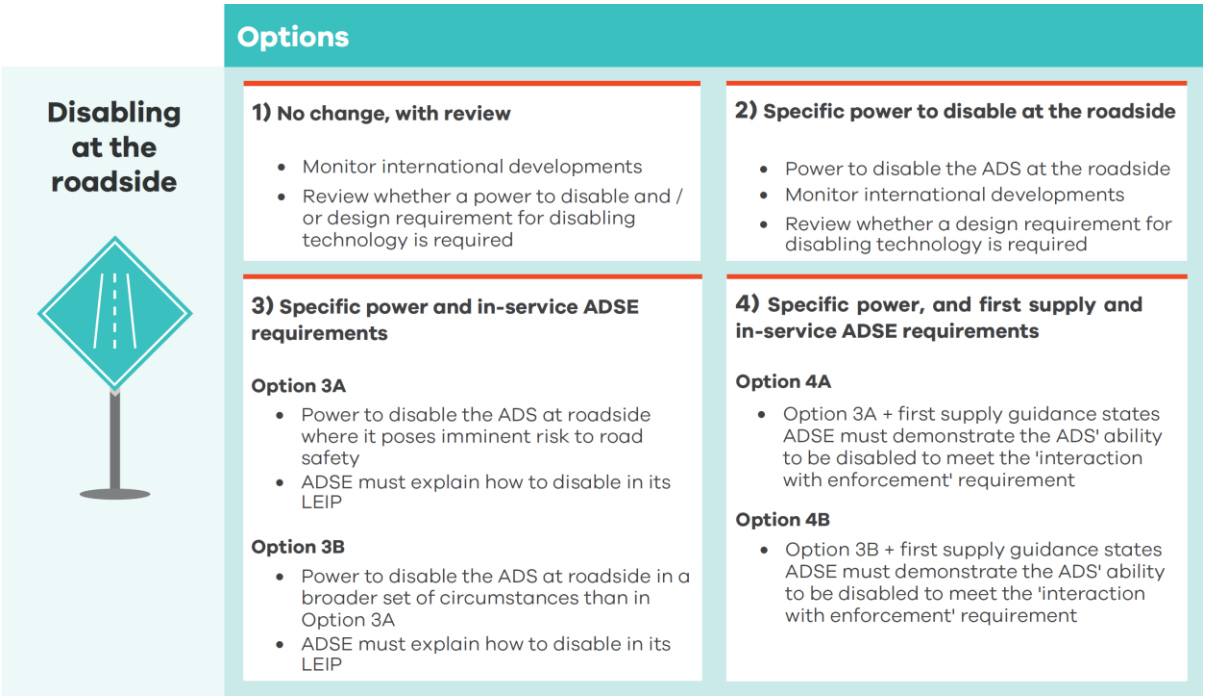
There are several options relevant to enforcement officers disabling an ADS. These options encompass both the legislative aspects of the issue (that is, powers of enforcement officers) as well as the practical aspects (that is, requirements on the ADSE to incorporate ADS-disabling technology[30]). We have set out four options with sub-options for disabling at the roadside, and a proposed approach for remote disabling.

[28] National Transport Commission, *The regulatory framework for automated vehicles in Australia*, February 2022, p. 46.

[29] The concepts of a 'minimal risk condition' and a 'minimum risk manoeuvre' are defined in the current draft of ADR 90/01. See: Vehicle Standard (Australian Design Rule 90/01 – Steering System) 2021, Appendix B, clauses 1.22 and 1.24.

[30] In this paper 'ADS-disabling capability' refers to the capability that would allow enforcement officers to disable the ADS, whether at the roadside or remotely.

Figure 2. Options to disable at the roadside



Disabling at the roadside – options

Option 1 – No change, with review

There is no new power for enforcement officers to disable an ADS themselves at the roadside. There is also no guidance or requirement on ADSEs to include disabling technology in ADSs (though they may do so). Australian governments will monitor international developments and review whether a power or design requirement (or both) is required for disabling an ADS at the roadside if international consensus emerges.

This would be an interim option, with a clear point for review should international consensus emerge on the need for disabling technology in ADSs. It would ensure that Australia kept in step with international consensus or standards around disabling an ADS at the roadside. However, should ADSEs already provide this technology in their ADSs, as we understand some are, enforcement officers would not have powers under the law to use this functionality.

We note that, regardless, enforcement officers would have the ability to contact the ADSE, who would likely be able to disable the ADS.

Option 2 – A specific power

Enforcement officers have a specific power to disable the ADS themselves only at the roadside, but there are no requirements or guidance for the ADSE to include disabling technology in their ADS (though they may do so). Australian governments will monitor international developments and review whether a design requirement is required for disabling an ADS at the roadside if international consensus emerges.

Similar to option 1, this option would not place requirements on, or provide guidance for, an ADSE to include disabling technology that enforcement officers could use to disable an ADS. However, as noted above, we understand that companies such as Waymo are already developing this procedure. This option would allow enforcement officers to use this technology, if made available by an ADSE. However, ADSEs would not be required to make this specific technology available. They would still be required to ensure the ADS can interact in some way with enforcement officers under requirements in ADR 90/01 and provide information on how this interaction would work in their interaction protocol. This option will also ensure Australia keeps in step with international consensus or standards around disabling an ADS at the roadside.

We note that the circumstances in which the power could be used could be narrow (that is, only where an ADS poses an imminent safety risk) or broader, as expanded on in options 3 and 4 below.

Option 3 – A specific power and in-service ADSE requirements

Option 3A – Enforcement officers have a specific power to disable the ADS themselves only at the roadside and only in circumstances where, unless disabled, the ADS poses an imminent risk to road safety. The ADSE will need to explain how an officer can disable the ADS at the roadside in its enforcement interaction protocol.

Option 3B – Enforcement officers have a specific power to disable the ADS themselves only at the roadside but in a broader set of circumstances than in option 3A – for example, where the automated vehicle was observed as driving in an unsafe way prior to stopping, where the officer perceives there to be a safety risk or where the officer considers an offence could occur. The ADSE will need to explain how an officer can disable the ADS at the roadside in its LEIP.

Options 3A and 3B provide enforcement officers with a specific power to disable the ADS at the roadside.

Interaction protocol guidance issued by the in-service regulator, stating that ADSEs must show how the ADS can be disabled at the roadside by enforcement officers, has the effect of ensuring that ADSEs provide this technology. In effect, an in-service requirement for this technology is introduced.

The requirements in the current draft of ADR 90/01 about interaction with enforcement may not extend to ensuring enforcement officers can disable the ADS at the roadside. There is a risk therefore that an ADSE's first supply requirements would not correspond with what is required in service. While the same outcome would be achieved in terms of providing the technology and giving enforcement officers' powers to use it, if there is no requirement at first supply for this technology then it may be unreasonable to introduce such a requirement in service through the LEIP requirements.

Given many automated vehicle manufacturers are based overseas, this makes Australia a technology taker. Having an Australia-specific technological requirement for ADS-disabling technology could also act as a disincentive for ADSEs to enter the Australian market, creating a regulatory barrier to market entry. Introducing a requirement that is out of step with international consensus and standards could result in companies not introducing or delaying introduction of their ADSs in Australia given the extra cost of incorporating the technology, especially because Australia is a technology taker. If this occurs, realising the full benefits of automated vehicles for consumers may be delayed. Both the first supply and in-service frameworks have been designed to be technology neutral, with safe outcomes rather than prescriptive technology requirements being the focus.

The options differ with respect to the circumstances in which enforcement officers can use their power to disable an ADS. Option 3A provides enforcement officers with the power to disable an ADS at the roadside in circumstances where, unless disabled, the ADS poses an imminent risk to road safety. This narrower approach recognises that, in most circumstances, it is desirable for the ADSE to control the technology it is responsible for while allowing flexibility for enforcement officers to take action where there is imminent danger.

Option 3B provides enforcement officers with the power to disable an ADS at the roadside in broader circumstances. We have noted scenarios such as observing the ADS driving in an unsafe way prior to stopping, the officer's perception that there is a safety risk, or where the officer considers an offence could occur (such as driving away from the scene of a crash). We are interested in views on whether these kinds of scenarios do warrant intervention by enforcement officers to disable an ADS or not.

Option 4 – A specific power, and first supply and in-service ADSE requirements

Option 4A – Enforcement officers have a specific power to disable the ADS themselves only at the roadside and only in circumstances where, unless disabled, the ADS poses an imminent risk to road safety. First supply guidance will state that ADSEs will need to demonstrate the ability of the ADS to be disabled by an officer at the roadside in order to meet the 'interaction with enforcement' requirement in ADR 90/01; and LEIP requirements will provide that the ADSE must explain how an officer can disable the ADS at the roadside.

Option 4B – Enforcement officers have a specific power to disable the ADS themselves only at the roadside but in a broader set of circumstances than in option 4A – for example, where the automated vehicle was observed as driving in an unsafe way prior to stopping, where the officer perceives there to be a safety risk or where the officer considers an offence could occur. First-supply guidance will state that ADSEs will need to demonstrate the ability of the ADS to be disabled by an officer at the roadside in order to meet the 'interaction with enforcement' requirement in ADR 90/01; and LEIP requirements will provide that the ADSE must explain how an officer can disable the ADS at the roadside.

Options 4A and 4B correspond with options 3A and 3B, in that they provide enforcement officers with a specific power to disable the ADS at the roadside and provide for LEIP guidance to state that ADSEs must show how the ADS can be disabled at the roadside by enforcement officers. In addition, these options propose that the Department of Infrastructure, Transport, Regional Development and Communication drafts guidance for ADSEs on how they could meet the 'interaction with enforcement' requirement in ADR 90/01 to cover the capability of ADS technology to allow enforcement officers to disable an ADS at the roadside.

Unlike in options 3A and 3B, options 4A and 4B provide consistent messaging to ADSEs at first supply and in service about the need for their ADSs to provide for disabling at the roadside by enforcement officers. Having this requirement at the outset will avoid any potential for confusion about the required capabilities of ADS technology in Australia.

As with options 3A and 3B we note that having an Australia-specific technological requirement could also be a barrier to entry because it may be out of step with international consensus and standards and would not fit with the goals of the regulatory framework to be technology neutral.

As well, options 4A and 4B differ from each other in the same way as options 3A and 3B regarding the circumstances in which enforcement officers can use their power to disable an ADS at the roadside. Option 4A provides enforcement officers with the power to disable an ADS at the roadside in circumstances where, unless disabled, the ADS poses an imminent risk to road safety. Option 4B provides for enforcement officers to disable an ADS at the roadside in broader circumstances. We are interested in views on the circumstances in which this intervention is warranted.

Disabling remotely – proposed approach

Proposed approach – No change, with review

There is no new power for enforcement officers to disable an ADS themselves remotely. There is also no guidance or requirement on ADSEs to include remote disabling technology in ADSs (though they may do so). Australian governments will monitor international developments and review whether a power or design requirement (or both) is required for disabling an ADS remotely if international consensus emerges or if this technology emerges within industry.

The need for remote disabling technology is unclear. However, to balance government and industry views, this would be an interim approach, with a clear point for review should international consensus emerge on the need for remote disabling technology in ADSs or if there are industry developments around this technology. It would ensure that Australia kept in step with international consensus or standards around disabling an ADS remotely and industry developments. However, we understand that remote ADS disabling technology is not currently being considered for international vehicle standards and that potential ADSEs are not currently contemplating introducing this technology.

Enforcement officers remotely disabling an ADS in a 'kill-switch' type way could create some significant safety risks, similar to those created by remote engine immobilisation. They key difference is that disabling an ADS while it is operating does not necessarily mean the vehicle stops (so potentially the safety risks are even greater). Having such a feature introduces significant safety risks through abuse or manipulation of ADS technology because it provides an intrusion point for cyberattacks.

The alternative pathway of issuing a command to an ADS to bring the vehicle to a minimal risk condition still leaves open an intrusion point for cyberattacks. In addition, it may be difficult for the ADS to respond to a remotely sent direction or command if the reason enforcement officers are seeking to disable the ADS is because the automated vehicle is driving unsafely due to an ADS fault. It may be more reasonable where there is a fault with the vehicle itself; however, enforcement officers may not be able to make this distinction at the roadside.

