Regulating government access to C-ITS and automated vehicle data

August 2019

Policy paper

National Transport Commission

Report outline

Title Regulating government access to C-ITS and automated vehicle data

Type of report Policy paper

Purpose Recommendations approved by the Transport and Infrastructure Council in August 2019

Abstract This policy paper considers the new privacy challenges associated with government collection and use of data likely to be generated by C-ITS and automated vehicle technology. It shows that Australia’s information access framework may not be sufficient to address these challenges and recommends broad design principles to guide the development of C-ITS and automated vehicle laws and aligned standards.

Key words Data, information, C-ITS, automated vehicles, privacy, privacy challenges, surveillance, government access, government collection, government use, information access framework, design principles

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

Foreword

The National Transport Commission is working with the state, territory and Commonwealth governments on a program of regulatory reform to ensure Australians gain the potential benefits of automated vehicles. This work aims to develop flexible and responsive end-to-end regulation for the commercial deployment of automated vehicles that supports safety and innovation.

Cooperative intelligent transport systems (C-ITS) and automated vehicle technology offer the possibility of fundamentally changing how transport is provided and unlocking a range of safety, productivity, environmental and mobility benefits. Data generated by these technologies has the potential to inform and enhance government decision making, but at the same time this technology raises potential new privacy challenges for individuals.

Regulating government access to C-ITS and automated vehicle data recommends a way forward for regulating government access to C-ITS and automated vehicle technology data that addresses this balance.

I would like to acknowledge the valuable input provided by stakeholders in informing this policy paper. I encourage government, industry and the wider community to continue to work with us on the next steps in this policy development and on our broader automated vehicle regulatory reform agenda to ensure Australians can gain the benefits of this technology.

Carolyn Walsh
Chair and Commissioner

Contents

List of tables

List of figures

Executive summary

The purpose of this paper is to provide analysis and recommendations on the following three issues that the National Transport Commission (NTC) consulted publicly on during 2018:

- potential new privacy challenges of government access to data generated by cooperative intelligent transport systems (C-ITS) and automated vehicle technology
- the adequacy of Australia's 'information access framework'[1] to address these new privacy challenges
- a recommended approach for reform if the current framework is not sufficient.

Context

This work is part of the NTC's broader automated vehicle national reform program, which aims to put **end-to-end regulation** in place to support the safe commercial deployment and operation of **automated** vehicles.

This paper delivers on transport ministers' decisions from 2013 and 2016, which require the NTC to consider options to manage government access to C-ITS and automated vehicle data.[2]

This paper is limited to examining if additional privacy protections for government collection and use of data generated by C-ITS and automated vehicle technology are needed. It does not consider:

- access to data by motor accident injury insurers
- new powers for government agencies to access data
- Australia's information access framework as it applies to the private sector
- access to data by consumers for disputing liability.

In the broader automated vehicle national reform program, the NTC is considering two matters that were out of scope for this project:

- data recording and sharing obligations on automated driving system entities[3]
- new powers for governments to access data, including for law enforcement purposes.

[1] We use the term 'Australia's information access framework' to refer to existing privacy protections, and powers to collect data that collectively provides the framework for governments to access, use and disclose data. This includes legislation at the state and federal levels. The main elements are privacy laws, government collection powers and surveillance device laws.

[2] In 2016 the Transport and Infrastructure Council recommended 'That the NTC develops options to manage government access to automated vehicle data, having regard to achieving road safety and network efficiency outcomes and efficient enforcement of traffic laws, balanced with sufficient privacy protections for automated vehicle users.' In 2013 the Standing Council on Transport and Infrastructure agreed in principle to stronger privacy restrictions for government access to C-ITS data (in the event that C-ITS data was deemed to be personal information) and recommended that 'In the event that individuals can be reasonably identified from the safety data message broadcast by C-ITS devices, that specific legislative protections are developed to define in what circumstances organisations that are exempt from compliance with privacy principles, including enforcement agencies, may access C-ITS personal information.'

[3] Entities looking to bring the automated vehicle technology to market.

Consultation

In September 2018 we released a discussion paper. The key issues we sought stakeholder feedback on were:

- the adequacy of Australia’s information access information access framework for government access to C-ITS and automated vehicle technology data
- if reform is needed to address new privacy challenges.

We received 41 submissions from a wide range of stakeholders including state and territory governments, local governments, legal firms, peak industry bodies, consultancies and industry. Our recommendations to the Transport and Infrastructure Council are informed by the feedback.

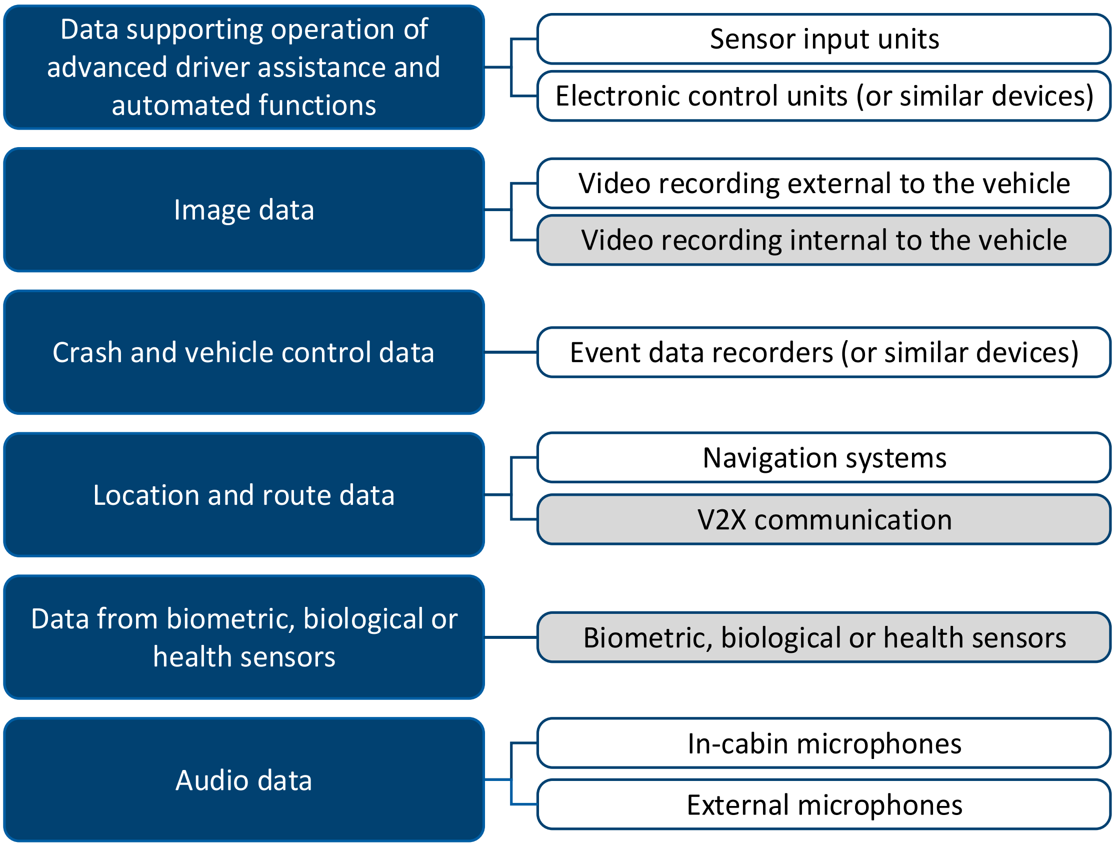
Overview of technology in vehicles

C-ITS data is produced when components of the transport network (vehicles, roads and infrastructure) communicate and share real-time information (for example, information on vehicle movements, traffic signs and road conditions) through C-ITS devices. These communications can produce data such as vehicle speed, location or direction.

Automated vehicle data is derived from a combination of vehicle technology sources that support the performance of the dynamic driving task by the automated driving system.

Figure 1 provides an overview of technology in vehicles – both current and future. Highlighted in grey are three C-ITS and automated vehicle technologies the NTC considers may create new privacy challenges and are likely to be widespread in future vehicles.

Figure 1. Overview of technology in vehicles


Data supporting operation of advanced driver assistance and automated functions
Sensor input units
Electronic control units (or similar devices)
Image data
Video recording external to the vehicle
Video recording internal to the vehicle
Crash and vehicle control data
Event data recorders (or similar devices)
Location and route data
Navigation systems
V2X communication
Data from biometric, biological or health sensors
Biometric, biological or health sensors
Audio data
In-cabin microphones
External microphones

Benefits of government access to information generated by vehicle technology

Stakeholder feedback, particularly from transport agencies, highlighted that information generated by vehicle technology could inform and enhance government decision making. The four main categories where information generated by C-ITS and automated vehicle technology could aid government decision making are:

- law enforcement
- automated vehicle safety
- traffic management and road safety as part of network operations
- infrastructure and network planning as part of strategic planning.

Stakeholders also noted the importance of balancing potential improved government decision making and public benefits with sufficient privacy protections for C-ITS and automated vehicle users. There is a risk that broad collection and use by government of this information will be a barrier to the take-up of C-ITS and automated vehicle technology in Australia.

What are the potential new privacy challenges and are they sufficiently addressed?

The NTC has identified three categories of new privacy challenges of C-ITS and automated vehicle technology:

- **Category 1**: new data captured by automated vehicle technology.

  In-cabin cameras and biometric, biological or health sensors are the most likely automated vehicle technologies to create new privacy challenges. Such technologies are either not contained in current vehicles or are limited in use.

- **Category 2**: C-ITS technology may allow for more widespread direct collection of location data by government.

  The type of data generated by C-ITS technology (speed, location and direction) is broadly similar to data generated by technology contained in current vehicles. However, C-ITS technology still presents new privacy challenges because of how widespread the direct collection of this data by government may be in the future. The risk is therefore not linked to the type of data, but rather the method and potential volume of collection.

- **Category 3**: C-ITS and automated vehicle technology will generate a greater breadth and depth of data.

  This introduces new privacy challenges because more data is generated and stored, and there is an increased opportunity for data linking by government.

The NTC considers that C-ITS and automated vehicle technology will most likely generate personal information and sensitive information, especially when held by road agencies and law enforcement agencies. Such agencies are likely to have access to a wide range of data, and the technical capacity to analyse that data, which could aid identifiability. As such, government access to this data may affect individual users of C-ITS and automated vehicle technology.