Question 5: In what instances might an ADS need to be disabled by an enforcement officer to ensure safe outcomes?

Question 6: If enforcement officers should have a power to disable an ADS, in what circumstances should this power be used? For example, should it only be used where the ADS poses an imminent risk to road safety unless it is disabled, or are there other reasons?

Question 7: Which is your preferred option for enforcement officers disabling an ADS at the roadside? Why?

Question 8: Do you agree with the proposed approach to enforcement officers disabling an ADS remotely?

3.2 Powers and processes once an ADS is disabled

Once an ADS is disabled, further action is likely required. Initial consultation with government stakeholders indicated two key considerations:

- Getting the automated vehicle off the road. Enforcement officers would need to consider:
  - Whether the ADS or the vehicle is malfunctioning (that is, whether the vehicle can be safely driven manually); it may be difficult to tell this at the side of the road.
  - If the vehicle can safely be driven manually, whether one or more of the vehicle occupants can perform the driving task.
  - Whether the vehicle needs to be transported to a particular location. For example, because the only vehicle occupants are children or those with specific disabilities.[31]

  This issue will be considered further in this chapter.
- Referring the matter to the in-service regulator, including to account for the same potentially faulty ADS being installed in other automated vehicles. Sharing data with, and referring the matter to, the in-service regulator will be considered further in chapter 8.

[31] As a related point, we note child protection laws may allow police to remove children from dangerous situations; however, this may not be the desired action immediately for practical reasons (e.g. it may be more convenient to move the vehicle from the road first, then remove the child once in a safer location).

3.2.1 Existing and proposed mechanisms

Current state and territory laws contain provisions for removing vehicles from the road, provided certain conditions are met. Some examples include:

- *Road Transport Act 2013* (NSW) s 142(a): If a danger or obstruction to traffic on a road is caused by a vehicle that has been involved in an accident or broken down, an appropriate officer may remove the vehicle … and take other steps as may be necessary to protect the public and facilitate the free flow of traffic
- (in relation to an unattended or broken-down vehicle that may be an obstruction to traffic or creating an imminent risk of serious harm to public safety) WA's Road Traffic (Administration) Act, s 46(2): The officer may move the vehicle … by driving or towing it or otherwise, to the extent reasonably necessary to prevent or minimise the harm or risk, or prevent or remove the obstruction.

There are also provisions in current state and territory laws for vehicles to be seized or impounded including for offences such as failing to stop a vehicle for police (*Road Transport (Safety and Traffic Management) Act 1999* (ACT) ss 5C, 10B(1)(a), 10C, and *Police Powers and Responsibilities Act 2000* (Qld), ss 69A(1)(b), 754, 74).

Provisions relating to vehicle defect notices may also be relevant. There are generally multiple levels of vehicle defects (for example, minor defects and major defects). In circumstances where an ADS is disabled at the roadside, this could indicate that there is a major vehicle defect. A vehicle defect notice puts limits on the vehicle's use and can require it to be moved to another location.

For example, Road Transport (Vehicle Registration) Regulation 2007 (NSW) cl 70 provides that a major vehicle defect notice may be issued where further use of the vehicle could constitute an imminent and serious safety risk. In that circumstance, the defect notice must state how the vehicle must be moved to another location.[32]

The ability of vehicle defect notice powers and vehicle seizure and impounding provisions to be used by enforcement officers to remove automated vehicles from the road appears limited:

- Provisions relating to vehicle seizure and impounding do not appear to be useful for immediate removal of an automated vehicle from the road. For example, the provisions in the ACT's Road Transport (Safety and Traffic Management) Act require a court to first convict a person of a relevant offence before the vehicle can be impounded.
- Vehicle defect notice powers focus on ensuring the remedying of vehicle defects rather than on removing a vehicle from the road at a particular time. In addition, the extent to which an issue with the ADS would amount to a vehicle defect is not clear.

This is relevant for both conventional and automated vehicles.

[32] See Road Transport (Vehicle Registration) Regulation 2007 (NSW), cl 70(1)(a) and 70(5)(c).

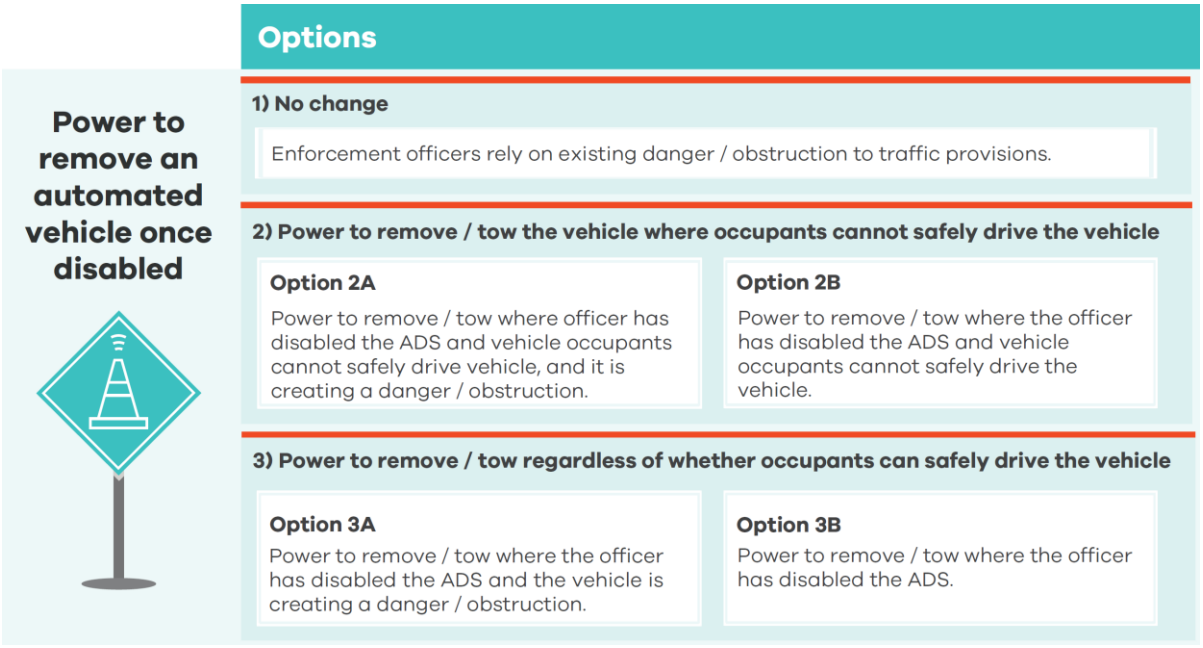
The most adaptable powers appear to be those relating to removing the vehicle from the road due to a danger or obstruction to traffic. However, some of the preconditions – such as requiring the vehicle to be broken down, involved in an accident or unattended – may not apply in circumstances where the ADS has been disabled. In addition, in circumstances where the vehicle needs to be transported to a particular location (for example, because the only vehicle occupants are children), it may be insufficient to simply move or tow the vehicle only to the extent necessary to remove the danger or obstruction the vehicle is causing (as the provisions generally require).

Given the above gaps in the existing regulation, the existing police powers may be insufficient to remove an automated vehicle from the road once its ADS has been disabled.

3.2.2 Proposed options

We propose three options to address the issue of enforcement officers being able to remove an automated vehicle from the road once its ADS has been disabled.

Figure 3. Power to remove an automated vehicle once disabled - options



Option 1 – No change

Enforcement officers will rely on the existing danger and obstruction to traffic provisions to remove an automated vehicle from the road once its ADS has been disabled.

Under this option, enforcement officers will need to rely on the existing danger and obstruction to traffic provisions to remove an automated vehicle from the road once its ADS has been disabled.

As previously noted, we consider there are gaps in the existing regulation such as preconditions (for example, requiring the vehicle to be broken down, involved in an incident or unattended) or scenarios where a vehicle should be transported to a particular location rather than just removed from the road (for example, where the occupants are children). This may result in enforcement officers being unable to remove an automated vehicle from the road.

Option 2 – Power to remove or tow the vehicle where occupants cannot safely drive the vehicle

Option 2A – Enforcement officers have the power to remove or tow the vehicle where they have disabled the ADS and one or more vehicle occupants cannot safely drive the vehicle with the ADS disabled. The vehicle must be creating a danger or an obstruction to traffic.

Option 2B – Enforcement officers have the power to remove or tow the vehicle where they have disabled the ADS and one or more vehicle occupants cannot safely drive the vehicle with the ADS disabled. The vehicle does not need to be creating a danger or an obstruction to traffic.

Under options 2A and 2B, enforcement officers would have a power to remove or tow an automated vehicle where they have disabled the ADS, but the power would be limited to situations where one or more vehicle occupants cannot safely drive the vehicle. However, one key challenge with these options is the ability for enforcement officers at the roadside to determine whether the automated vehicle is safe to be driven manually. For example, where the vehicle was driving in an unsafe way, the officer may not be able to determine whether this was due to an ADS fault or vehicle fault.

If enforcement officers cannot decide this at the roadside, then whether the occupants can safely drive the vehicle no longer becomes a relevant consideration because the officer would not know whether the vehicle itself could be safely driven in manual mode.[33]

Under option 2A, the power could only be used where the vehicle was creating a danger or an obstruction to traffic. Under option 2B, the power is broader and could be used in any circumstance. This would allow for enforcement officers to move the vehicle to a particular location in scenarios such as taking unaccompanied children or people with mobility issues in the vehicle to a safe place or more convenient place. These scenarios may be more likely in automated rather than conventional vehicles.

[33] We note that access to data is considered further in the next chapters; however, there may still be instances where relevant data cannot be accessed at the roadside for practical reasons.

Option 3 – Power to remove or tow the vehicle regardless of whether occupants can safely drive the vehicle

Option 3A – Enforcement officers have the power to remove or tow the vehicle where they have disabled the ADS but are not required to consider whether one or more vehicle occupants can safely drive the vehicle with the ADS disabled. The vehicle must be creating a danger or an obstruction to traffic.

Option 3B – Enforcement officers have the power to remove or tow the vehicle where they have disabled the ADS but are not required to consider whether one or more vehicle occupants can safely drive the vehicle with the ADS disabled. The vehicle does not need to be creating a danger or an obstruction to traffic.

Under options 3A and 3B, enforcement officers would have a power to remove or tow an automated vehicle where they have disabled of the ADS, regardless of whether there are occupants who could safely drive the vehicle. Unlike option 2, this option would not require the officer to determine whether the vehicle could be driven safely by an occupant, which may be a more practical outcome at the roadside. As with the reasoning behind options 2A and 2B, options 3A and 3B allow enforcement to use the power in particular scenarios, when the vehicle is creating a danger or an obstruction to traffic, consistent with current powers (3A) or in any circumstance (3B).

Question 9: Which is your preferred option for the powers and processes for enforcement officers after an ADS is disabled? Why is this your preferred option?

4 Overview of enforcement needs and access to automated vehicle data

Key points

- Enforcement officers will need to access data to respond to automated vehicle road safety risks.
- Enforcement officers may need additional powers to access automated vehicle data.
- There is a desire for access to automated vehicle data in real time, or shortly following a crash or a road rule infringement.

This chapter considers relevant data needs and provides an overview of some of the issues around enforcement access to automated vehicle data. Chapters 5 and 6 then address specific issues in detail, such as data access at the roadside, additional data availability, access and admissibility considerations.

4.1 Data needs to respond to automated vehicle road safety risks

When automated vehicles begin operating on Australian roads, enforcement officers will need to access data to respond to automated vehicle road safety risks. This includes accessing data for crash investigations and reporting, and in relation to road rule infringements.

Automated vehicles introduce a range of enforcement data needs that are not relevant for conventional vehicles. Police stakeholders outlined that enforcement officers will need to collect and access a range of data to determine key safety information such as:

- whether a vehicle is an automated vehicle
- whether the ADS is engaged and the level of automation at which the ADS is engaged
- transition demands or prompts to human users
- when takeover occurred between the ADS and the human driver
- relevant data following a crash
- for level 3 vehicles, whether the person is a driver or fallback-ready user at a point in time and whether the fallback-ready user took back control within a reasonable time.

This data can broadly be described as ADS operational data; however, it is important to note that these are desired ADS data, which are different from what is contained in the draft ADR 90/01 discussed in chapter 5.

Other relevant data includes data from in-vehicle cameras to determine, for example, whether the fallback-ready user should have taken over control of the driving task. This is distinct from ADS operational data.

4.2 Enforcement access to data – overview

The QUT report provides a summary of currently available enforcement powers relevant to accessing automated vehicle data:

- There are no direct powers in state and territory law concerning access to ADS data. When considering whether there are indirect powers to access ADS data, the location of the possible data is significant (QUT, 2021, pp. 33-34).
- For operational data that is stored onboard the automated vehicle, powers to gather information from vehicles may be sufficient, whereas a power to access premises to obtain vehicle-related data would be relevant in the case where vehicle data is transmitted and stored in an ADSE repository.
- State and territory powers for accessing ADS operational data are fragmented (QUT, 2021, p. 38).
- Powers relating to serious criminal investigations are likely broad enough to cover the access and copying of ADS data from an automated vehicle or a repository at an ADSE's premises. However, these powers do not relate to road safety and road traffic laws.
- For road safety and road traffic laws, powers in Queensland and South Australia may allow accessing ADS data for both light and heavy vehicles, and from both the ADS directly and repositories at ADSE premises. However, in other states and territories these powers are more defined (although more powers may be available for heavy vehicles than for light vehicles).

Stakeholder feedback reveals a strong desire for timely and unconstrained access to automated vehicle data. A range of data is desired by enforcement – for example:

- data relating to an automated vehicle involved in a crash
- surveillance or in-vehicle camera data collected by the automated vehicle
- verbal information from the fallback-ready user (in a level 3 automated vehicle) or the passengers (for level 4 and level 5 automation)
- using data from the in-vehicle cameras. We also briefly discuss visual indicators as they relate to giving enforcement officers information about the engagement status of the ADS.

There was a strong desire for data collection to happen as quickly as possible after an incident. This includes officers being able to determine whether the ADS or a human driver was in control at the time of the incident and to be able to have this information on hand as a crash report is compiled, not after the report has been issued. These practical issues, and their relationship to currently available powers of enforcement, are considered in chapters 5 and 6.

Question 10: Is there additional automated vehicle data that law enforcement officers need in order to respond to the road safety risks of automated vehicles?

Question 11: What is your view on whether the law should explicitly state a time limit on providing enforcement with access to automated vehicle data?

5 Access to data at the roadside and more broadly

Key points

- Several mechanisms for accessing data at the roadside and more broadly are being considered.
- Currently, there are no clear powers that are relevant for enforcement officers to access ADS operational data at the roadside.
- Powers for enforcement officers to collect and access data from the in-service regulator and other agencies may be more consistent with current information sharing arrangements between government agencies.

5.1 Practical considerations for accessing data at the roadside

Broadly, this chapter considers issues relating to availability and accessibility of ADS operational data at the roadside.

Stakeholders have noted that the key issues from a practical perspective are the format of the ADS operational data, and how enforcement officers can download and analyse the data.

Some more specific issues are:

- the need for information to be available in real time following a crash or infringement so enforcement officers can make an assessment at the scene
- automated vehicles having a standardised port that enforcement officers can plug into to access data
- the availability of equipment to download relevant data at the roadside
- issues around connectivity to access cloud data, particularly in rural areas
- the ability for enforcement officers to access data from event data recorders in a wider range of circumstances than what is allowed for conventional vehicles.

5.1.1 ADSEs are considering how they can provide data at the roadside

Potential ADSEs are thinking about how they may provide ADS operational data to enforcement officers at the roadside.

One potential ADSE noted that enforcement officers can call a remote operator centre when seeking to access data at the roadside. This potential ADSE would store data in the ‘cloud’ rather than in the vehicle, but there is a built-in ability to interact with third-party systems – so where the ADSE needs to share data with enforcement officers in a live format, that may be possible.

Several potential ADSEs explained that the location for storing data would most likely differ between fleet-managed and privately owned vehicles. For fleet-managed vehicles, it is unlikely that data would be stored in the vehicle (because ADSEs have an interest in drawing insights from the data collected). Data (including specific data from an event or collision) could be offloaded and pooled at 'terminals', and enforcement officers could contact the ADSE to get the data they need. Data storage in the vehicle is more likely for privately owned vehicles. There could be a port inside the vehicle that would allow enforcement officers access to standardised data.

An industry group suggested that manufacturers will generally store data in the vehicle.

5.1.2 Existing and proposed mechanisms for accessing data at the roadside

Requirements in ADR 90/01

The current version of ADR 90/01 requires the ADSE to implement a process to provide enforcement personnel and agencies with immediate access to certain types of recorded data, where those personnel or agencies are authorised to request it, which covers:

- ADS software versions
- ADS engagement and level of automation history
- self-check history
- requests to intervene history
- Data Storage System for Automated Driving history
- the identity of the vehicle.[34]

We include all of these when we reference data for the purposes of this discussion.

The current ADR 90/01 also provides that '[a]uthorised access to recorded data must be available at the roadside' and '[t]he ADSE must support authorised access to recorded data either digitally, through the vehicle [human machine interface], or via immediate contact with the ADSE'.[35] This appears to correspond with the methods potential ADSEs are considering (from the vehicle, from the 'cloud', by contacting the ADSE at the roadside) as discussed in section 5.1.

Corporate obligations

As well as meeting the requirements in ADR 90/01, at first supply ADSEs must also show how they can meet an ongoing data recording and sharing capability corporate obligation (National Transport Commission, 2022, pp. 23-24).

The obligation covers several factors, but the following are particularly relevant:

- relevant parties (including police) receive information about the level of automation engaged at a point in time if required
- data is provided in a standardised, readable and accessible format when relevant
- data relevant to the enforcement of road traffic laws and the general safe operation of the ADS (including data relevant to crashes) is stored in Australia.

[34] Vehicle Standard (Australian Design Rule 90/01 – Steering System) 2021, Appendix B, section 3.2.34.

[35] Ibid., section 3.2.35.

Law enforcement interaction protocol

The requirement for ADSEs to develop and maintain a LEIP (discussed in section 2.1.2) is relevant to accessing data at the roadside. As previously noted, the protocols could cover how officers can access ADS data (such as the level of automation engaged) at the roadside or during an investigation.

Data Storage System for Automated Driving

The DSSAD records and stores vehicle data to track significant interactions between the driver and the ADS to identify who or what was controlling the vehicle at a given time or whether the driver was requested to take over the control of the vehicle.

WP.29[36] is developing international requirements for the DSSAD for an ADS. Requirements for a DSSAD are already included as part of UN Regulation No 157, which relates to automated lane-keeping systems.[37] Some of the requirements in the DSSAD part of the regulation are that:

- each vehicle equipped with an automated lane-keeping system must be fitted with a DSSAD (clause 8.1)
- each vehicle fitted with a DSSAD must at least record an entry for (among other matters):
  - system activation
  - system deactivation due to various factors
  - transition demand by the system due to various factors
  - start and end of emergency manoeuvres
  - event data recorders
  - trigger input
  - collisions
  - severe automated lane-keeping systems and vehicle failures
  - minimum risk manoeuvre engagement by the system (clause 8.2.1)
- each entry must include a range of data elements such as reason for occurrence and timestamp (clause 8.3.1)
- DSSAD data must be available subject to requirements of national law (clause 8.4.1)
- data stored in the DSSAD shall be easily readable in a standardised way via the use of an electronic communication interface, at least through the standard interface (OBD port) (clause 8.4.4)
- the manufacturer must provide instructions on how to access the data (clause 8.4.5).

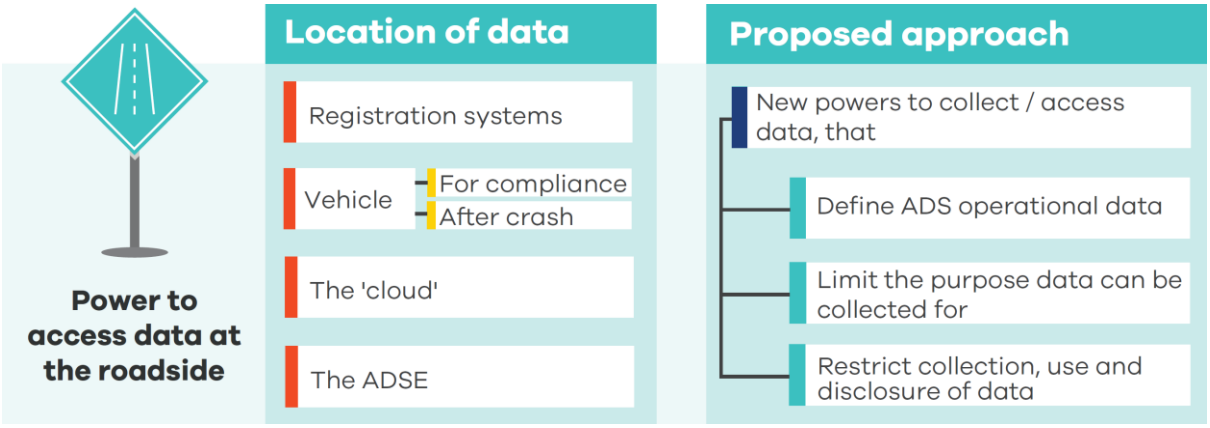
[36] WP.29 is the World Forum for the Harmonization of Vehicle Regulations, a permanent working party of the United Nations. A paper provided to a recent meeting of the EDR/DSSAD subgroup on DSSAD outlines recommendations from various countries about the proposed way forward for DSSAD.

[37] See: UNECE (4 March 2021), *UN Regulation No. 157 – Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems*. The official text is contained in ECE/TRANS/WP.29/2020/81, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/087/82/PDF/G2008782.pdf?OpenElement.

The DSSAD requirements for an automated lane-keeping system provide some insights into how the DSSAD for ADSs more broadly may be developed.

5.2 Powers to access data at the roadside

Figure 4. Power to access data at the roadside



5.2.1 Power to access data from registration systems

Enforcement officers currently have powers to access state and territory registration system data. They access registration data to obtain information about the registered owner (such as their licence number and licence conditions via automatic number-plate recognition as mentioned in 1.4.1) and about the vehicle (such as whether it is registered, written off, and so on).

Taking NSW legislation as an example, there are several provisions that, when read together, provide NSW Police with the power to access registration system data. These are:

- Road Transport Act, s 64, which prohibits release of registration system data unless another law allows release
- Road Transport (Vehicle Registration) Regulation 2017 (NSW), cl 134, which allows release of registration system data in circumstances when the release would be allowed under NSW privacy laws
- *Privacy and Personal Information Protection Act 1998* (NSW), s 23, which allows disclosure of personal information (registration system data is personal information) for a law enforcement purpose.

Some limited ADS operational data (such as whether the vehicle is an automated vehicle) may be available through state and territory registration systems in the future. Work by Austroads, mentioned in 1.3.2, looked at data requirements for automated and electric vehicle registration and noted that to support the registration of automated and electric vehicles, changes may be required to jurisdictional registration systems. The project recommended ‘a small additional data set for automated and electric vehicles and draft data definitions for further development’.

5.2.2 Power to access data from the vehicle

ADS operational data may be stored onboard the automated vehicle and possibly accessed through powers authorising the gathering of information from vehicles (QUT, 2021, p. 34).

Powers to inspect and take evidence from a vehicle in the context of general law enforcement and criminal investigations are generally not relevant to support roadside enforcement for automated vehicles because road rule and traffic law offences are generally too minor to require the police to exercise these powers (QUT, 2021, pp. 34-35).

Power to access data for compliance purposes

Powers to access data from the vehicle for road traffic and vehicle compliance are more limited. Powers in Queensland and South Australian legislation may be broad enough to allow access to ADS operational data for road safety and vehicle compliance;[38] however, it is unclear whether these powers extend to data held within an ADS. Other states and territories have more limited powers (QUT, 2021, pp. 35-36).