The NTC considers that the privacy challenges may not be sufficiently addressed under Australia’s information access framework for the following reasons:

- Surveillance device laws are unlikely to place practical restrictions on government collection of personal information.
- While privacy principles do not authorise the collection of personal information, they do not restrict (because they allow/permit) direct collection of personal information by government agencies if the information 'is necessary for one or more of its functions or activities'.[4] This facilitates government's increased ability to directly collect C-ITS personal information.
- Law enforcement collection, use and disclosure of C-ITS and automated vehicle data may result in increased opportunities for surveillance.
- Road transport laws in some jurisdictions contain provisions to facilitate data sharing between road agencies and police.
- Requirements to destroy or de-identify personal information may not in practice greatly reduce the amount of personal information held by government. Government may therefore continue to use and disclose the greater breadth and depth of personal information generated by C-ITS and automated vehicle technology once it is collected.
- There is inconsistency in the current information access frameworks for government agencies across states and territories.

What are the options to address the new privacy challenges?

The gaps identified in the information access framework primarily relate to potentially wide allowable collection, use and disclosure of personal information, especially for law enforcement purposes. For this reason, we developed options to focus on limiting the collection, use and disclosure of C-ITS and automated vehicle data to specific purposes.

In the discussion paper we proposed separate options for addressing these challenges for C-ITS technology and for automated vehicle technology because the issues and implementation options differ.

We presented four options for addressing the new privacy challenges of automated vehicle technology:

- option 1: rely on the existing information access framework to address the new privacy challenges of automated vehicle technology (no change)
- option 2: agree broad principles on limiting government collection, use and disclosure of automated vehicle data[5] (reform option)
- option 3: limit government collection, use and disclosure of automated vehicle data from in-cabin cameras and biometric, biological or health sensors to specific purposes (reform option)
- option 4: limit government collection, use and disclosure of all automated vehicle data to specific purposes (reform option).

We also presented three options for addressing the new privacy challenges of C-ITS technology:

- option 1: rely on the existing information access framework to address the new privacy challenges of C-ITS technology (no change)

[4] Australian Privacy Principle 3.1.

[5] Note in the discussion paper we referred to 'information' throughout these options instead of 'data'.

- option 2: agree broad principles on limiting government collection, use and disclosure of C-ITS data (reform option)
- option 3: limit government collection, use and disclosure of all C-ITS data to specific parties and purposes (reform option).

Stakeholder feedback highlighted similarities in the issues for C-ITS and automated vehicle technology. At this early stage of regulatory framework development, the NTC considers it is possible to have a broadly similar approach for both technologies. We have therefore combined the options analysis for both C-ITS and automated vehicle data in this policy paper. However, we note that, in future, the broad approach we recommend can be refined to consider variations in timeframes for deployment and uptake, specific challenges and risks of each technology and the differences in implementation paths. The NTC is not proposing that a single legislative framework covering C-ITS and automated vehicles needs to be established.

NTC’s recommended approach

At this stage of C-ITS and automated vehicle development, we consider that option 2 is the preferred option.

Because option 2 agrees broad design principles, we consider it best addresses the identified challenges while ensuring that governments can appropriately use data from future vehicle technology to benefit the community. These principles will help guide further development of the regulatory framework for C-ITS and automated vehicle technologies while providing a sufficient degree of flexibility as the technology develops.

The broad design principles are set out in Table 1.

Table 1. Principles for government access to C-ITS and automated vehicle data

The laws and aligned standards for 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 provide 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.

Next steps

The above design principles will guide:

- the NTC's development of laws to regulate government access to automated vehicle data. This work will specifically relate to proposals for compliance and enforcement mechanisms for automated vehicle regulation, which will flow from current work on in-service safety of automated vehicles. This work is due to begin at the end of 2019
- Austroads' development of the National Intelligent Transport Systems Architecture Framework.

Transport and infrastructure ministers have also directed the NTC to lead a new piece of work, with support from states, territories and Austroads, on government access and use of C-ITS and automated vehicle data, including for network efficiency and investment purposes. We will develop the scope and timing for this work in 2019.

1 Context

Key points

- The National Transport Commission is reviewing government access to data and privacy protection regulations in Australia in light of significant developments in transport technology and potential privacy issues that may arise.
- This paper makes recommendations on government access to cooperative intelligent transport systems and automated vehicle data and privacy regulations in Australia.

1.1 Objectives

1.1.1 Purpose of this policy paper

The purpose of this policy paper is to:

- outline potential new privacy challenges associated with government collection and use[6] of data generated by cooperative intelligent transport systems (C-ITS) and automated vehicle technology
- apply Australia's information access framework[7] to government collection and use of data likely to be generated by C-ITS and automated vehicle technology
- consider feedback received as part of consultation for the discussion paper on the adequacy of the information access framework to cover any new privacy challenges and proposed options for reform
- recommend an approach for addressing privacy challenges associated with government collection and use of information generated by C-ITS and automated vehicle technology.

1.1.2 Objectives of this work

The objective of this work is to assess whether Australia's information access framework applying to government collection and use of data is sufficient to protect privacy given the significant developments in transport technology. In particular, we need to consider the adequacy of existing regulation in light of the types and amount of data that future transport systems will be able to produce.

We focus on two areas that form a limited part of intelligent transport systems (ITS): C-ITS and automated vehicles. C-ITS means a technology platform that enables components of the transport network (vehicles, roads and infrastructure) to wirelessly communicate and share real-time data, including data on vehicle movements, traffic signs and road conditions. Automated vehicles are vehicles that include an automated driving system capable of performing the entire 'dynamic driving task' (steering, acceleration, braking and monitoring

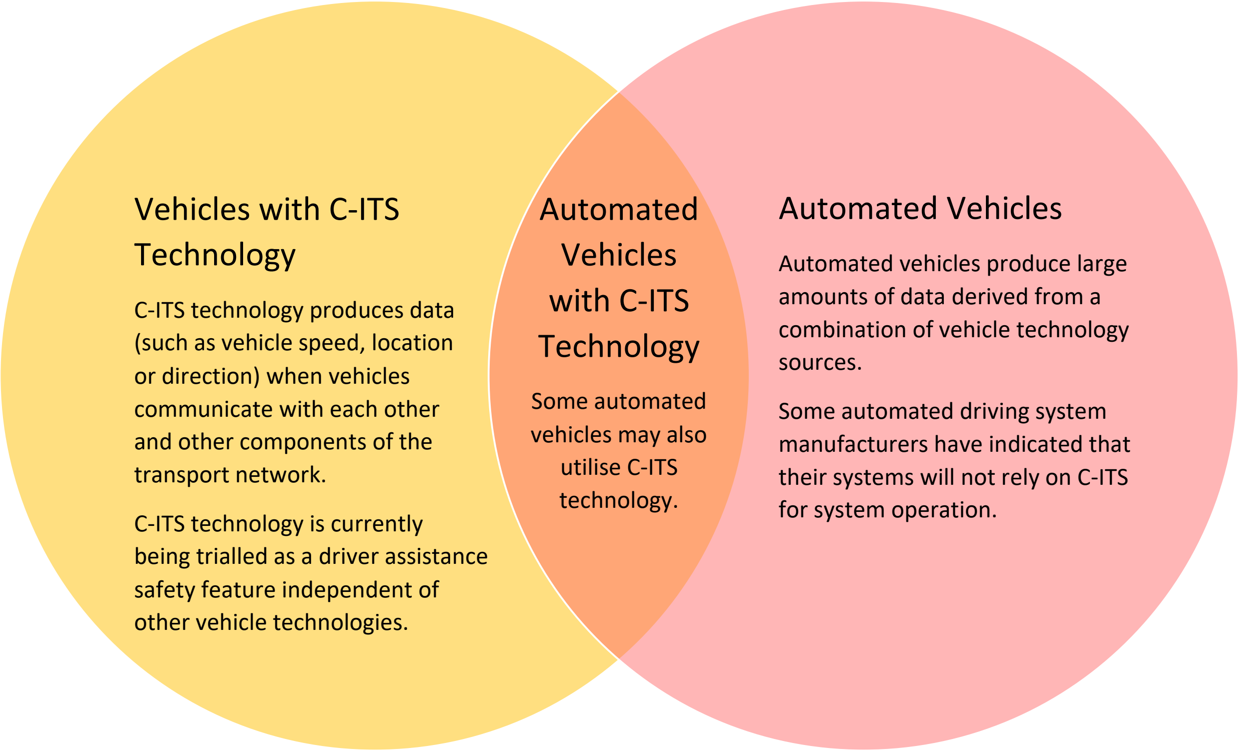
[6] In this policy paper 'use' is generally intended to broadly cover use, disclosure and de-identification or destruction of information. In chapters 5, 6 and parts of 7, use, disclosure and de-identification or destruction are discussed as separate concepts.

[7] We use the term 'Australia's information access framework' to refer to existing privacy protections and powers to collect data that collectively provides the framework for governments to access, use and disclose data. This includes legislation at the state and federal levels. The main elements are privacy laws, government collection powers and surveillance device laws.

the driving environment) on a sustained basis. This technology will most likely produce and retain data about vehicle behaviour and vehicle occupants.

Figure 2 highlights that C-ITS and automated vehicles are related but separate elements of the ITS ecosystem.

Figure 2. C-ITS and automated vehicles as elements of the ITS ecosystem



Vehicles with C-ITS Technology

C-ITS technology produces data (such as vehicle speed, location or direction) when vehicles communicate with each other and other components of the transport network.

C-ITS technology is currently being trialled as a driver assistance safety feature independent of other vehicle technologies.

Automated Vehicles with C-ITS Technology

Some automated vehicles may also utilise C-ITS technology.

Automated Vehicles

Automated vehicles produce large amounts of data derived from a combination of vehicle technology sources.

Some automated driving system manufacturers have indicated that their systems will not rely on C-ITS for system operation.

1.2 About the National Transport Commission

The NTC is a statutory agency that proposes nationally consistent land transport reforms to the Transport and Infrastructure Council. The council comprises Commonwealth, state and territory ministers who are responsible for transport and infrastructure.

The NTC contributes to achieving national reform priorities that are agreed by the council. Our reforms are objectively assessed against the following policy objectives:

- improve transport productivity
- improve environmental outcomes
- support a safe transport system
- improve regulatory efficiency.

One of our key focus areas is removing regulatory barriers to innovative transport technologies that have significant safety, productivity and environmental benefits.

1.3 What problem are we trying to address?

When vehicles with C-ITS and automated technology are ready for commercial deployment, there are risks that privacy concerns will be a barrier to their take-up and use in Australia. Consumers may be uncomfortable about the amount and type of personal information governments could access or have concerns because government access is inconsistent or unclear. This could delay the deployment of this technology, which has the potential to significantly improve road safety. The problem is discussed in further detail in Chapter 2.

Australia's existing information access framework was developed when C-ITS and automated vehicle technology did not exist. The breadth, depth and type of data that can be produced by this technology was unknown. Most notable is that current Commonwealth and state and territory information privacy regulations provide a low threshold to exempt enforcement activities from privacy principles.

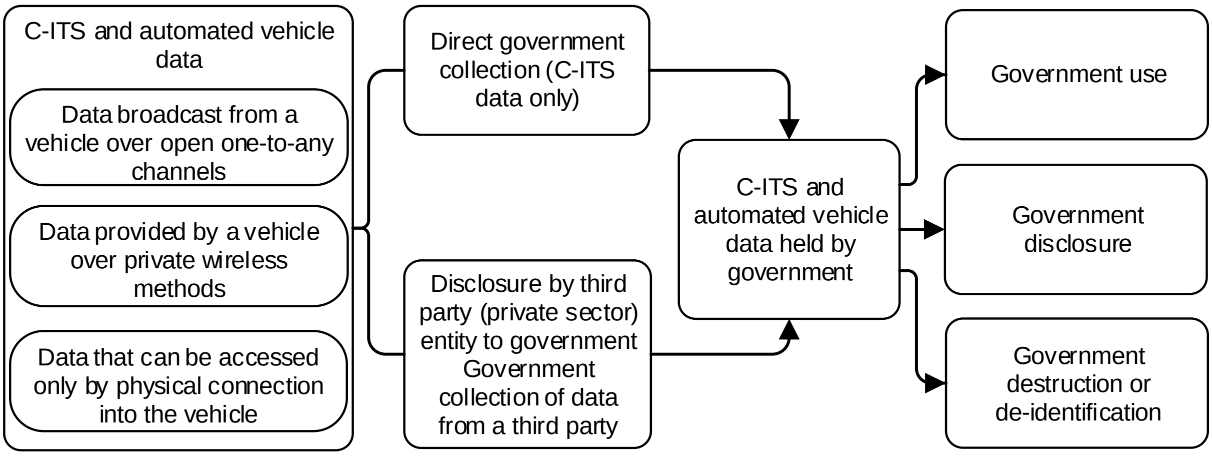
The NTC recognises that there may be an additional element to the problem – that individuals do take up the technology but continue to use it while their privacy is not sufficiently addressed. However, the NTC has a mandate for transport policy reform and not a broader privacy advocacy role. As such, the NTC is focusing on privacy issues as they relate to barriers to using technologies that can significantly improve road safety.

We assess the extent of the problem by examining what is different about government access to data generated by C-ITS and automated vehicle technology and whether there are sufficient privacy challenges to require change.

- **Chapter 2** outlines the paper's scope and assumptions.
- **Chapter 3** discusses data generated by current and future vehicle technology.
- **Chapter 4** discusses the benefits of government access to data generated by vehicle technology.
- **Chapter 5** considers new privacy challenges of C-ITS and automated vehicle technology.
- **Chapter 6** discusses gaps in Australia's information access framework to manage government access.
- **Chapter 7** assesses options and recommends an approach for managing government access to C-ITS and automated vehicle data.
- **Chapter 8** outlines principles for regulating government access to C-ITS and automated vehicle data.
- **Chapter 9** outlines the next steps for this work.

Figure 3 represents the possible movement of C-ITS and automated vehicle data accessed by government.

Figure 3. Movement of C-ITS and automated vehicle data accessed by government


C-ITS and automated vehicle data
Data broadcast from a vehicle over open one-to-any channels
Data provided by a vehicle over private wireless methods
Data that can be accessed only by physical connection into the vehicle
Direct government collection (C-ITS data only)
Disclosure by third party (private sector) entity to government Government collection of data from a third party
C-ITS and automated vehicle data held by government
Government use
Government disclosure
Government destruction or de-identification

1.4 Legal research and consultation

1.4.1 University of New South Wales legal research report

Academics from the University of New South Wales prepared a legal research report for the NTC in mid-2018. *The privacy and data protection regulatory framework for C-ITS and AV systems*[8] (the UNSW report) analyses the application of Australia's information access framework to data generated by C-ITS and automated vehicle technology.

The UNSW's report informed and supported the NTC's development of issues and analysis in the discussion paper and this policy paper.

1.4.2 Consultation to date

In September 2018 the NTC published the discussion paper *Regulating government access to C-ITS and automated vehicle data* (the discussion paper). It outlined new privacy challenges associated with government collection and use of data generated by C-ITS and automated vehicle technology. It posed 13 questions for stakeholders as well as potential reform options.

We received 41 submissions. Of these, 35 were public and are available on the NTC website.[9] Six submissions were made confidentially. Submissions were received from a wide range of stakeholders including state and territory governments, local governments, legal firms, peak industry bodies, consultancies and industry.

The NTC has incorporated views expressed by stakeholders into our analysis in this policy paper. To provide maximum transparency about our reasoning while protecting the rights of stakeholders to make confidential submissions, we refer to these views in our analysis by only identifying the sector from which they came.

1.5 Key terms used in this paper

Automated vehicles are vehicles that include an ADS that is capable of performing the entire driving task (steering, acceleration, braking and monitoring the driving environment) on a sustained basis.[10]

Automated driving system (ADS) means the hardware and software that are collectively capable of performing the entire dynamic driving task on a sustained basis.[11]

Automated driving system entity (ADSE) means the legal entity responsible for the ADS. This could be the manufacturer, operator or legal owner of the vehicle, or another entity seeking to bring the technology to market in Australia.

Automated vehicle data is derived from a combination of vehicle technology sources that support the performance of the dynamic driving task by the ADS.

Cooperative intelligent transport system (C-ITS) means a technology platform that enables components of the transport network (vehicles, roads and infrastructure) to

[8] The UNSW report can be accessed at https://www.ntc.gov.au/Media/Reports/(A4689742-E776-D8B3-1837-C4F6F3969B2E).pdf.

[9] Submissions can be accessed at https://www.ntc.gov.au/submissions/history/?rid=166821&pid=11450.

[10] ADSs that perform the entire dynamic driving task while engaged are contained in levels 3–5 automated vehicles, as defined in the Society of Automotive Engineers (SAE) International Standard J3016, *Taxonomy and definitions for terms related to driving automation system for on-road vehicles* (SAE J3016), p 19.

[11] This term has been paraphrased from SAE J3016.

wirelessly communicate and share real-time information, including data on vehicle movements, traffic signs and road conditions.

C-ITS data is produced when components of the transport network communicate and share real-time information through C-ITS devices. These communications can produce data such as vehicle speed, location or direction. The focus of this policy paper is on data produced by vehicles.

Data aggregation is any process in which data is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to get more information about particular groups based on specific variables such as age, profession or income.

Data linking means a process for combining individual records from two or more data sources. Datasets that may not independently identify an individual may do so when linked.

De-identified data means data from which the obvious personal identifiers have been removed. It covers both information that cannot be re-identified and pseudonymised information (the removal of individual identifiers). When data is pseudonymised it is most likely still identifiable when combined with other data.

Personal information means (broadly) information about a reasonably identifiable individual. Definitions of personal information are discussed in more detail in section 5.4.

1.6 Background

1.6.1 Mandate

This work derived from two previous recommendations agreed by the Transport and Infrastructure Council (the council) in 2016 and the then Standing Council on Transport and Infrastructure (SCOTI) in 2013.

In November 2016 the council agreed to recommendation 8 in the NTC's policy paper, *Regulatory reforms for automated road vehicles*:

> **Recommendation 8**: That the NTC develops options to manage government access to automated vehicle data, having regard to achieving road safety and network efficiency outcomes and efficient enforcement of traffic laws, balanced with sufficient privacy protections for automated vehicle users.

In 2013 SCOTI agreed in principle to stronger privacy restrictions for government access to C-ITS data (if C-ITS data was deemed to be personal information). SCOTI approved the following recommendation in the NTC's policy paper *Cooperative Intelligent Transport Systems Final Policy Paper*:

> **Recommendation 4**: In the event that individuals can be reasonably identified from the safety data message broadcast by C-ITS devices, that specific legislative protections are developed to define in what circumstances organisations that are exempt from compliance with privacy principles, including enforcement agencies, may access C-ITS personal information.

An independent privacy impact assessment prepared in August 2016 on behalf of Austroads found that data messages broadcast by vehicles in C-ITS should be treated as personal information (van Dijk, 2017, p. 5). The privacy impact assessment concluded, consistent with the position in the European Union (EU),[12] that the broadcast messages exchanged by

[12] Refer to the discussion in section 8.2.3 of the UNSW report.

vehicles are personal information. This meant that the pre-condition in recommendation 4 had been satisfied and further work needed to be done.

1.6.2 Broader national reform program for automated vehicles

The regulating government access to C-ITS and automated vehicle data work is part of the NTC's broader automated vehicle national reform program for the safe commercial deployment and use of automated vehicles. Other elements of the NTC's national reform program include:

- **In-service safety for automated vehicles**: Ministers have agreed to an approach for the safety assurance of automated vehicles at first supply. The NTC is now developing options for regulatory reforms to assure the safe operation of automated vehicles while they are in-service. This work examines:
  - the role of different parties in in-service safety of automated vehicles including ADSEs, manufacturers, repairers, owners and others
  - any additional safety duties that should apply to these parties
  - the institutional and regulatory arrangements to support these duties.

  We released a consultation regulation impact statement for public consultation in July 2019.
- **Motor accident injury insurance and automated vehicles**: We developed options to support the deployment of automated vehicles, with the aim of ensuring that crash victims are no worse off in accidents involving automated vehicles. We submitted recommendations to the council in August 2019.[13]

The NTC is collaborating closely with the Commonwealth, Austroads and the state and territory governments to ensure an integrated regulatory system can be delivered for deploying vehicles with automated functions.