There is possibly greater adaptability of existing powers to access ADS data in relation to heavy vehicles, such as:

- Victoria's Road Safety Act, *1986* ss 114(2)(ii) and 115(3)(d)), which allow police or authorised officers to copy documents relating to the vehicle or its use accessible from electronic equipment in the vehicle.
- The NSW Road Transport *Act 2013* Part 6.1, which allows for the seizure of monitoring devices and records fitted in a vehicle.

However, the adaptability of these provisions to access ADS operational data is still unclear. For example, s 155 of the New South Wales Act allows police officers to take and retain automatic data stored in a device fitted in the vehicle for specific purposes only, such as where a person is killed in an accident, or the driver has committed a major offence. This would not be broad enough to capture data following a road traffic law breach.

Overall, the QUT report noted that state and territory powers for accessing ADS operational data for road and vehicle law compliance are not uniform and are particularly limited in states and territories other than Queensland and South Australia (QUT, 2021, p. 38).

The HVNL provides some additional powers to access data from vehicles. It allows authorised officers to enter heavy vehicles for monitoring and investigation purposes, and to access and copy digital data.[39] While these could potentially allow for the collection of ADS operational data, they are powers to monitor or investigate whether an occasion has arisen for to exercise powers under the HVNL rather than to access data from heavy vehicles more broadly.

The QUT report also noted that surveillance device laws may have some applicability to collecting ADS operational data from the vehicle; however, there are several limitations, particularly that the 'powers are contingent on the use of surveillance devices for the purposes of their respective Acts, and then usually only under a warrant or emergency authorisation' (QUT, 2021, pp. 40-41).

[38] See, for example, *Police Powers and Responsibilities Act 2000* (Qld), ss. 54 and 64(2)€; *Road Traffic Act 1961* (SA), ss. 40Q, 40R and 41E.

[39] Heavy Vehicle National Law, ss 520, 521.

Power to access data following a crash

Some (but not all) states and territories have additional powers to access data in relation to vehicle crash investigations that may allow access to ADS operational data from the vehicle, with powers in Queensland and South Australia the most flexible (QUT, 2021, pp. 38-39).

For example:

- Queensland's Police Powers and Responsibilities Act, s 56(1) allows police officers 'to obtain information about the cause of a relevant vehicle incident and the circumstances in which it happened' (relevant vehicle incidents include road incidents involving vehicles causing personal or property damage)
- NSW's Law Enforcement (Powers and Responsibilities) Act, ss 90 and 95 provide relatively extensive investigatory powers where a crash has resulted in death or serious injury.

5.2.3 Power to access data from the 'cloud'

Industry stakeholders, particularly potential ADSEs focusing on a fleet ownership model, have noted that ADS operational data may be stored on network servers or terminals external to the vehicle, rather than in the vehicle itself. For simplicity, we refer to this type of data storage as 'cloud' storage.

There do not appear to be any specific powers for accessing data from the 'cloud' because access to digital data is generally limited to access from devices within the vehicle or at a premises (rather than data stored on a network in an online environment). Powers to access data from ADSEs are discussed below, in section 5.2.4.

5.2.4 Power to access data by contacting the ADSE at the roadside

Some industry stakeholders, including ADSEs focused on a fleet ownership model, have noted that their business models focus on enforcement officers being able to contact the ADSE's fleet operations or a remote operator centre 24 hours a day, as needed. This includes for purposes such as seeking access to data at the roadside.

Some current powers that could allow enforcement officers to obtain ADS operational data from ADSEs at the roadside include:

- Queensland's Police Powers and Responsibilities Act, s 54: It is lawful for a police officer to make any reasonably necessary inquiry, investigation, inspection, examination, or test for establishing whether or not an offence against the Road Use Management Act or the Heavy Vehicle National Law (Queensland) has been committed.
- *Road Traffic Act 1961* (SA), ss 40W and 40X, which allow an authorised officer, for compliance purposes, to direct a responsible person to provide specific records or information about a vehicle.

These powers do not appear broad enough to allow access specifically to ADS operational data in all circumstances. This is especially the case when there are preconditions to these powers, for example, the need to exercise the power for a compliance purpose.

Some states and territories have additional powers to allow officers to access data from ADSEs that relate to identifying the driver of the vehicle at a point in time. This may be relevant to determining whether the ADS was engaged at the time of a crash, for example. For states and territories that do have this power, there are differences in the officer's ability to identify the driver, with identification more difficult in some states and territories than others.

Additionally, if the ADS was in operation, it cannot be considered the 'driver', as discussed in section 2.1.1 (QUT, 2021, p. 93). For example, the formulation of the power in South Australia could require the ADSE to provide ADS operational data (QUT, 2021, pp. 30-31).[40] However, because these powers are to be exercised on a driver, this power could have limited applicability if the ADS was engaged.

ADSEs focusing on a fleet ownership model are also generally focusing on developing dedicated automated vehicles. Therefore, powers relating to identifying the driver are likely of limited relevance because the ADS will be performing the driving task. Powers relating to identifying the driver may be more relevant to obtaining non-DDT information from vehicle occupants.

Access to ADSE operational data following a crash

As outlined in the section above, some states and territories have additional powers to access data in relation to vehicle crash investigations. Where they exist, those powers would most likely apply to accessing ADS operational data from the ADSE.

Some stakeholders indicated that clear standards need to be in place to enable access to data without enforcement having to go through a third party because this will most likely add a layer to the data gathering process and hinder efficiency.

5.3 Proposed approach to data access at the roadside

Currently, there are no clear powers that are relevant for enforcement officers to access ADS operational data at the roadside. Current powers are fragmented, with some states and territories having powers that are more adaptable to automated vehicles than others. Even in states where powers are the most broad and adaptable, the applicability of these powers to automated vehicles is not clear.

Other than for accessing data from registration systems (which could provide only very limited relevant data), it appears unlikely that enforcement officers can rely on current powers to access ADS operational data at the roadside. For some jurisdictions, the gaps are greater than for others.

[40] *Summary Offences Act 1953* (SA), s 74AB(1): A police officer may ask a person questions for the purpose of obtaining information that may lead to the identification of the person who was driving, or who was the owner of, a vehicle on a particular occasion or at a particular time.

We propose that states and territories include new data collection and access powers that would allow enforcement officers to collect or access ADS operational data at the roadside. This will require:

- A clear definition of what is meant by ADS operational data.
- Purposes for which ADS operational data can be collected by enforcement officers at the roadside, and subsequently used by enforcement officers.
- Restrictions on collection, use and disclosure of ADS operational data by enforcement officers beyond those purposes.

These three points are considered below. We propose that, before introducing any new data collection and use powers for enforcement officers, states and territories complete a privacy impact assessment.

5.3.1 A clear definition of 'ADS operational data'

As part of its first supply requirements, the ADSE needs to certify that it can provide immediate access to certain types of recorded data. The draft requirements are contained in the current public draft of ADR 90/01, discussed in section 5.1.2.

We propose that an approach to defining ADS operational data is to align it with the description of recorded data in ADR 90/01 when that ADR is finalised. That way, the powers to request ADS operational data will align with the types of data ADSEs are required to provide.

5.3.2 Purposes for which ADS operational data can be collected by enforcement officers at the roadside, and subsequently used by enforcement officers

We propose that the purposes could be articulated as follows:

- Enforcement officers can collect ADS operational data at the roadside for the purpose of determining liability for traffic offences and crashes that involve an automated vehicle, and for crash investigation and reporting where an automated vehicle is involved. This includes, but is not limited to, ADS operational data that may show:
  - whether the automated driving system or the fall-back ready user was controlling the vehicle at a given point in time
  - the level of automation engaged
  - any transition requests or prompts to the human user
  - factors causing or contributing to a breach of a road traffic law or crash.

We note that these are proposed powers to collect and use available data and not requirements that the ADSE make the data available and accessible (these are contained in the ADSE's first supply requirements).

5.3.3 Restrictions on collection, use and disclosure of ADS operational data by enforcement officers beyond those purposes

Previous NTC work that considered regulating government access to automated vehicle data noted that automated vehicle data could reveal personal information. Design principles developed as part of this work provided that laws relating to automated vehicles should: [41]

- 'align government entities' approach to managing … automated vehicle data with the objectives underlying personal information'
- 'embed access powers and privacy protections for … automated vehicle data in legislation'
- 'specify the … automated vehicle data covered, the purposes for which the data can be used and the parties to whom the purpose limitations apply while not impeding access to data with a warrant or court order authorising a different use' (National Transport Commission, 2019, pp. 5-6).

Noting these design principles, we propose that the collection and use of ADS operational data by enforcement officers be restricted to specific purposes (as discussed in section 5.3.2), unless the data can be accessed under other existing processes (such as access to data with a warrant or court order authorising a different use).[42]

The existing and proposed mechanisms described in section 5.1.2 cover a broad range of issues relevant to availability and accessibility of ADS operational data at the roadside. The requirements in the current version of ADR 90/01 outline relevant ADS operational data and methods for enforcement officers to access this data at the roadside. ADR 90/01 also specifically refers to the Data Storage System for Automated Driving (DSSAD) history as a relevant type of recorded data and would encompass the international DSSAD developments as they develop. The DSSAD requirements for an ADS may be relatively prescriptive and all-encompassing.

Generating very specific Australian requirements could limit the market access for automated vehicles. The existing and agreed mechanisms to access data offer a middle ground between developing Australia-specific requirements and waiting for international decisions on this topic.

---

[41] In 2019, we developed a set of design principles for managing government access to automated vehicle data that would guide further work by the NTC. These design principles were noted by transport ministers. These are contained in the Appendix.

[42] One example that may be relevant in considering use and disclosure restrictions is restrictions on releasing registration information: *Road Transport Act 2013*, s 64(3) – Transport for NSW must ensure that information in the NSW registrable vehicles register that is of a personal nature or that has commercial sensitivity for the person about whom it is kept is not released except as provided by the statutory rules or under another law.

A more recent example (although not in the transport context) is Part 8A of the *Public Health and Wellbeing Act 2008* (Vic). By way of summary, it provides that authorised officers will have specific powers relating to core compliance and enforcement enabling them to require information or documents, inspect premises, and so on.

The laws will enshrine a person's right to privacy, with an offence to use information obtained through contact tracing for non-public health purposes.

Australian governments should continue to monitor international developments and review if international consensus on ADS data arises. This is an interim option, and governments should commit to a clear point for review should international consensus emerge. It would ensure Australia keeps in step with international consensus or standards around accessing ADS data at the roadside. This would include developments relevant to the Data Storage System for Automated Driving.

Such an approach would ensure we are considering options which are both Australia-specific and internationally aligned. In the meantime, issues relating to availability and accessibility of ADS operational data at the roadside would be covered by the requirements in ADR 90/01 and the ongoing data recording and sharing obligations discussed above.

Government and industry integration

Law enforcement authorities should continue to build relationships with strategic automated vehicle industry partners active in developing and implementing automated vehicle infrastructure technologies in Australia. Establishing collaborative relationships with ADSEs, manufacturers and research organisations will allow authorities to gain a more precise vision of future automated vehicle capability and law enforcement interaction requirements. Law enforcement agencies may see benefit in greater integration with the vehicle sector and working directly with industry partners to evaluate the emergence of the technology's capability to interact with law enforcement. Expertise on emerging automated vehicle technologies embedded within a law enforcement agency could support development of systems and processes for interacting with automated vehicles.

Question 12: What new powers would be required for enforcement officers to access ADS operational data at the roadside?

Question 13: Do you agree that there could be greater integration between government and industry as expertise on the emerging technology develops? How practical is this?

Question 14: How could industry grow and develop relationships with government and law enforcement agencies?

5.4 Access to data other than at the roadside

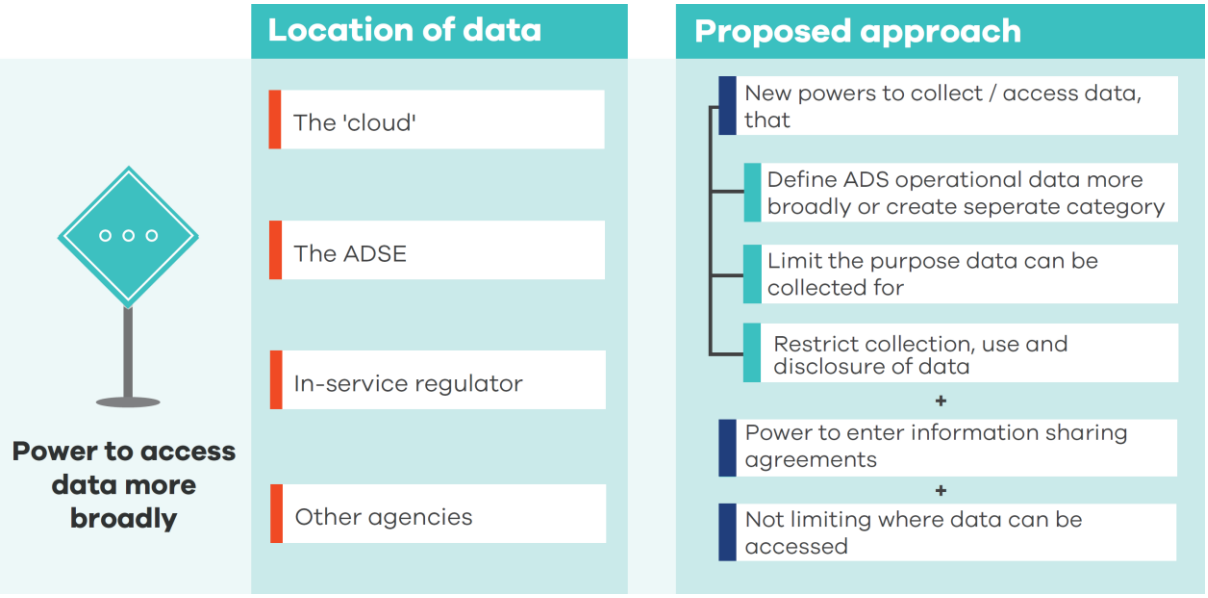
There may be circumstances where accessing certain ADS operational data at the roadside is not possible or necessary. For this reason, it is relevant to consider accessing data more broadly.

This section assesses whether enforcement officers have powers to access ADS operational data more broadly under current state and territory laws and proposes an approach to address identified gaps. We also consider some practical issues relating to access to data, other than at the roadside.

The issues and gaps are similar to those we identified in the powers for accessing ADS operational data at the roadside. That is, there are no clear current powers that are potentially relevant for enforcement officers to access ADS operational data more broadly.

It therefore appears unlikely that enforcement officers can rely on current powers to access ADS operational data more broadly. Potentially relevant data sources are considered individually, and an approach to address gaps is discussed once all data sources are considered and the issues and gaps identified.

Figure 5. Power to access data more broadly



5.4.1 Power to access data other than at the roadside – from the 'cloud'

As noted in section 5.2.3, there do not appear to be any specific powers for accessing data from the 'cloud' because access to digital data is generally limited to access from devices within the vehicle or at a premises (rather than data stored on a network in an online environment).

5.4.2 Power to access data other than at the roadside – from ADSEs

The powers discussed in section 5.2.4 relating to enforcement officers accessing ADS operational data by contacting the ADSE at the roadside would also apply to accessing data from ADSEs more broadly. However, there are additional potentially relevant data access powers for enforcement officers that can broadly be described as accessing data from premises.

Examples of powers that may allow enforcement officers to access ADS operational data located at an ADSE's premises are:

- Queensland's Police Powers and Responsibilities Act, s 57, which allows a police officer to enter a place and stay at a place for the time reasonably necessary for the purpose of exercising other data collection powers
- SA's Road Safety Act, ss 40S, 40T and 41E, which allow enforcement officers to inspect and search premises, and provide authority to seize digital devices or copy digital information. The QUT report notes that 'these provisions seem reasonably adapted to accessing ADS data, provided that the purpose is in relation to compliance or investigation of breaches of Australian road laws' (p. 36).

Powers to access data from premises have similar limitations for enforcement officers as powers for collecting data from the vehicle (discussed in section 5.2.2). The powers are fragmented and not uniform across states and territories, and collection for road safety and road traffic law purposes is quite circumscribed in most states and territories.

The HVNL provides some additional powers to access data from premises. It allows authorised officers to enter premises for monitoring and investigation purposes, and to access and copy digital data.[43] While these could potentially allow for the collection of ADS operational data, they are powers to monitor or investigate whether an occasion has arisen for to exercise powers under the HVNL rather than to access data from premises more broadly.

Following a crash

As discussed in section 5.2.4, some states and territories have additional powers to access data in relation to vehicle crash investigations. Some of these powers also include a power to enter premises. For example, Queensland's Police Powers and Responsibilities Act, s 57 (discussed in section 5.2.2) also applies to accessing crash data.

5.4.3 Power to access data other than at the roadside – from the in-service regulator

Under the proposed new Automated Vehicle Safety Law, the in-service regulator has information access, collection and sharing powers. While the detail of these has not yet finalised, it is likely that the in-service regulator's information sharing powers could extend to enforcement officers.

An example of an information sharing power from a regulator to police is in the HVNL (s 686B): The Regulator may give information included in the database of vehicles to:

a. a registration authority for a participating jurisdiction or another Australian jurisdiction; or
b. a police force or police service for a participating jurisdiction or another Australian jurisdiction.

The types of information that enforcement officers may want to receive from the in-service regulator include:

- who the ADSE for the automated vehicle is (acknowledging this may be less relevant if not received at the roadside)
- whether the ADSE responsible for the ADS has left the market (and therefore, the ADS should not be operating)
- whether the in-service regulator has suspended an ADS fleet (and therefore, the ADS should not be operating).

Compared with ADSEs, it is unlikely that the in-service regulator will store much relevant ADS operation data to share with enforcement officers. The ADSE will have the operational data rather than the ISR; the ISR will only have operational data if provided by the ADSE (for example, if the ISR is investigating an ADSE incident).

There are no existing powers for police to access ADS operational data or other information from the in-service regulator.

[43] Heavy Vehicle National Law, ss 495, 496, 497, 500.

5.4.4 Power to access data other than at the roadside – from other agencies

Enforcement officers may seek ADS operational data from other agencies such as other police agencies and transport agencies.

There is no uniform approach under state and territory laws for sharing vehicle data with other enforcement and regulatory agencies (QUT, 2021, p. 42). There are provisions in South Australia, Queensland, Western Australia and Victoria that allow disclosure of information gathered under transport laws with corresponding authorities.

The South Australian disclosure powers may be the most relevant:

- Road Traffic Act, s 41L: Any records, devices or other things seized under this Act, or any information obtained under this Act, may, for the purposes of law enforcement, be given to any public authority of any jurisdiction (including any corresponding Authority) considered appropriate by the Minister or the Commissioner of Police, but only after consultation with the public authority concerned.

Some state and territory laws also contain provisions that facilitate information sharing between transport agencies and police. For example:

- Queensland's Transport Operations (Road Use Management) Act, s 17E allows the chief executive (of the Department of Transport and Main Roads) to enter into a written arrangement about giving and receiving information with the police commissioner, including the electronic transfer of information daily.

Powers to share vehicle data between agencies is a patchwork of provisions across the states and territories, and it is not clear that existing provisions would allow enforcement officers to access ADS operational data or other relevant information from other agencies.

5.4.5 Practical matters relating to accessing data more broadly

In relation to accessing ADS operational data from ADSEs, the issues and mechanisms for addressing those issues discussed in the roadside sections of this chapter would also apply here. These issues include the need for information to be available in real time, standardising ports from which officers can access data and connectivity to the cloud.

We consider that enforcement officers could also receive data and information from the in-service regulator and potentially other agencies. Enforcement officers would most likely receive data or information other than ADS operational data from these agencies. For example, the types of information that enforcement officers may want to receive from the in-service regulator include:

- who the ADSE for the automated vehicle is (acknowledging this may be less relevant if not received at the roadside)
- whether the ADSE responsible for the ADS has left the market (and therefore, the ADS should not be operating)
- whether the in-service regulator has suspended an ADS fleet (and therefore, the ADS should not be operating).

There do not appear to be any practical issues with accessing available data from the in-service regulator and other agencies.

5.5 Proposed approach to data access other than at the roadside

In section 5.3, we proposed an approach for data collection and access powers that would allow enforcement officers to collect or access ADS operational data at the roadside. We consider that approach is also relevant to accessing ADS operational data more broadly, with reference to the following considerations:

- For access to ADS operational data more broadly, the suggested approach to align ADS operational data with the description of recorded data in ADR 90/01 when that ADR is finalised may be insufficient or incomplete, particularly because there are parties other than ADSEs that enforcement officers may seek data from. For example, useful data may relate to whether an ADSE has left the market or whether an ADS fleet has been suspended. It may therefore be relevant to:
  - include a more expansive definition of ADS operational data, or
  - include a separate category of automated vehicle data.

  The latter option may allow for a clearer split between accessing data at the roadside or from the ADSE and accessing data from other parties.
- Powers for enforcement officers to collect and access data from the in-service regulator and other agencies could be considered as part of information sharing arrangements (that is, through new powers to enter into information sharing arrangements rather than new specific collection and access powers). This may provide greater flexibility and be more consistent with current information sharing arrangements between government agencies. However, these information sharing arrangements should still be subject to the purpose restrictions (consistent with those outlined in sections 5.3.2 and 5.3.3, adding in any broader purposes as discussed directly above).
- To remove doubt, it may be useful to note that enforcement officers can access ADS operational data from the in-service regulator, other enforcement agencies and ADSEs, but ensure that this is not considered an exhaustive list.

Question 15: What new powers do enforcement officers need to access ADS or other automated vehicles' operational data more broadly than at the roadside?

Question 16: Could aligning ADS operational data with the description of recorded data in a (finalised) ADR 90/01 cause any issues?

Question 17: Will enforcement officers have sufficient powers to investigate crashes involving automated vehicles?

6 Additional data availability and access considerations

Key points

- There are extra sources of information in automated vehicles that help law enforcement officers interact with them and investigate potential safety violations. These include visual indicators and in-vehicle cameras.
- The collection of data by law enforcement should be limited in scope and clear on the purpose for which that data is being used.
- The key data retention issues relate to ensuring data is retained in challenging circumstances and for a reasonable period of time.

This section discusses data availability and access matters relating to additional sources of information including vehicle-mounted visual indicators and in-vehicle cameras, as well as how enforcement officers could obtain information from vehicle occupants. We also review issues relating to data retention and admissibility.

6.1 Visual indicators

Police stakeholders have noted the potential benefits of external visual indicators on an automated vehicle, particularly to show who is in control and the level of automation engaged. Some police stakeholders noted that this would alleviate many issues relating to driver and ADS responsibility when conducting roadside enforcement and traffic camera enquiries.

6.1.1 Industry's approach to visual indicators

Potential ADSEs have varying positions regarding the use of visual indicators on their vehicles. These vary from easy to identify vehicle indicators being included in the design to an explicit reluctance to place a visual identifier on vehicles.

- Waymo explains that its automated vehicles can be easily identified by Waymo logos and are always fully automated – they will not have any person in the driver's seat either steering or otherwise controlling the vehicle (Waymo, 2021).
- One potential ADSE noted that there are currently visual indicators on its vehicles (a light that changes colour and blinks) to show whether it is in automated mode.
- Another potential ADSE explained that its research and testing suggests there are potential concerns with using visual indicators – not only can they be a distraction to human drivers, but human drivers may also change their behaviour around an automated vehicle. For example, an automated vehicle may come across as a cautious driver, which could infuriate some road users, and permanently displaying the status of the vehicle is problematic from that perspective.

The Automated Vehicle Safety Consortium's best practice guidance for first responder interactions also provides recommendations around identifying an ADS-DV, recommending that ADSEs should document in interaction plans a description of features and contextual cues that would help distinguish an ADS-DV from a conventional vehicle (Automated Vehicle Safety Consortium, 2020).

6.1.2 Visual indicators as a requirement in Australia and abroad

Draft ADR 90/01 does not include requirements for visual indicators. Without requirements for including visual indicators, it would be up to each individual ADSE to decide whether to include them.