Figure 4 illustrates the existing end-to-end regulatory process and the initiatives underway at each stage by each agency or entity to prepare for automated vehicles.

[13] The policy paper *Motor Accident Injury Insurance and Automated Vehicles* can be accessed at https://www.ntc.gov.au/current-projects/motor-accident-injury-insurance-and-automated-vehicles/?modeId=1064&topicId=1166.

Figure 4. Creating an end-to-end post-trial regulatory system for automated vehicles

Stage	Initiative	Owner	Status
Import and manufacture	UN harmonization of vehicle standards	Commonwealth	Ongoing
	Safety criteria for first supply of automated vehicles	Commonwealth	Ongoing
Registration and licensing	Framework for registration and licensing of automated vehicles	Austroads	Ongoing
	Integrating advanced driver assistance systems in driver education	Austroads	Ongoing
On the road	In-service safety for automated vehicles	NTC	Ongoing
	Operation of automated heavy vehicles in remote and regional areas	Austroads	Complete
	National enforcement guidelines for automated vehicles	NTC	Complete
	Regulating government access to C-ITS and automated vehicle data	NTC	Ongoing
	Review of motor accident injury insurance and automated vehicles	NTC	Ongoing
Infrastructure	Infrastructure for automated vehicles: freeways and highways, traffic signs, line markings	Austroads	Ongoing
	Road authority data for connected and automated vehicles	Austroads	Ongoing

1.6.3 Interdependencies

Ministers have agreed that ADSEs must show how they meet a set of safety criteria and obligations at first supply. One such criterion is data recording and sharing.[14] This criterion requires ADSEs to record and provide certain data (such as crash data and data about who is in control of a vehicle) to relevant parties (including law enforcement and other government agencies).

While the criterion requires ADSEs to record and share data, it does not provide a power for government agencies to access the data. The NTC will consider specific legislative powers for government to access relevant automated vehicle data as part of the compliance and enforcement options for automated vehicles. The outcomes from this policy paper will guide the development of these broader automated vehicle reforms.

[14] More information about the criterion can be found in the NTC's *Safety assurance for automated driving systems: decision regulation impact statement* (November 2018).

Any new powers and obligations relating to data recording and sharing introduced as part of the automated vehicle national reform program (including any compliance and enforcement options) will affect the analysis of Australia's information access framework.

1.7 Relevant developments on data privacy

A range of recent reports and legislative amendments in Australia relating to data and privacy have informed the analysis in this paper. These are detailed in Appendix A and cover:

- the Australian Government's response to the Productivity Commission Data Availability and Use Inquiry
- recent reports on de-identification
- privacy protections introduced under the My Health Record system.

Information about international approaches to data privacy can be found at Appendix B and in the UNSW report in sections 8 and 9.

2 Scope and assumptions

Key points

- The scope of this paper is to examine whether additional privacy protections for government collection and use of data generated by C-ITS and automated vehicle technology are needed. The paper also recognises the benefits of, and the need for an appropriate authorising environment for, government access to this data.
- The NTC adopts the following assumptions:
  - Because of the potential for data linking, it is difficult to irreversibly de-identify personal information in most circumstances.
  - Internationally, information access frameworks will remain inconsistent with varying standards around data privacy. Any policy recommendations will closely consider international developments on data privacy.
  - The NTC may propose specific legislative powers to access relevant automated vehicle data as part of in-service safety reform.

2.1 Purpose of this chapter

The purpose of this chapter is to outline:

- the scope of the NTC's regulating government access to C-ITS and automated vehicle data work
- the assumptions adopted by the NTC in carrying out its analysis in the policy paper.

2.2 Scope

In the discussion paper the NTC outlined the scope of this work as limited to examining whether additional privacy protections for government collection and use of data generated by C-ITS and automated vehicle technology are needed.

In the discussion paper we described the following areas as outside the scope of this work:

- Australia's information access framework as it applies to the private sector (for example, consumers' ability to opt out of ADSEs collecting personal information)
- access to automated vehicle data by motor accident injury insurers
- obligations for ADSEs to record and share data generated by automated vehicles, and new powers for government agencies to access this data (including for law enforcement purposes to determine who is in control of an automated vehicle)
- access to automated vehicle data by consumers for disputing liability (for example, data showing which party was in control for defending road traffic infringements).[15]

[15] The NTC has previously considered individual access to automated vehicle data for disputing liability. This is reflected within the safety criteria developed for ADSEs to self-certify against when bringing vehicles to market. ADSEs must show how individuals will receive data to dispute liability when the individual makes a reasonable request. It should be noted that consumer access to data for broader reasons is not within the current scope of the NTC's work. Further discussion of the Australian Government's consideration of consumer access to particular data as part of a Consumer Data Right is in Appendix A and section 1.6 of the discussion paper.

2.2.1 Stakeholder feedback

Several stakeholders submitted that the scope outlined in the discussion paper may be too limited and that the NTC should consider broader matters. These matters are detailed below.

2.2.1.1 Benefits of government access to data

We received feedback (discussed throughout the policy paper) that we should consider the benefits of government access to C-ITS and automated vehicle data and broader issues such as the need for an appropriate authorising environment for government access to this data in more detail. For example, Austroads submitted that the NTC 'extend the focus of the discussion paper to *realisation of benefits with privacy safeguarded*'.

State and territory governments have asked the NTC to consider government access and use of C-ITS and automated vehicle data, including for network efficiency and investment purposes. This is further discussed in Chapter 9.

2.2.1.2 Privacy protections for private sector access to data

Some stakeholders suggested that the scope of the work be expanded to consider access to data and privacy protections beyond government to include the private sector (Austroads, DTMR, iMOVE, OIC QLD, PwC Legal, RAC WA[16]).

Deloitte suggested a need to 'clarify the government's role in regulating data collection and usage by the private sector'. TCA submitted that the legislative framework should apply to all parties accessing the data.

A key reason for the suggestion that there is a need to consider private sector access to data was the view that a holistic approach is required. As outlined in section 2.2.2.1, the overall privacy framework in Australia already differentiates between government and the private sector. The private sector is uniformly regulated under the Australian Privacy Principles (APPs), whereas government agencies are covered by inconsistent jurisdiction-based privacy regulation.

Submissions from Transurban and an automotive manufacturer expressed the view that privacy protections for the private sector are sufficiently covered through the APPs. The automotive manufacturer suggested that imposing additional privacy regulation only on the automotive industry would place unnecessary regulatory compliance requirements on an industry already sufficiently covered by the APPs.

Some submissions suggested that access by insurers and how such data is shared between government and insurers should be considered (RACQ, IAG). A government agency submitted that a consistent baseline approach for data access by government and insurance agencies is needed.

Two Information Commissioners (OIC QLD, OVIC) highlighted that the private sector often partners with government to deliver government services. They suggested that consistent privacy and data security standards should apply irrespective of whether it is the public or private sector accessing the data. IAG submitted that the nature of a government's relationship with its private sector partners and the access third-party private sector entities are given to personal information collected by government is not always clear.

2.2.1.3 Broader consideration of data privacy protection beyond C-ITS and automated vehicle data

Some stakeholders suggested expanding the scope of the work beyond C-ITS and automated vehicle data. PwC Legal and EROAD suggested that existing privacy protections

[16] See Appendix E for a full list of the submitting organisations and their abbreviations.

should be reviewed more broadly rather than limiting the review to C-ITS and automated vehicle data. The Australian Logistics Council submitted that 'a privacy standard that can be universally applied across all applications where data is collected from the transport and logistics sector for statutory and other purposes' should be developed.

2.2.2 NTC conclusions

2.2.2.1 Private sector access and privacy

For the reasons below, we do not propose to expand the scope of this work to focus on the private sector.

- Regulating private sector access to C-ITS and automated vehicle data is outside the NTC's mandate agreed by transport ministers (outlined in section 1.6.1). The NTC's mandate limits this work to regulating government access to C-ITS and automated vehicle data.
- Unlike government agencies, which are covered by inconsistent jurisdiction-based privacy regulation, the APPs apply consistently to private sector entities. The requirement for all private sector entities to comply with the APPs was noted by some stakeholders. In addition, certain exceptions to complying with the privacy principles only apply to government agencies (these law enforcement exceptions are discussed in more detail in Chapter 5 of the discussion paper).
- Concerns about private sector access to data is a much broader issue than automated vehicle policy and regulation. Private sector access to data and its impact on privacy is being considered more broadly by other organisations, most recently by the Australian Competition and Consumer Commission (Australian Competition and Consumer Commission, 2018b).
- The NTC is currently progressing work on motor accident injury insurance and automated vehicles, which considers access to automated vehicle data by motor accident injury insurers.
- The NTC will be developing a compliance and enforcement framework for automated vehicle regulation. It will consider new powers and authorisations for government access to automated vehicle data and accommodate additional privacy protections covering government agencies if necessary. We are not proposing to introduce powers or data access authorisations for private sector entities.

The NTC notes that some stakeholders tied the need to consider the private sector with the increase in public–private sector partnerships. The NTC understands this issue is not limited only to C-ITS and automated vehicles data and is already being addressed by government agencies. Private sector entities working for or on behalf of government may be contractually bound to comply with specific data protection requirements when accessing data from government entities.[17]

In limiting the scope to regulating government access, we are not proposing reforms to current frameworks that regulate private sector access. However, we acknowledge that there may be a public perception that private sector entities delivering services typically provided by government, such as toll road operators, should follow similar requirements to public sector agencies. The NTC will consider this point in developing any reforms in this area.

[17] For example, VicRoads must enter into an information protection agreement with relevant parties before disclosing relevant data to these parties (*Road Safety Act 1986* (Vic) s 90N). Such agreements must cover a range of matters including the purposes for which information is disclosed by VicRoads to the relevant party and an undertaking by the relevant party that the data will be used or disclosed only for that specific purpose.

2.2.2.2 Broader consideration of data privacy protection beyond C-ITS and automated vehicle data

The NTC has a mandate for transport policy reform (and for this work, C-ITS and automated vehicle data) and not a broad privacy advocacy role. Other organisations with a more specific privacy mandate are better placed to consider privacy concerns more holistically.

2.2.2.3 Benefits of government access to data

We have refined the scope of this work to place a stronger emphasis on the benefits of, and the need for an appropriate authorising environment for, government access to C-ITS and automated vehicle data. This refined scope is reflected in the rest of the policy paper.

The scope of this paper is to examine whether additional privacy protections for government collection and use of data generated by C-ITS and automated vehicle technology are needed. The paper also recognises the benefits of, and the need for an appropriate authorising environment for, government access to this data.

The following areas are outside the scope of this work:

- access to automated vehicle data by motor accident injury insurers
- obligations for ADSEs to record and share data generated by automated vehicles, and new powers for government agencies to access this data
- Australia’s information access framework as it applies to the private sector
- access to automated vehicle data by consumers for disputing liability.

2.3 Assumptions in the discussion paper

The NTC adopted the following assumptions in the discussion paper.

1. It is difficult to irreversibly de-identify personal information.
2. Internationally, information access frameworks will remain inconsistent with varying standards around data privacy.
3. The safety assurance system will most likely include a data recording and sharing criterion, and the NTC may propose specific legislative powers to access relevant automated vehicle data.

We sought feedback on whether the identified assumptions are reasonable.

2.3.1 Stakeholder feedback

Assumptions contained in the discussion paper

Irreversible de-identification of personal information is difficult

Stakeholders broadly agreed with the assumption that it is difficult to irreversibly de-identify personal information:

- The AAA highlighted that it may not be possible to de-identify the data because it will most likely be linked with other government datasets.
- The TCA submitted that, in their experience in managing transport telematics data, it is inherently difficult (if not impossible) to permanently and irreversibly de-identify such data.
- OVIC noted that it is unlikely that a single technique can securely de-identify all types of data and that there is an inherent risk of re-identification.

- In supporting the assumption, DoT WA referred to 'the significant breadth and depth of data collected as well as the fact that data collected will contain many identifiers'.
- OAIC submitted that de-identification will depend on the context. To de-identify data effectively, entities must consider not only the data itself but also the environment the data will be released into.

This view was not shared by DTMR, who submitted that governments could use aggregated data for many legitimate uses, and this would be de-identified and not personal information.

International frameworks will remain inconsistent

Many stakeholders agreed with the assumption that international access frameworks will remain inconsistent with varying standards around data privacy:

- A government agency submitted that information access frameworks are different for each country, with no generally agreed framework to guide Australia's approach.
- DoT WA noted that international approaches vary significantly, and there is no consistent international approach to follow.
- Brisbane City Council submitted that identifying the inconsistency in international frameworks 'should ensure that the NTC's approach is best suited to the Australian national context'.

Some submissions emphasised the need to closely follow developments in international approaches and suggested aligning with them where appropriate (AAA, Austroads, TCA, Transurban, two government agencies, an automotive manufacturer). EROAD stated that the EU General Data Protection Regulation (GDPR)[18] is the 'best reference model'. The DTMR submitted that departures from international approaches will act as a barrier to adopting C-ITS and automated vehicle technology in Australia.

The safety assurance system will include a data recording and sharing criterion

Stakeholders broadly agreed with the assumption that a safety assurance system will most likely include a data recording and sharing criterion and that the NTC may propose specific legislative powers as part of the safety assurance system work. DoT WA and the DTMR supported the need for legislative powers to enable access to automated vehicle data. The Truck Industry Council disagreed with assumption 3, submitting that the UN is developing data recording and sharing requirements; therefore, the NTC should not develop unique Australian requirements.

The problem statement

Many submissions supported the problem statement's position that there are risks that privacy concerns about government access to C-ITS and automated vehicle data will be a barrier to take-up and use of the technology in Australia:

- The FCAI submitted that the collection and use of C-ITS and automated vehicle data by government for secondary purposes (a purpose that is not the original purpose of collection) is a major privacy challenge for consumers that could discourage take-up of the technology.
- A government agency considered that a failure to properly address privacy concerns regarding government access to or use of C-ITS and automated vehicle data could present barriers to the uptake and use in Australia.
- iMOVE and the TCA submitted that adopting the technology will be impeded if the community is concerned about risks to privacy.

[18] See Appendix B for an explanation of data protection in the EU and the GDPR.

- The ATA, the Law Society of New South Wales and Squire Patton Boggs submitted that government collection, use and disclosure of C-ITS and automated vehicle data must be appropriately limited to ensure consumer buy-in and avoid delayed take-up.
- Squire Patton Boggs highlighted that the Australian public has recently shown a general unwillingness to surrender its privacy, noting the national unease with the My Health Record. Squire Patton Boggs stated that while consumers may tolerate global technology companies collecting large amounts of personal data, government collection of C-ITS and automated vehicle data raises new concerns.
- OVIC highlighted that strong privacy protections will help build community trust and confidence in government collection and use of C-ITS and automated vehicle data and have a positive impact on automated vehicle uptake.

Some stakeholders considered that there was an untested assumption in the problem statement that government access to C-ITS and automated vehicle data will be a barrier to adoption.

- The DTMR submitted that private sector access may be a greater barrier to uptake than government access.
- DoT WA stated that there is a lack of evidence to suggest that government data access will be a barrier.
- The IAG stated that Australians are willing to accept some curtailment of their privacy in favour of law and order and insurance.
- The DITCRD submitted that safety, cybersecurity and liability are greater community concerns than privacy.

2.3.2 NTC conclusions

Assumptions contained in the discussion paper

Irreversible de-identification of personal information

The submissions we received on the difficulty of de-identifying personal information are largely consistent with initial stakeholder consultation described in the discussion paper. The NTC's assumption highlights the difficulty of irreversible de-identification because of the potential for data linking, rather than suggesting that de-identification is never possible. The NTC has amended the assumption to clarify this point. The NTC recognises that fully aggregated data is unlikely to be personal information.

International frameworks will remain inconsistent

The NTC recognises the importance of Australia aligning with international standards relevant to regulating government access to C-ITS and automated vehicle data. The NTC's second assumption recognises the inconsistency in current international information access frameworks. We propose that we do not follow a particular international approach at this stage, suggesting that we align with international approaches where appropriate. For clarity, we have amended the assumption to recognise the need to align with international standards.

The safety assurance system will include a data recording and sharing criterion

The council decided in November 2018 that ADSEs will be required to self-certify against safety criteria the first time an ADS is supplied to the market. The safety criteria include a data recording and sharing criterion. This element is now a fact rather than an assumption. The NTC is considering the in-service element of this obligation as part of its work on the in-service safety of automated vehicles. The NTC will also consider any specific legislative powers as part of that work and not within this policy paper.

The problem statement

While some stakeholders suggested there is a lack of evidence that government access will be a barrier, numerous stakeholders agreed there is a need to appropriately limit government access to ensure consumer acceptance. Many stakeholders noted recent issues with government access to data, such as the My Health Record, causing concerns for Australians. The NTC considers there is reasonable evidence to support that there is a risk that privacy concerns about government access will be a barrier to take-up.

We recognise that privacy is just one of several community concerns about C-ITS and automated vehicles. We are aiming to address all issues that may be barriers to take-up, including privacy.

The NTC adopts the following assumptions for this policy paper:

- Because of the potential for data linking, it is difficult to irreversibly de-identify personal information in most circumstances.
- Internationally, information access frameworks will remain inconsistent with varying standards around data privacy. Any policy recommendations will closely consider international developments on data privacy.
- The NTC may propose specific legislative powers to access relevant automated vehicle data as part of in-service safety reform.

3 Data generated by current and future vehicle technology

Key points

- Stakeholders broadly agreed with the NTC's overview of current vehicle technology and C-ITS and automated vehicle technology. Based on stakeholder feedback we:
    - amended the reference from 'V2V/V2I communication' to 'V2X communication'
    - included a range of more specific current and anticipated technologies as examples within the broader categories
    - recognised that in automated vehicles certain technologies, including electronic control units, may be referred to using different terminology.
- The NTC's overview is illustrative only and is likely to change as the technology evolves.

3.1 Purpose of this chapter

The purpose of this chapter is to:

- describe and respond to stakeholder feedback on data generated by current vehicle technology and anticipated C-ITS and automated vehicle technology
- provide an overview of data generated by current vehicle technology and anticipated C-ITS and automated vehicle technology that highlights the main differences between current and future vehicle technology to assist with identifying and analysing any new privacy challenges arising from government access to C-ITS and automated vehicle data.

3.2 Overview of data generated by current and future vehicle technology

The NTC's overview of technology in vehicles in this chapter covers vehicle technology (both current and future) capable of generating and recording data. In the discussion paper, the NTC identified three C-ITS and automated vehicle technologies that may create new privacy challenges and are likely to be widespread in future vehicles. These are <u>underlined</u> in the following list:

- **Data supporting operation of advanced driver assistance and automated functions**
    - Sensor input units
    - Electronic control units
- **Image data**
    - Video recording external to the vehicle
    - <u>Video recording internal to the vehicle</u>
- **Crash and vehicle control data**

    - Event data recorders (or similar devices)
- **Location and route data**
    - Navigation systems
    - V2V/V2I communication
- **Data from biometric, biological or health sensors**
    - Biometric, biological or health sensors
- **Audio data**
    - In-cabin microphones
    - External microphones

We sought feedback on whether we accurately captured current vehicle technology and anticipated C-ITS and automated vehicle technology and the data produced by it.

3.3 Stakeholder feedback

3.3.1 Data and information

Several stakeholders submitted that there is a distinction between data and information, suggesting that the NTC make this distinction clear (AAA, FCAI, Truck Industry Council, a government agency).

The AAA, FCAI and Truck Industry Council referred to the definitions in the Productivity Commission's 2017 *Data Availability and Use Inquiry report*, which identified that data refers to unorganised material, whereas information is generally organised material.

The FCAI and Truck Industry Council further stated that their submissions to the NTC's discussion paper were based on it focusing on government access to data, not information.

3.3.2 Current vehicle technology and C-ITS and automated vehicle technology

Many stakeholders, including the AAA, Australian Motorcycle Council, Brisbane City Council, Calibre and DoT WA, considered that the discussion paper accurately captured current vehicle technology and C-ITS and automated vehicle technology.

Several stakeholders, including those that broadly agreed with the NTC's overview, suggested including additional technology data sources (AAA, Calibre, FCAI, RACQ, RAC WA, Transurban, Truck Industry Council, a government agency). In section 3.4 we explain how we have refined the overview of technology in vehicles in this paper to reflect stakeholder feedback.