Internationally, the question around external optical signals indicating whether the ADS is engaged is an open one and it is unclear whether such requirements will be introduced. WP 1 is considering the issue of optical and audible signals from the perspective of other road users, rather than enforcement officers (for example, signalling the vehicle's intent). While no resolution has been reached, discussions and proposals have noted potential safety risks to other road users, such as distraction, of automated vehicles using optical and audible signals to indicate their automation status. An informal paper submitted by Germany at a recent WP 1 meeting noted that such signals should not be used as a general rule, but only in very specific scenarios as a temporary solution (Global Forum for Road Traffic Safety 2021)

In addition, other data sources previously discussed in this paper may be more reliable for enforcement purposes. For example, data from a vehicle about the level of automation engaged leading up to a crash is probably more reliable and perhaps more useful than an enforcement officer observing a visual indicator at just the right time before a crash.

6.1.3 Proposed approach to visual indicators

Introducing Australia-specific design requirements could act as a barrier for automated vehicles entering the Australian market, especially because Australia is a technology taker. While the draft ADR 90/01 does contain some Australia-specific design requirements (such as compliance with Australian road rules and verifying for the Australian road environment), these requirements are generally safety critical.

We also acknowledge the mixed safety outcomes from research cited above and, noting this, we propose that we continue to monitor international developments and introduce requirements for visual indicators if they are agreed international automated vehicle standards (or, at the very least, there is a level of international consensus about the need for visual indicators). This would ensure we are internationally aligned and could occur through the more standard ADR development process.

6.1.4 Questions

Question 18: What are your thoughts on the proposed approach to visual indicators on automated vehicles?

Question 19: What other relevant international or technological developments relating to visual indicators on automated vehicles are you aware of?

6.2 Access to data from in-vehicle cameras

Police stakeholders indicated that there was a potential need for cameras to be included in automated vehicles to assist with determining whether the fallback-ready user should have taken over control or is meeting its obligations when the ADS is engaged. Police stakeholders noted that because fallback-ready users will have obligations at the same time as an ADSE, police need this information at the roadside.

Practical issues of accessing the data from in-vehicle cameras includes:

- whether automated vehicles will have in-vehicle cameras, and whether relevant data from these cameras will be available for enforcement officers to collect
- if the cameras are available, the period they will record for
- how enforcement officers can access data from in-vehicle cameras at the roadside.

6.2.1 In-vehicle camera prevalence in automated vehicles

In previous work we completed, stakeholders informed us that automated vehicles are likely to rely on inward-facing cameras to monitor human driver alertness and behaviour (National Transport Commission, 2019, p. 25). A potential ADSE we consulted with noted that certain countries have suggested that some level of video recording should be included in the Data Storage System for Automated Driving requirements.

We received some more general feedback that even if in-vehicle cameras are incorporated, it is possible that they will only record for short periods of trips (for example, the last three minutes of a journey on a rolling basis).

6.2.2 Powers to access data from in-vehicle cameras

Enforcement powers for accessing data from the vehicle may potentially also apply to accessing data from in-vehicle cameras. Even if these powers do apply to in-vehicle cameras, noting the issues and gaps discussed in section 5.2.2, particularly fragmentation and lack of uniformity, there are still likely to be gaps in these powers for accessing data from in-vehicle cameras. We are not aware of any other powers for accessing data from in-vehicle cameras.

In previous work NTC has completed, we explained in detail how data from in-vehicle cameras could be both personal and sensitive information (National Transport Commission, 2019, Chapter 4). The principles relating to purpose and restrictions outlined in sections 5.3.2 and 5.3.3 would therefore also apply to data from in-vehicle cameras. However, the purposes themselves should be much narrower because, for automated vehicle-specific roadside enforcement purposes, the data is relevant only in relation to enforcing fallback-ready user obligations.

Whether or not there is a gap in collection powers also depends on whether relevant data from in-vehicle cameras will be available for enforcement officers to collect. We will consider this further in a subsequent paper. For the purposes of the current discussion, we will proceed on the basis that relevant data from in-vehicle cameras may be available.

Noting the likely gaps in current enforcement powers to access data from in-vehicle cameras, it may be relevant to include new powers for enforcement officers to access this data. We note that these would be powers to access available data, rather than requirements that such data be available.

6.2.3 Proposed approach to accessing data from in-vehicle cameras

We note that there are no specific requirements in the current ADR 90/01 for automated vehicles to have in-vehicle cameras. ADR 90/01 has broad requirements for the ADS to monitor the 'Operator' (which includes the fallback-ready user), for example:

- The ADS must incorporate a system that detects whether the Operator is available to conduct the dynamic driving task.[44] Criteria for determining Operator availability include eye blinking, eye closure, conscious head or body movement.[45]
- The ADS must also detect if the Operator is attentive, which includes consideration of the Operator's gaze direction and head movement.[46]

Such monitoring could be done through in-vehicle cameras but could probably be achieved through other means such as relevant sensors. Even if the monitoring is achieved through cameras, ADR 90/01 does not require the ADS to record any of its monitoring activities.

We propose that the overall approach to articulating such a power could be as follows:

- Enforcement officers can collect data from in-vehicle cameras for the purpose of enforcing fallback-ready user obligations including, but not limited to, determining whether:
  - the person is a driver or fallback-ready user at a point in time
  - the fallback-ready user took back control within a reasonable time.
- Collection and use of data from in-vehicle cameras by enforcement officers should be restricted to these specific purposes unless the data can be accessed under other existing processes (such as access to data with a warrant or court order authorising a different use).
- We continue to monitor international developments and include specific requirements for in-vehicle cameras only if these are agreed internationally. Such an approach would ensure we are internationally aligned and would most likely occur through the more standard ADR development process.

We consider that, before introducing any new data collection and use powers for enforcement officers, states and territories should complete a privacy impact assessment.

Question 20: Do you agree with the proposed approach to enforcement officers having the practical ability to access data from in-vehicle cameras?

[44] Vehicle Standard (Australian Design Rule 90/01 – Steering System) 2021, Appendix B, clause 3.3.51.

[45] Ibid., clause 3.3.53.

[46] Ibid., clause 3.3.54.

6.3 Obtaining information from vehicle occupants

Enforcement officers may be able to obtain relevant information from vehicle occupants including information about who was in control of the vehicle at a particular point in time. Enforcement officers could obtain this information at the roadside.

This section assesses whether enforcement officers have powers to access data from vehicle occupants under current state and territory laws.

6.3.1 Existing powers to obtain information from vehicle occupants

There are some existing powers for enforcement officers to obtain relevant information from vehicle occupants. The most relevant powers appear to be those directed towards determining the identity of drivers (as this is linked to who was in control of a vehicle at a particular point in time).

These include:

- SA's Summary Offences Act, s 74AB[47]
- NSW's Law Enforcement (Powers and Responsibilities) Act, s 14[48]
- WA's Road Traffic Administration Act, s 34.[49]

The QUT report notes that Victoria and the ACT do not seem to have specific roadside enforcement powers directed at determining the identity of drivers (QUT, 2021, p. 33).

Unlike in conventional vehicles, there is potential for the only occupants of an automated vehicle to be people with a disability that prevents them from giving admissible evidence or they may be children who are unable to give admissible evidence as well.

Powers to obtain relevant information from vehicle occupants is somewhat limited, particularly in some jurisdictions. In addition, even if relevant information is obtained, there may be restrictions on whether it can be used as evidence. However, this may not in and of itself create an issue or gap because it may not actually be essential for enforcement officers to obtain information from vehicle occupants. Police stakeholders suggested that witness evidence (for example, the driver saying that they were not in control of the vehicle when it went through a red light) could easily be fabricated without other evidence to support it.

---

[47] *Summary Offences Act 1953* (SA), s 74AB: A police officer may ask a person questions for the purpose of obtaining information that may lead to the identification of the person who was driving, or was the owner of, a vehicle on a particular occasion or at a particular time. The QUT report (pp. 30-31) notes that this South Australian power is the most adaptable formulation and is particularly expansive as it is not limited to drivers, owners or passengers, or by suspicion of an alleged offence.

[48] *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW), s 14, which provides that a police officer can require drivers, passengers and owners to disclose the identity of drivers and passengers. This power is, however, limited by requiring a connection to an indictable offence, and so is not broadly applicable to offences under road safety and traffic laws (which are not usually indictable) (QUT, 2021, p. 31).

[49] *Road Traffic Administration Act 2008* (WA), s 34, which provides that a police officer can ask a responsible person for information that may lead to the identification of the driver or person in charge of the vehicle at the time of an alleged offence. This power is, however, limited by the definition of a responsible person, which means a person to whom possession or control of the vehicle was entrusted at the time of the alleged offence. The QUT report (p. 31) suggests this could include occupants of an automated vehicle (as arguably having possession of the vehicle).

Where appropriate, existing powers to obtain information from vehicle occupants could complement other data collection and access powers of enforcement officers, but we do not consider that there is a specific issue or gap with these existing powers that needs to be addressed.

Question 21: Do you agree that existing powers to obtain information from vehicle occupants do not need to be amended to accommodate automated vehicles?

6.4 Data retention

Stakeholders suggested there needs to be a requirement for an ADS to retain data post-crash, as data may be lost or corrupted when the automated vehicle is involved in a crash. Stakeholders also questioned whether data could be retrieved if the vehicle has no power. We also received feedback that the period relevant data is retained for is important because data may need to be used in future prosecutions.

The key data retention issues therefore relate to ensuring data is retained in difficult circumstances and for a reasonable period.

6.4.1 Industry data retention capability

One industry group is considering long retention periods or up to six months as part of their discussion about the Data Storage System for Automated Driving. However, the industry group noted the period of retention may be less for vehicles such as taxis, which would be travelling many more kilometres compared with privately owned vehicles.

6.4.2 Existing and proposed mechanisms to address the issue of data retention

Corporate obligations

The ongoing data recording and sharing capability corporate obligation discussed in section 6.1.2 is also relevant to data retention. It requires the ADSE to explain how it will ensure 'data is retained to the extent necessary to provide it to relevant parties (the amount of time data is retained may depend on the purpose(s) the information could be used for – for example, law enforcement and insurance)'.[50]

[50] National Transport Commission, *The regulatory framework for automated vehicles in Australia*, February 2022, p. 24.

Data Storage System for Automated Driving

UN Regulation No 157 (which includes requirements for a DSSAD for an automated lane-keeping system) covers issues relating to retrieving data post-crash and when the vehicle has no power, and ongoing data availability. It provides that:

- '[t]he data shall be retrievable even after an impact of a severity level set by UN Regulations Nos. 94, 95 or 137. If the main on-board vehicle power supply is not available, it shall still be possible to retrieve all data recorded on the DSSAD, as required by national and regional law'[51]
- '[o]nce the storage limits of the DSSAD are achieved, existing data shall only be overwritten following a first in first out procedure, with the principle of respecting the relevant requirements for data availability. Documented evidence regarding the storage capacity shall be provided by the vehicle manufacturer'.[52]

As noted in section 6.1.3, the DSSAD requirements for automated lane-keeping systems provide some insights into how the DSSAD for ADSs more broadly may be developed.

6.4.3 Proposed approach to data retention

We note that retrieving data post-crash and where the vehicle has no power relate to design requirements and are most likely to be covered off in first-supply requirements. The automated lane-keeping system's DSSAD requirements broadly capture these issues, and similar requirements may be included in DSSAD requirements for ADSs more broadly. Our proposed approach is to continue to monitor international developments and review if international consensus emerges. This is an interim option, and governments should commit to a clear point for review should international consensus emerge. It would ensure Australia keeps in step with international consensus or standards around data retention.

Issues relating to data retention for relevant periods are covered, at a high level, by the ongoing data recording and sharing obligation discussed in section 6.1.2. Feedback from industry indicates there are currently discussions at the international level regarding DSSAD data retention periods. Once these are decided, we propose they could then be included into Australia's regulatory framework. It is relevant to note that the *Privacy Act 1988* (Cwlth) could also affect the amount of time for which an ADSE can retain data.

6.5 Admissibility of data

There may be restrictions on using evidence in a prosecution depending on the type of witness getting interviewed and data admissibility more broadly.

6.5.1 Admissibility of data from vehicle and ADS

Automated vehicles present a new and very fertile ground for authorities to collect information, potentially relating to individual identities and mobility patterns.

[51] UNECE (4 March 2021), *UN Regulation No. 157 – Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems*, clause 8.4.3.

[52] Ibid, clause 8.4.2.

However, the act of collecting and storing this data does not necessarily mean it will be possible to admit this evidence to settle disputes or insurance claims. Powers to access data need to be informed by whether authorities would even be able to admit the data as evidence.

For offences picked up by a traffic camera, there is a question around which data source, the camera or the ADS, can be relied on for prosecution. Similarly, where both sets of evidence are being used, it is unclear how much weight should be given to automated vehicle data, especially in instances where the vehicle evidence and camera or witness testimony may be contradictory. There may be additional challenges with questioning witnesses at the scene, particularly if there is no able driver in the vehicle, if there are no passengers or if the passengers are unable to provide testimony – for example, if they are cognitively impaired. Information provided by vehicle occupant witnesses about who was in control of the vehicle may not necessarily be a useful source of data.

Consideration could also be given to the potential for inequality in dealing with crashes or incidents involving automated vehicles with those involving more conventional vehicles. Australian roads will most likely feature a mixed fleet for some time, consisting of vehicles of markedly different levels of automation. Automated vehicle data may provide an accurate reconstruction of the circumstances of, and reasons for, a crash to clarify liability issues. This cannot be replicated in a conventional vehicle. This may give rise to issues associated with the perception that automated vehicle drivers are being granted financial advantages, while conventional vehicle drivers are unfairly treated.

6.5.2 Certification of people accessing and evaluating data

The task of accessing and assessing automated vehicle data may need to be performed by a suitably qualified and certified person. Stakeholders noted that given the novelty of the technology, there may be difficulties with finding people experienced enough with automated vehicles to access, evaluate or give witness testimony during the prosecution of a case. Even if such experts exist, manufacturers may be reluctant to share how they collect data, and, as discussed previously, reluctant to provide system information to a person involved in providing expert evidence. New qualifications or certification requirements may be necessary to ensure data evaluation and expert witness advice and testimony is informed by the latest technological developments in the automated vehicle space.

6.5.3 Proposed approach to data admissibility

Existing powers in taking evidence from vehicle occupants, discussed in section 6.3.1, may be relevant to data admissibility. It may be necessary to ensure the existing powers allowing evidence to be obtained from vehicle occupants can also be used to submit vehicle data evidence into prosecution.

If certification of individuals accessing vehicle data is required, corporate obligations, mentioned in section 6.4.2, may be relevant to ensuring there are suitably qualified local experts trained in the proper procedure.

A potential approach to overcoming both the shortage of certified people as well as qualified expert witnesses could be mandating ADSEs to train individuals familiar with its ADS technology as part of their market entry and certification process. However, jurisdictions should be mindful that a person trained by a manufacturer may be influenced by that manufacturer and no longer be independent for the purposes of providing expert witness testimony.

Question 22: What are the current challenges in using vehicle data as evidence? What are your views on whether automated vehicle data will be admissible in settling liability?

Question 23: Which examples of current in-vehicle technology – particularly in heavy vehicles – would help in considering these issues?

Question 24: Are new standards or qualifications needed so people who currently give expert evidence can do so for automated vehicles?

7 Interactions with the in-service regulator, ADSEs and registered owners

Key points

- Enforcement officers may need to communicate with, report incidents to and run investigations with several entities. They include the in-service regulator, ADSEs and registered owners.
- States and territories may need new powers to allow enforcement officers to disclose relevant data and information to the in-service regulator and ADSEs.
- Powers to share data need to describe the types of data and the purposes for which data is being requested.

7.1 Sharing data with the in-service regulator

Enforcement officers will need to report incidents (such as an automated vehicle running a red light) to the in-service regulator for investigation. Stakeholders noted that where such an incident occurs because of a faulty ADS, all automated vehicles with that particular ADS would likely be affected. However, it would be a challenge for enforcement officers to determine whether there is a systemic safety issue. The types of data and information that enforcement officers could need to share with the in-service regulator would be:

- ADS operational data (discussed in chapter 6)
- data relevant to offences: registration (or other identifier), time, date, location and the suspected offence.

The in-service regulator could then use this data and information to exercise its functions and powers, such as investigating potential general safety duty breaches by ADSEs.

7.1.1 Powers to share data with the in-service regulator

Some states (particularly South Australia and Victoria) have provisions allowing transport authorities to disclose vehicle-related information with public authorities.[53] These general disclosure powers may be sufficiently broad to encompass ADS data (Brady, et al., 2021, p. 42).

The powers do, however, have limitations. For example, s 41L of SA's Road Traffic Act provides that 'any records, devices or other things seized under this Act, or any information obtained under this Act, may, for the purposes of law enforcement, be given to any public authority of any jurisdiction' (emphasis added). The limitation to law enforcement purposes may limit disclosure to the in-service regulator, who may not be considered a law enforcement agency. We understand that, in the past, the National Heavy Vehicle Regulator has had issues with obtaining data from enforcement agencies because its status as a law enforcement agency was unclear.

[53] See, for example: *Road Traffic Act 1961* (SA), s 41L; *Road Safety Act 1986* (Vic), Part 7B.

A further limitation is that the general disclosure powers do not exist in all states and territories and, where they do exist, they appear to be narrower than the South Australian provision.

7.1.2 Practical considerations of sharing data with the in-service regulator

Feedback from consultations reveal that timeliness of reporting to the in-service regulator is key, particularly to address any systemic safety issues with a particular ADS. There may need to be a direct reporting channel from enforcement officers to the in-service regulator to report incidents.

One stakeholder indicated strong support for the in-service regulator to be the central information and data repository and facilitate information sharing between relevant parties. Information from both enforcement officers and the ADSEs should be supplied to the in-service regulator for investigation, monitoring and compliance.

Police stakeholders also raised that enforcement officers do not attend the scene of every crash or incident, and low-impact crashes are reported online. Enforcement officers would not be aware of all relevant incidents that should be reported to the in-service regulator.

On this point, we note that the in-service framework agreed by ministers includes a requirement on ADSEs to report to the in-service regulator significant safety incidents and road traffic law breaches when the ADS is engaged or during transition of control with the human operator, and instances where it received an infringement notice from a state or territory agency (National Transport Commission, 2022, pp. 76-77).

In relation to this requirement, a police stakeholder also noted that due to the potential negative commercial impacts for ADSEs reporting these incidents, there may be issues with ADSEs acknowledging in a timely manner that their ADSs have systemic safety issues.

7.1.3 Proposed approach

Noting the limitations in current state and territory powers to share data and information with the in-service regulator discussed in section 7.1.1, we propose that states and territories include new powers that would allow enforcement officers to disclose relevant data and information to the in-service regulator.

As a starting point, the new powers should outline:

- the types of data and information enforcement officers can provide to the in-service regulator – this could include, but not be limited to, ADS operational data and relevant identifiers for offences
- the purposes for which the data and information can be disclosed by enforcement officers to the in-service regulator. The broad purpose could be ‘to assist the in-service regulator to exercise its functions and powers’. This could include, but not be limited to, more specific purposes such as for the purpose of the in-service regulator using the data or information when investigating potential general safety duty breaches.

There would also need to be restrictions on further disclosure by the in-service regulator.

These would most likely be contained in the AVSL rather than in state and territory legislation.[54] We propose that, before introducing any new data disclosure powers from enforcement officers to the in-service regulator, states and territories complete a privacy impact assessment.

The in-service regulator and enforcement agencies would also need to mutually agree on the timing for data provision and the relevant reporting channels.

The requirements on ADSEs to report relevant incidents to the in-service regulator complement the proposed powers for enforcement officers to disclose relevant data and information to the in-service regulator. In terms of ADSEs reporting in a timely manner, we have previously noted that '[t]imeframes and thresholds may need to be developed over time by the in-service regulator so may be better prescribed within supporting regulations' (National Transport Commission, 2021, p. 37) rather than in the AVSL.

Question 25: What are your thoughts on the proposed approach to enforcement officers sharing data with the in-service regulator?

Question 26: What other options for sharing data are there to consider?

7.2 Sharing data with ADSEs

In most circumstances it is practical for the in-service regulator to share data with ADSEs. However, there may be some unique, and possibly rare, sets of circumstances or specific situations where an enforcement officer may need to share data with ADSEs. Some situations could include:

- For communicating ad hoc events such as a flooded road or to provide notice of unmanned roadblocks.
- Following an incident where the ADSE is considered at fault or nominated as responsible. This could be information about the incident, such as what offence has been committed and any relevant contextual data.

7.2.1 Powers to share data with ADSEs

The QUT report noted that the 'patchwork of existing powers giving police and transport agencies the ability to disclose information gathered under policing, road and vehicle law cross the jurisdictions' would not allow enforcement officers to disclose data to ADSEs (QUT, 2021, p. 67). The report noted a substantial gap in state and territory powers concerning disclosure of data and information to ADSEs.

[54] The NTC commission a privacy impact assessment on the proposed in-service framework that considers the privacy implications of the collection, use and disclosure of personal information under the framework. The assessment is available online at: https://www.ntc.gov.au/transport-reform/ntc-projects/in-service-safety-AVs.

7.2.2 Practical considerations of sharing data with ADSEs

Stakeholders raised several practical considerations relating to enforcement officers sharing data with ADSEs. It may not be practical for enforcement officers to determine the responsible ADSE for an individual vehicle in every case so they can share data with the relevant ADSE.

Another potential issue to consider is how enforcement officers would communicate ad hoc events – for example, whether an automated vehicle would need to contain a specific type of technology to receive this data. A stakeholder also noted that another issue relates to the timeliness of information sharing between enforcement officers with ADSEs, particularly where another authority, such as local government, is managing an incident and how this could be done in a seamless way.

7.2.3 Proposed approach

Noting the gap identified in section 7.2.1, we propose that states and territories include new powers that would allow enforcement officers to disclose relevant data and information to ADSEs. At this stage, the specific situations in which ADSEs would require such disclosure are not all known and the purposes for disclosing data are likely to be quite varied. It is difficult to suggest an approach beyond recognising that such a power is probably needed. Stakeholders have noted that this power may not be necessary because the in-service regulator should be the only entity with which law enforcement shares data.

While we recognise the need to reduce the reporting burden on enforcement, there may be certain limited situations where the power to share data and information with an ADSE may be required. We recommend a power to share information with ADSEs to be drafted in a non-obligatory manner so law enforcement can develop an appropriate approach to sharing data with an ADSE, should they wish to do so.

Similar to other proposed data access powers, we propose that states and territories complete a privacy impact assessment before introducing new data disclosure powers.

Question 27: What other data may enforcement agencies need to share with the in-service regulator?

Question 28: Do you agree with the proposed approach of drafting new powers specifying the types and purpose of vehicle data that can be disclosed?

Question 29: Do you think the in-service regulator should establish a time window within which ADSEs must provide data?

Question 30: What are your thoughts on the proposed approach to enforcement officers sharing data with ADSEs?

Question 31: Do you agree a privacy impact assessment is required before introducing new data disclosure powers?

8 Operational impacts on enforcement roles, responsibilities and resources

Key points

- Automated vehicles will have an impact on the role, responsibility and resources of enforcement.
- It is difficult to quantify the scope of these impacts at the moment. We need to know more about automated vehicles and how they will operate in the Australian environment.
- State and territory governments should consider the potential operational impacts within their jurisdiction. This will help them plan for adequate training and investment in infrastructure.

Automated vehicles challenge the role of enforcement officers in routine encounters as well as at crashes. This will necessitate the development of new standards for such interactions. A key challenge will be for law enforcement to keep up with current automated vehicle technology and the extent to which the technology affects the operational role of law enforcement.

This chapter provides a collation of potential operational impacts on enforcement roles, responsibilities and resources. It is intended to acknowledge the issues and support states and territories in considering the potential operational impacts within their jurisdiction.