Brisbane City Council submitted that the NTC should also consider infrastructure data and data on kerbside usage.

A government agency submitted that C-ITS data should be limited to data from vehicles and not include data from roadside devices. The government agency also suggested limiting automated vehicle data to data that directly supports automated driving.

The AAA submitted that the NTC may have overstated the extent to which C-ITS and automated vehicle technology may be used. Deloitte and the RAC WA stated that current vehicles already generate and record data but did suggest that C-ITS and automated vehicle technology would allow for larger amounts of new data to be generated and stored.

3.3.3 Categorisation of C-ITS and automated vehicle data

Two submissions suggested alternative categorisations of C-ITS and automated vehicle data.

A government agency suggested that relying on the following three categories would better assess data collection issues:

- vehicle data broadcast to an ad-hoc network
- vehicle data communicated to a telecommunications network
- vehicle data that is stored.

Austroads similarly suggested that relying on the following three categories more closely aligns with how access to data would occur and the controls in place to safeguard privacy:

- data broadcast from a vehicle over open one-to-any channels
- data provided by a vehicle over private wireless methods
- data that can be accessed only by physical connection into the vehicle.

3.4 NTC conclusions

3.4.1 Data and information

Based on feedback from stakeholders, we generally use the term ‘data’ rather than ‘information’ in this paper. We continue to use ‘personal information’ and ‘sensitive information’ because these are terms defined in legislation.

3.4.2 Overview of vehicle technology and categorisation of C-ITS and automated vehicle data

We have updated the overview of technology provided in the discussion paper to reflect stakeholder feedback by:

- amending the reference from ‘V2V/V2I communication’ to ‘V2X communication’ to recognise that vehicles may communicate through C-ITS devices with components of the transport network other than vehicles, roads and infrastructure (however, we note that the NTC’s scope is focused on data generated by vehicles rather than the data generated by devices that interact with a vehicle)
- including a range of more specific current and anticipated technologies as examples within the broader categories
- recognising that in automated vehicles certain technologies, including electronic control units, may be referred to using different terminology.

These amendments are reflected in Table 2, which provides the NTC’s updated overview of technology in vehicles. This overview is illustrative only and is likely to change as the technology evolves. It is intended as a starting point for considering what is different about C-ITS and automated vehicle technology. It highlights that C-ITS and automated vehicle technology would allow for larger amounts of new data to be generated and stored.

Some submissions suggested including vehicle-to-mobile-device connectivity and mobile phone applications to enable automated vehicle on-demand capabilities. Our focus is on vehicle technology capable of generating and recording data. In the discussion paper we did not include sim cards in the vehicle as a separate technology, but rather as inputs into a vehicle’s navigation or infotainment system. Personal mobile phone devices fall into a similar category. For completeness, connection to a personal mobile phone device has been included as part of the description of navigation systems in Table 2. Infrastructure data and data on kerbside usage is similarly separate to vehicle technology capable of generating and recording data.

The NTC recognises there are alternative ways to categorise the data. We have updated Figure 3 in Chapter 1 (repeated as Figure 5 in Chapter 6) to incorporate the categories proposed by Austroads by including them within the first box representing C-ITS and automated vehicle data. We do agree that the way data can be accessed (for example, whether it is broadcast to all, broadcast in a private network or can only be accessed from a stored source) could make a difference to a government's ability to collect data in the first instance. However, it should be noted that categorising the data in this way focuses on the ease of initial access to the data from a practical perspective. Access safeguards in the technology itself is a related but separate question to whether governments can legally collect, use and disclose personal information. The NTC's overall categorisation highlights the main differences between current and future vehicle technology and assists in differentiating between more and less sensitive data.

Table 2. NTC's updated overview of technology in vehicles

Technology	Current vehicle technology	C-ITS and automated vehicle technology
Data supporting the operation of advanced driver assistance and automated functions		
Sensor input units (sensors, radars, cameras, Lidar)	Advanced driver assistance systems rely on sensors including ultrasonic sensors, external cameras and radars to recognise obstacles. External cameras are discussed under 'Image data' below.	ADSs are likely to rely on technology similar to that used for advanced driver assistance systems but with more widespread utilisation of Lidar technology for object avoidance and mapping, and infrared thermal imaging. Automated vehicles will generally rely on a larger number of higher quality sensors. External cameras are discussed under 'Image data' below.
Electronic control units (or similar devices)	Receive and act on data from sensor input units to record speed, journey distance and driving performance. Can also undertake vehicle self-diagnostic checks and provide warnings about vehicle faults.	Likely to be similar to current vehicles, but will use a wider range of sensor inputs, receive and produce a larger volume of data and require more powerful computers and software. Anticipated technology may be better termed as an 'integrated vehicle management system'.
Image data		
Video recording external to the vehicle (dashboard cameras, external camera input units)	Dashboard cameras capture images of vehicles and parties external to the vehicle. External camera input units can identify external parties and the numberplates of other vehicles in real time.	Likely to be similar to current vehicles, but: ▪ could rely on more cameras with higher resolution and stereo vision ▪ the data produced by external camera input units could be recorded and stored, rather than just identifying external parties and the numberplates of other vehicles in real time.
Video recording internal to the vehicle (in-cabin cameras)	Only utilised to a limited extent for monitoring purposes such as security (for example, taxis) and safety (for example,	Likely to be widespread for driver recognition and to monitor driver alertness and occupant behaviour. This could be used, for example, to determine whether it is safe for the ADS to hand back control to

Technology	Current vehicle technology	C-ITS and automated vehicle technology
	fatigue and distraction monitoring).	the human driver or for security monitoring in fleet vehicles. Could extend to whole-of-cabin video monitoring and recording.
Crash and vehicle control data		
Event data recorders (or similar devices)	Collect crash-related data from the vehicle in the seconds before and during a crash.	Likely to be broadly similar to current vehicles. May collect additional inputs (for example, who is in control of the vehicle) and store data over a longer period (not limited to when a crash occurs). Anticipated technology may be better termed as a 'Data Storage System for Automated Driving'.
Location and route data		
Navigation systems	Generally rely on a global navigation satellite system (GNSS) receiver, an electronic compass and/or connection to the mobile network (for example, through a sim card installed in the vehicle or via connection to a personal mobile phone device). Data received allows the vehicle route to be calculated and compared with the vehicle's current location throughout the journey. Past routes could be stored and retrieved later.	Likely to be similar to current vehicles, but automated vehicles may require greater resolution. May also rely on emerging technologies such as accelerometers, laser gyro and wi-fi and 4G/5G receivers to replace or enhance the GNSS signal.
V2X communication	Not contained in current vehicles.	Enables components of the transport network to data communicate and share real-time information including data on vehicle movements, traffic signs and road conditions. Vehicles may share speed, location and vehicle type among other attributes. Such data can be received by roadside equipment and pedestrian mobile phones.
Data from biometric, biological or health sensors		
Biometric, biological or health sensors	Unlikely to be contained in current vehicles, except for limited fatigue monitoring.	Automated vehicles may rely on these to: ▪ monitor driver alertness and behaviour to assist with determining whether it is safe for the ADS to hand back control to the human driver ▪ recognise drivers and occupants (such as through fingerprints or facial recognition) to customise the driving experience.

Technology	Current vehicle technology	C-ITS and automated vehicle technology
Audio data		
In-cabin microphones	Allow voice commands (and voice recognition systems) to operate some infotainment system functions.	Likely to be similar in nature to current vehicles. Automated vehicles could use audio inputs to, for example, activate automated functions.
External microphones	Unlikely to be contained in current vehicles.	Automated vehicles could respond to inputs from external microphones, for example, someone loudly shouting ‘stop’, horns or sirens.

4 Benefits of government access to C-ITS and automated vehicle data

Key points

- Government access to C-ITS and automated vehicle data would inform and enhance decision making in areas including law enforcement, traffic management and road safety, as well as in infrastructure and network planning.
- The benefits of government access to this data need to be balanced with the privacy of the individuals using the technology.

4.1 Purpose of this chapter

The purpose of this chapter is to:

- outline the need for, and benefits of, government access to C-ITS and automated vehicle data
- discuss how the benefits gained from government access must be balanced with the privacy of individuals using the technology.

4.2 Overview of benefits of government access to data

Data generated by vehicle technology will inform and enhance government decision making. Data is essential for service delivery, and the economic benefits of data can be realised when it informs individual, business and government decision making (Productivity Commission, 2017).

In the discussion paper we identified three main categories where C-ITS and automated vehicle data could inform and enhance government decision making:

- law enforcement
- traffic management and road safety as part of network operations
- infrastructure and network planning as part of strategic planning.

We also noted that there may be other applications and benefits from government accessing this data. These included the broad safety, security, environmental and transport efficiency objectives of government.

We suggested that it is important to balance any potential improved decision making and public value with sufficient privacy protection for C-ITS and automated vehicle users. This will ensure government collection and use of data does not act as a barrier to the take-up of C-ITS and automated vehicle technology.

4.2.1 General stakeholder feedback

4.2.1.1 Benefits of government access to data

Many stakeholders agreed with the three main categories we identified where C-ITS and automated vehicle data would inform and enhance government decision making (AAA, Australian Motorcycle Council, Brisbane City Council, EROAD, Law Institute of Victoria, PwC Legal, RACQ, Transurban, a state government).

We discuss specific stakeholder feedback on these three categories in section 4.3.

4.2.1.2 Balancing the benefits of government access with the privacy of individuals

A strong theme emerging from submissions was the need to balance the benefits of government access to data with the privacy of individuals using C-ITS and automated vehicle technology. The importance of this balance was explicitly noted by many stakeholders (Austroads, Department of State Growth Tasmania, EROAD, iMOVE, Infrastructure Victoria, ITS Australia, Law Institute of Victoria, Law Society of NSW, NHVR, NSW Young Lawyers, RAC WA, a road transport agency).

Stakeholders had different views on how to strike this balance. Some, such as NSW Young Lawyers, emphasised the importance of individual privacy. Others, such as Austroads, DTMR and iMOVE, emphasised the community and societal benefits government access to vehicle technology data could offer.

Some stakeholders considered that government should only be able to access data for uses that would benefit the general public, in particular for public safety outcomes (ATA, Australian Motorcycle Council, Maurice Blackburn Lawyers). EROAD and Maurice Blackburn Lawyers considered there should be an external review process to determine whether access to data is in the general public's best interest.

Submissions from the ATA, the Law Institute of Victoria and Maurice Blackburn Lawyers specified outcomes data should not be used for. These included:

- data collection for insurance purposes
- the commercialisation of data
- covert law enforcement or surveillance
- data matching by government departments seeking to achieve outcomes unrelated to safety, policy or planning outcomes (for example, by the Australian Taxation Office).

Maurice Blackburn Lawyers noted similarities between the issues the NTC is considering and those considered by the Senate Inquiry into the My Health Record System.[19]

The FCAI and Truck Industry Council proposed that government should only be able to access, collect and use data that provided a net public benefit. For example, the FCAI suggested that C-ITS data will provide significant benefits to traffic management and road safety, but if the same data were used for traffic law enforcement this could discourage take-up of the technology. This would lead to slower introduction and delayed road safety and traffic management benefits.

EROAD also referenced the 'net benefit' concept, stating that government access to data for motives that may include convenience, circumventing controls or cost-effectiveness should only occur where the private costs are equal to or less than the public benefit created by this access.

OVIC stated that strong consideration should be given to the problem that government is trying to address by accessing C-ITS and automated vehicle data. Data should not be collected and used simply because it is accessible – the necessity of collecting it must be justified.

The OIC QLD considered that unanticipated uses for vehicle technology data are likely to emerge. Frameworks need to be sufficiently robust and transparent to accommodate these unanticipated uses.

NSW Young Lawyers considered that, at this stage, privacy concerns outweigh the need for government access to C-ITS and automated vehicle data. The impact of the use of this data

[19] The final Senate Inquiry report into the My Health Record System can be accessed at: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Community_Affairs/MyHealthRecordsystem/Final_Report.

on individual privacy must first be ascertained, particularly given the sensitive nature of data that can be generated by automated vehicle and C-ITS technology.

4.2.1.3 What type of data should government have access to?

Some stakeholders expressed views on the type of data that government should be able to access.

The FCAI and Truck Industry Council considered that the data that government will collect should be defined.

Some submissions focused on placing limitations on the type of data government should be able to use for law enforcement:

- The Truck Industry Council did not support the use of 'real time' data or retrospective data for law enforcement activities such as speeding and only supported the use of de-identified data.
- The RACQ submitted that data use 'should be restricted to post-event law enforcement and investigations … and not extend to constant real-time monitoring for traffic infringement purposes'. It suggested that where a speed camera has already identified a speeding event, using data to determine who was driving would be appropriate. Conversely, using C-ITS data alone to identify a speeding event would not be appropriate. This type of monitoring would deter public uptake of C-ITS.
- A road transport agency suggested there could be a case for putting restrictions on government use of V2X data for enforcement purposes because it might deter uptake and the data might not be of an evidentiary standard.

Some submissions considered whether government would need access to data that identifies an individual:

- A road transport agency noted that, for many uses, road authorities would be unlikely to need to identify individuals and that data should be de-identified and aggregated where possible.
- The RAC WA noted that access to identifiable data should be limited, supported by robust due processes and appealable when individuals considered their privacy had been breached.
- The TCA observed that it was not necessary for government to access raw data. They also considered the approach taken could be guided by international developments and local assessments.

4.2.1.4 Who should be able to access data?

Some stakeholders expressed views on the need to define 'government' clearly and which agencies within government should be able to access data.

The FCAI and Truck Industry Council suggested that the term 'government' needs to be clearly defined when considering access to C-ITS and automated vehicle data. The Truck Industry Council queried whether a private toll road operator should have similar rights of access to data for traffic management planning as a state government road manager would on a state-owned public road.

The RAC WA proposed that data access could deliver benefits not only for roads and road agencies but for all modes of transport, all users of transport systems and across all tiers of government. It suggested that V2I and V2X data may be important to other areas of government and that this should be considered in determining the purposes and uses for data collection as well as the government agencies permitted access for specific reasons.

RAC WA suggested that the permitted uses and access to data should in turn be made clear to transport users.

A government agency raised the possibility that government agencies may not have the skills to analyse the data they have access to. This could impede government's ability to rapidly identify and respond when data collection had resulted in a privacy breach.

Squire Patton Boggs suggested reducing the amount or type of data that can be accessed by local government might be a positive given the costs and risks associated with managing this type of data.

4.3 Categories where data could enhance government decision making

Some stakeholders suggested additional categories or amendments to the three categories we identified where C-ITS and automated vehicle data could enhance government decision making. We used this feedback to develop five main categories where C-ITS and automated vehicle data could inform and enhance government decision making:

1. law enforcement
2. automated vehicle safety
3. network operations – traffic management and road safety
4. strategic planning – infrastructure and network planning
5. other purposes (including public safety, environmental protection and mobility).

The next sections discuss these five categories and the stakeholder feedback we received.

4.4 Category 1: Law enforcement

In the discussion paper we proposed that data from C-ITS and automated vehicle technology could be useful for road traffic law enforcement. Suggested possible uses included:

- identifying whether a human driver or ADS was in control of an automated vehicle at the time of a crash or breach of a road traffic law
- determining if 'fallback-ready users' in automated vehicles are sufficiently vigilant to respond to ADS requests to take back control (image data internal to the vehicle and data from biometric, biological or health sensors can be used to monitor driver attention and alertness)
- providing evidence of current traffic offences such as speeding.

We also identified data that could be useful for law enforcement outside of road transport:

- location data of a suspect in a terrorism investigation
- video recordings of criminal behaviour occurring inside a vehicle
- video recordings and data from biometric, biological or health sensors (such as indicators of stress) as evidence of a person's state of mind at a point in time.

4.4.1 Stakeholder feedback

Many stakeholders agreed that law enforcement was one of the main categories where government access to C-ITS and automated vehicle data could inform and enhance government decision making (AAA, Brisbane City Council, Law Institute of Victoria, NHVR, road transport agencies).

The DTMR supported clear statutory collection mechanisms for roadside enforcement to access information to determine liability for traffic offences and crashes quickly and outside of court processes. Another road transport agency and the Law Institute of Victoria also supported a requirement for enforcement agencies to have the ability to capture data that shows who is in control of an automated vehicle at any point in time.

Other suggested uses for C-ITS and automated vehicle data were:

- assessing compliance with road access permissions
- detecting people using devices while driving (for example, mobile phones)
- non-transport-related law enforcement such as investigating assaults or property damage (Brisbane City Council), locating missing children and national security (Calibre, a state government, a territory government).

4.5 Category 2: Automated vehicle safety

In the discussion paper we suggested that entities that are responsible for the safety assurance system for automated vehicles may require access to automated vehicle data. This would be required to investigate contraventions of an ADSE’s obligations or for monitoring or auditing an ADSE.

In November 2018 ministers agreed that an ADSE must self-certify against a set of safety criteria and obligations before their ADS will be approved at first supply to the Australian market. One of the obligations centres on data recording and sharing. The ADSE must record data relevant to enforcing road traffic laws and the general safe operation of the ADS (including data relating to crashes). Recorded data must be provided by the ADSE to relevant parties (such as police, insurers, road agencies and consumers) as necessary and in compliance with requirements under the *Privacy Act 1988* (Cth).

This places an obligation on ADSEs to record and share data; however, it does not provide a power for government agencies to access this data. We will consider specific legislative compliance and enforcement options for automated vehicles in a later phase of work.

4.5.1 Stakeholder feedback

The DTMR considered clear legislated collection mechanisms for roadside enforcement are necessary, and this needs to be considered as part of obligations placed on ADSEs under a safety assurance system. Its submission suggested a risk to the security and safety of C-ITS and automated technologies if government did not have access to provide appropriate oversight of technical platforms. The DTMR also suggested an emerging consensus that fully automated vehicles (SAE level 5) will need to be connected with other users and infrastructure. Therefore, it suggested that placing limits on connected data sharing risks fully automated vehicles being unlikely beyond limited use cases or applications.

The DTMR and Law Institute of Victoria observed that it is important for insurers to be able to access C-ITS and automated vehicle data to determine liability for crashes.

The Australian Motorcycle Council and Maurice Blackburn Lawyers submitted that insurer access to data for commercial purposes is not appropriate. Access to data for insurers is outside the scope of this policy paper but is being considered in other areas of our automated vehicle reforms.

4.6 Category 3: Network operations – traffic management and road safety

In the discussion paper we proposed that C-ITS and automated vehicle data could be useful for traffic management and road safety as part of network operations. For example:

- Road management agencies can use real-time C-ITS data to manage network congestion, traffic management and traffic signal phase timing in response to changing traffic conditions or traffic incidents.
- Road management agencies could use data from connected vehicles about the weather, road conditions and structural assets and share the data with other road users to manage safe operating conditions (for example, to notify users of severe weather and emergency conditions) (Weeratunga & Somers, 2015).

4.6.1 Stakeholder feedback

A number of stakeholders agreed that network operations was one of the main categories where government access to C-ITS and automated vehicle data could inform and enhance government decision making (AAA, ATA, Austroads, Brisbane City Council, DTMR, FCAI, Infrastructure Victoria, Law Institute of Victoria, RACQ, Truck Industry Council, two road transport agencies).

The AAA considered that government agencies using real-time data to manage traffic and improve the efficiency of existing assets would have flow-on environmental and fuel-saving benefits.

Some stakeholders gave specific examples where C-ITS data (specifically vehicle-to-infrastructure data) could benefit traffic management. Examples included traffic light phasing, direct notification from vehicles of breakdowns, and data showing where road segments are nearing capacity.

A road transport agency noted that there were likely to be some future traffic management uses where vehicle identification would be important. For example, C-ITS applications could enable priority at intersections for emergency vehicles or heavy vehicles requesting traffic light phasing. The FCAI considered the use of traffic data would only be appropriate where collected, de-identified and used by government infrastructure owners to improve network efficiency and safety.

4.7 Category 4: Strategic planning – infrastructure and network planning

In the discussion paper we suggested that C-ITS and automated vehicle data could be useful for strategic planning relating to infrastructure and network investment. Governments could use C-ITS data to consider vehicle interactions with the road environment and identify areas to prioritise for future road investment.