8.1 Modified role for enforcement officers

We recognise that automated vehicles have the potential to reduce the use of police to enforce traffic safety laws and allow these resources to be reallocated to other serious criminal activities. We also acknowledge that once automated vehicles begin operating on the roads, the role enforcement officers will play at a crash scene or incident may change.

The existing responsibility of officers is to investigate the crash and ensure correct forensic procedures are followed. Enforcement is tasked with making observations about the scene, questioning those involved and witnesses, and ensuring that those involved are not in further danger. We anticipate an additional public safety role for enforcement officers in providing information to the in-service regulator about ADS issues.

Officers will need to consider the actions of a human driver (if a conventional vehicle was also involved), ADS, fallback-ready user and possibly passengers in the absence of a human operator. Officers will need to enforce ADSE and fallback-ready user obligations at the same time, and this may present a challenge in the field. The need for quick reporting to the in-service regulator following certain incidents may put added pressure on enforcement officers.

We acknowledge that enforcement officers would play a significant part in this process as first responders despite establishing the role of ADSEs to report incidents to the in-service regulator. States and territories will need to plan for additional resourcing and training and apply existing frameworks where appropriate to ensure enforcement officers are equipped for the uptake of automated vehicles.

8.2 Cost implications of automated vehicles

8.2.1 Training in multiple vehicle systems and costs

Automated vehicles will increase training and resourcing requirements on law enforcement to accommodate a changed road environment. Enforcement officers' familiarity with what they can encounter in the field may be challenged as emerging technologies and a variety of ADSEs and ADSs enter the market. Officers may need training in multiple vehicle systems and the processes that may be unique to automated vehicles. Law enforcement entities will require a sustained investment in officer training. Consequently, there may be a time impact on officers, possibly more so in the early stages of deployment, and, as stakeholders have pointed out, it may be difficult to quantify the extent of the impact at this point in time. Familiarity with ADS technology and staff training will be a necessary investment to uphold the regulatory framework that is yet to be established.

8.2.2 Cost of inconsistent interfaces between automated vehicles and enforcement

Enforcement officer technology is often linked to other complex systems. Other costs associated with the emerging role of this technology include the possibility that there will be inconsistencies between the interfaces of automated vehicles and enforcement. Enforcement officers may be unable to interact with the vehicles, causing a rise in costs associated with a delay in standard enforcement processes. There may be a need to purchase or build and maintain new devices or systems, such as software licences, and stringent data reporting requirements will necessitate further training for enforcement and compliance officers to recognise what the expectations and processes are.

Stakeholders noted the need for standardisation of processes to ensure a consistent and seamless data transfer between ADSEs and law enforcement. However, as Australia will ultimately need to follow major international standards development and market evolutions, states and territories should be prepared for additional costs associated with ensuring law enforcement systems align with ADSEs.

8.2.3 Implications of process to the infringement system

The emergence of automated vehicles will also likely involve changes to the existing automated infringement system. Authorities may need to first determine whether the ADS was engaged at the point of infringement and then determine whether the infringement notice is sent to the registered owner or the ADSE, or both. Processes relating to nominating the 'driver' may also need to change, and this will most likely require a supporting education campaign to improve public awareness.

Finally, the changes to processes around camera-detected road rules breaches will probably require changes to IT systems, requiring states and territories to review their current IT infrastructure and potentially invest in new systems.

8.3 Case study – camera-detected road rule breaches

The purpose of this case study is to highlight some of the relevant interactions between enforcement officers, registered owners, ADSEs and the in-service regulator.

In the NTC's most recent policy paper on the regulatory framework for automated vehicles in Australia, we noted the following (National Transport Commission, 2022, p. 59):

- Where a human driver breaches a road rule while driving an automated vehicle and the ADS was not engaged, they will continue to be subject to relevant state and territory infringements (or other relevant sanctions).
- However, the matter should be referred to the in-service regulator and investigated as a potential breach of the general safety duty where either:
  - the ADS was clearly engaged at the time of the breach
  - the driver considers the ADS was engaged, or
  - control is unclear.
- In the early stages of automated vehicle rollout in Australia, the current infringements system could be used to issue an infringement notice to the registered owner or operator in the first instance, with the ability for them to subsequently nominate the ADSE as responsible. States and territories will need to further consider this process.

The policy paper contains further detail about this approach (National Transport Commission, 2022, pp. 59-60).

In initial consultation for this project, we received feedback from government and police stakeholders about this case study:

- There are time limitations on taking action against a person for a road transport law breach. This varies by jurisdiction but is generally six to 12 months. Timeliness of process and interaction with relevant parties is critical because avenues for investigation degrade over time, regardless of formal statutory time limits.
- There should be a new process for sending infringement notices. Before sending an infringement notice to the registered owner, enforcement officers could make initial enquiries to establish whether a human was or should have been in control of the automated vehicle at the time. If the ADS was in control, enforcement officers could report directly to the in-service regulator. There were, however, some comments that requiring enforcement officers to conduct a preliminary investigation was a waste of resources.
- The current process could result in owners always nominating the ADSE as responsible. False driver nominations occur today but are likely to increase with automated vehicles. This may be a small issue initially, but it will increase over time. The in-service regulator will have a large volume of information and nominations to deal with. The ADS is not expected to breach road rules very often, and there are millions of camera-detected offences each year.
- Registered owners could be pursued for obstruction of justice and other offences if they nominate the ADSE as responsible while knowing the ADS was not engaged at the time of the offence. There is merit in communicating this to registered owners.

We are not proposing an approach or suggesting that states and territories create new infringements systems. Rather, we are suggesting some high-level principles states and territories could consider when looking at the issue of camera-detected road rule breaches involving automated vehicles. Infringement systems differ between jurisdictions, and whether a new process is needed is for states and territories to consider.

Some stakeholders noted that any changes to the current infringements system could have significant IT implications. We suggest some high-level principles are that:

- Appropriate action can always be taken against the responsible party.
- Any changes to current processes can be justified with relevant improvements such as time and cost savings.
- The process is timely not only from a statute of limitations or evidentiary perspective but also from the perspective of reporting potential breaches to the in-service regulator. Where an incident occurs because of a faulty ADS, all automated vehicles with that particular ADS would likely be affected, creating significant road safety risks. Processes that ensure timely reporting of camera-detected road rule breaches to the in-service regulator are preferable (although, as discussed in section 5.1.2, ADSEs would also be required to report these breaches to the in-service regulator).

9 Conclusion and next steps

Key points

- We are seeking submissions to this discussion paper by 5 September, 2022.
- Following the close of the consultation period we will develop recommendations for infrastructure and transport ministers.

9.1 Conclusion

In this discussion paper we have set out a number of potential issues relating to on-road enforcement. Broadly, these issues include:

- Enforcement officer powers and practical considerations for providing on-road directions to automated vehicles.
- Enforcement officer powers to disable an ADS, practical considerations for disabling an ADS and processes after an ADS has been disabled.
- Enforcement access to automated vehicle data is highly desired and will require support through a robust regulatory framework that considers the future data needs, availability, access and admissibility.
- The relationship between enforcement officers and the in-service regulator, ADSEs and registered vehicle owners, as it relates to the timeliness of data sharing, process and types of data to be communicated.
- The operational impacts of automated vehicles on enforcement roles, responsibilities and resources.

We have proposed options and approaches for addressing the above challenges, consistent with the NTC's role in developing a national approach that allows enforcement officers to interact with automated vehicles and respond to the safety risks they may raise.

The tension between the uncertainty of the future technological capabilities and the desire to be prepared when automated vehicles appear on our roads will persist for some time. That is why we believe it is imperative the Commonwealth, state and territory governments continue to collaborate closely and support further ongoing engagement with industry as the technology capabilities evolve and develop.

We recognise the desire for the NTC to propose definitive solutions. However, in anticipation of the ADS technology continuing to be developed and refined, we have attempted to propose options and approaches that offer jurisdictions the flexibility to adapt, both to the technological changes in the ADS as well as the evolving law enforcement requirements, over time.

9.2 Next steps

We are seeking views on the consultation topics presented in this discussion paper and any other matters relevant to the interaction between law enforcement and automated vehicles. The period for written submissions and other feedback will close on Monday 5 September, 2022. Further information on providing a submission can be found on page 3. During the consultation period we will undertake further consultation with stakeholders. Following this, we will develop a policy paper and recommendations for the approval of infrastructure and transport ministers.

Appendix Design principles for government access to C-ITS and automated vehicle data

The laws and aligned standards for cooperative intelligent transport systems (C-ITS) and automated vehicles should:

1. balance the benefits of government access to C-ITS and automated vehicle data with additional privacy protections to appropriately limit the collection, use and disclosure of C-ITS and automated vehicle data

2. be consistent with, and informed by, existing and emerging Australian and international privacy and data access frameworks

3. embed access powers and privacy protections for C-ITS and automated vehicle data in legislation

4. clearly define C-ITS and automated vehicle data in inclusive and technology neutral terms

5. align government entities' approach to managing C-ITS and automated vehicle data with the objectives underlying existing concepts of personal information

6. specify the C-ITS and automated vehicle data covered, the purposes for which the data can be used and the parties to whom the purpose limitations apply while not impeding access to data with a warrant or court order authorising a different use

7. recognise the importance of notifying users in plain English about government collection, use, disclosure and storage of C-ITS and automated vehicle data

8. recognise that meaningful informed consent is important but provides avenues for government entities to balance individuals' expectations of privacy in alternative ways where obtaining such consent is not possible

9. recognise the difficulty of irreversibly de-identifying C-ITS and automated vehicle data in many circumstances

10. support data security

11. allow for regular review of privacy protections for C-ITS and automated vehicle data.

References

57th Queensland Parliament Transport and Resource Committee, 2021. *Inquiry into vehicle safety, standards and technology, including engine immobiliser technology,* September 2021 s.l.: s.n.

Austroads, 2020. *Data requirements for automated and electric vehicle registration.* [Online] Available at: https://austroads.com.au/latest-news/data-requirements-for-automated-and-electric-vehicle-registration
[Accessed 13 April 2022].

Automated Vehicle Safety Consortium, 2020. *Best Practice for First Responder Interactions with Fleet-Managed Automated Driving System-Dedicated Vehicles (ADS-DVs).* [Online] Available at: http://go.sae.org/rs/525-RCG-129/images/AVSC00005202012.pdf?mkt_tok=NTI1LVJDRy0xMjkAAAGAyi0PKlIhzQJBHS9XuFmUqX_KTbcXR8-II1PPG-AXWwxM_BGq3dbZCFTWdCyuKH-7SZjSawp3SZrU9TaqI_gtcKigTjsRSZuIsLBeP_OemLdQhA
[Accessed 19 April 2022].

Brady, M., Tranter, K. & Bennett, B., 2021. *Applicability of state and territory roadside enforcement powers to automated vehicles,* Brisbane: Queensland University of Technology.

Cruise, 2021. *Driverless Deployment Program Guidance for First Responders,* s.l.: s.n.

Global Forum for Road Traffic Safety, 20-24 September. *Position statement on optical and/or audible signals in the context of driver assistance systems, advanced driver assistance systems and autonomous vehicles,* s.l.: Submitted by Germany, 83rd session, Geneva.

National Transport Commission, 2019. *Regulating government access to C-ITS and automated vehicle data: Policy paper,* Melbourne: National Transport Commission.

National Transport Commission, 2021. *A national in-service safety law for automated vehicles,* s.l.: s.n.

National Transport Commission, 2022. *The regulatory framework for automated vehicles in Australia,* Melbourne: National Transport Commission.

National Transport Commisssion, 2018. *Changing driving laws to to support automated vehicles,* s.l.: s.n.

QUT, 2021. *Applicability of State and Territory Roadside Enfrocement Powers to Automated Vehicles,* s.l.: s.n.

Waymo, 2021. *Waymo autonomously driven Chrysler Pacifica – Emergency response guide and law enforcement interaction protocol.* [Online]
[Accessed 2022].

National Transport Commission
Level 3/600 Bourke Street
Melbourne VIC 3000
Ph: (03) 9236 5000
Email: enquiries@ntc.gov.au
www.ntc.gov.au