4.7.1 Stakeholder feedback

Some stakeholders agreed that strategic planning was one of the main categories where government access to C-ITS and automated vehicle data could inform and enhance government decision making (AAA, Brisbane City Council, DTMR, Law Institute of Victoria, RACQ TCA).

The Australian Logistics Council noted its support for developing a freight observatory that would collect data to assist public and private decision-makers in policy and investment decisions. However, they noted that industry required assurance that data would be collected independently of government and for statistical purposes only.

4.8 Category 5: Other purposes

4.8.1 Stakeholder feedback

Stakeholders identified a range of other possible reasons for government access to data, which are described below.

Wider public safety outcomes

A state government and a territory government described potential road safety benefits from access to data that identified 'near misses', dangerous driving, damaged infrastructure or relevant data from the site of an emergency.

The DTMR considered that limiting data sharing could mean that the estimated road safety benefits (reduction in crashes) of connected and automated vehicles would not be realised.

Environment

A government agency considered data could be used by government for environmental scanning. Examples included measuring environment and weather data, and tracking native, endangered or feral wildlife by using data indicating a collision between a vehicle and an animal.

Road pricing

DoT WA suggested that C-ITS and automated vehicle data could be used for revenue collection or demand management purposes – for example, road user charging or congestion charging for empty vehicle travel.

Mobility

Deloitte noted that there were opportunities for data to be used for commercial applications in both the government and private sectors, in particular for improving transport services and mobility options for customers. Similarly, DoT WA noted private sector access to government data could facilitate third-party services such as affordable mobility services. It also noted that data could feed into existing open data sources that are used by third parties for commercial, research or other purposes.

Infrastructure Victoria indicated that more open, real-time data on government transport systems would help to promote transport system efficiency, fair market competition, integration, consistency and user privacy.

4.9 Need for further examination of 'use cases'

The DTMR submitted that restrictions on government access to data should not be considered until a decision is made on what powers are or should be available to support government access. It suggested a comprehensive review of all use cases where data can deliver commercial or public value.

Austroads suggested it would be in the community's interest for the NTC to provide examples that demonstrate how benefits could be realised with privacy remaining safeguarded.

The RAC WA proposed developing a variety of scenarios to assess the effects of access on individual privacy. Deloitte noted that the extent of data collection, access and usage will depend on how the technology is taken up in Australia (for instance, predominantly privately-owned vehicles or a shared fleet). It suggested that the NTC map the effects of these scenarios on data collection, access and usage to better inform the opportunities and challenges of each uptake scenario.

4.10 NTC conclusions

In this chapter we have summarised the reasons why government may want to collect and use C-ITS and automated vehicle data. There are number of benefits that can be gained from government access to this data.

However, it is vital that these benefits are weighed against the privacy of users of the technology. As identified in our problem statement, if consumers are uncomfortable about the data that government can access, there is a risk that this will act as a barrier to take-up and use of C-ITS and automated vehicle technology in Australia.

We acknowledge the feedback received emphasising the need for this balance to be recognised in the future regulatory framework. This balance was weighted by some stakeholders on the side of individual privacy and by others on the side of the benefits of government access. In Chapter 6 we discuss privacy challenges in detail.

We acknowledge views about the advantages of a more comprehensive review of use cases and collation of scenarios. We have engaged with relevant stakeholders directly on this matter. In particular, state and territory governments have asked the NTC to consider government access and use of C-ITS and automated vehicle data, including for network efficiency and investment purposes. Ministers have now made decisions about a new piece of work to be led by the NTC, which is further detailed in Chapter 9.

The outcomes of this policy paper will guide development of our other automated vehicle reforms. This will include considering specific legislative powers for government access to data as part of the compliance and enforcement approach for automated vehicles.

In terms of who should have access to data, we refer to ‘government’ as broadly meaning Commonwealth, state and territory and local governments. However, given their role in road transport, our focus has been on state and territory governments including law enforcement agencies for traffic law enforcement activities. We are not considering government agencies without a role in road transport as part of this phase of work. Private entities, including, for example, toll road operators, are out of scope of the NTC’s work.

5 New privacy challenges of C-ITS and automated vehicle technology

Key points

- C-ITS and automated vehicle technology present new privacy challenges due to the type, breadth and depth of data they generate.
- These privacy challenges may affect individual users of C-ITS and automated vehicle technology because the generated data is likely to be personal information and sensitive information.

5.1 Purpose of this chapter

The purpose of this chapter is to:

- outline the new privacy challenges of government collection, use and disclosure of the type, breadth and depth of data generated by C-ITS and automated vehicles technology
- analyse whether the identified new privacy challenges relate to personal information and sensitive information.

5.2 New privacy challenges of C-ITS and automated vehicle technology

In the discussion paper we outlined the privacy challenges that may arise from government collection, use and disclosure of data generated by C-ITS and automated vehicle technology. These challenges could arise not only because of the type of data generated by the technology but also because of the breadth and depth of data generated. We identified three categories of potential new privacy challenges:

- new data captured by automated vehicle technology
- C-ITS technology allowing for more widespread direct collection of location data by governments
- C-ITS and automated vehicle technology generating a greater breadth and depth of data.

5.2.1 Stakeholder feedback

We sought feedback on whether we had accurately captured the new privacy challenges arising from data generated by C-ITS and automated vehicle technology relevant to government collection and use.

The majority of stakeholders that submitted on this issue considered we had captured the potential new privacy challenges (Australian Motorcycle Council, Brisbane City Council, Calibre, Law Institute of Victoria, Law Society of New South Wales, PwC Legal, RAC WA, Squire Patton Boggs, TCA, Transurban, Truck Industry Council, a state government).

The AAA and EROAD both emphasised that the breadth and depth of data collected and potential for data linking to identify individuals was the most important new privacy challenge. The TCA noted that multiple devices will be used to transmit data in the future (for example, vehicles, roadside devices, smartphones) and that ‘unless the architecture requires it, each application could develop their own privacy and security system under existing principles'.

Brisbane City Council considered that the potential for 'mass surveillance' was the largest barrier to uptake and that this presented a challenge in the Council's dual capacities as an infrastructure owner and law enforcement agency.

The OIC QLD and Law Society of New South Wales noted that privacy challenges will continue to emerge as C-ITS and automated vehicle technology develops and becomes more widespread, and as new uses for data and means of data linking are operationalised.

The DTMR and the DITCRD did not agree that C-ITS and automated vehicle technology gave rise to new privacy challenges. The DTMR considered that existing privacy protections negated the existence of new privacy challenges. The DITCRD considered that current technology already generated the same type of data that C-ITS and automated vehicle technology would. Examples of current technology given included mobile phones, stand-alone and vehicle-installed GPS devices, dashcams and smart watches.

The Tasmanian Department of State Growth acknowledged the new privacy challenges identified but considered existing privacy protections adequately covered these.

Calibre agreed with the new privacy challenges identified but noted that some of the automated technology identified as potentially generating new data such as in-cabin cameras have already been incorporated in vehicles in Australia.

DoT WA and the AAA suggested it would be difficult to anticipate the technology and how it will be used in automated vehicles and that we could therefore not know if the identified privacy challenges would eventuate.

5.2.1.1 Additional privacy challenges and other considerations

The IAG considered that audio data generated from within automated vehicles would present a new privacy challenge because it could contain data as sensitive as data from video recordings.

The RACQ noted that external video cameras in an automated vehicle could be accessed and recorded remotely and that automated vehicles themselves could be remotely operated. These two factors would allow automated vehicles to operate as surveillance devices. The RACQ considered this a new privacy challenge similar to challenges associated with unmanned aerial vehicles.

The FCAI and OVIC considered that using data for secondary purposes is a major privacy challenge – for example, using V2X data for enforcing traffic laws.

Squire Patton Boggs considered that inconsistent approaches to privacy across states and territories presented a privacy challenge.

DoT WA considered more data was required to determine the extent of the privacy challenge. It suggested some privacy challenges could be negated by a vehicle occupant's ability to opt in or out of using technology that shared data and that there would be implications for users with reduced capacity to provide consent.

5.2.2 NTC conclusions

Most stakeholders agreed with our assessment of the new privacy challenges of C-ITS and automated vehicle technology.

Existing technology captures data similar to that generated by C-ITS and automated vehicle technology. However, it is not just the type of data that creates privacy challenges but also the breadth and depth of the data generated. As well, we acknowledge comments that some existing technology like smart watches and fitness trackers may capture some health data.

However, we consider these do not raise the same privacy challenges as automated vehicle and C-ITS technology because it is not clear how governments would be able to access this data, nor is it proposed that government should have a right to access this data.

We distinguish new privacy challenges of C-ITS and automated vehicle data from challenges that already exist. Therefore, we have chosen not to explicitly include audio data from in-cabin microphones as a new privacy challenge because in-cabin microphones in automated vehicles are most likely similar in nature to those already used in current vehicles.

We acknowledge the concerns raised by the RACQ about the potential use of automated vehicles as surveillance devices. We consider that the image data captured would be the same and therefore the technology itself would not present a new privacy challenge.

As with all our proposed automated vehicle reforms, we undertake our analysis in a context of uncertainty. To ensure that regulatory frameworks for C-ITS and automated vehicles are ready in time for deployment, it is necessary to proceed with this work now. We acknowledge the lack of certainty over the extent to which the identified privacy challenges will eventuate. Close engagement with industry and government will continue to guide us in developing our proposals.

The potential new privacy challenges of C-ITS and automated vehicle technology are summarised below.

5.3 Summary of new privacy challenges of C-ITS and automated vehicle technology

5.3.1 New data captured by automated vehicle technology

Some automated vehicle technology (such as in-cabin cameras and biometric, biological or health sensors) is unlikely to be in current vehicles or, if it is, used for specific limited purposes. This technology could generate new data that could be particularly sensitive.

5.3.2 C-ITS technology may allow for more widespread direct collection of location data by government

Technology in current vehicles (for example, electronic control units and navigation systems) can generate speed, location and direction data. Government currently collects this data in a limited way via technology such as road safety cameras, automatic numberplate recognition, infrared traffic loggers and roadside collection devices.

C-ITS technology will generate broadly the same type of speed, location and direction data. However, in the future, government may directly collect this data on a wider basis. Where C-ITS messages broadcast by vehicles are received by government-owned infrastructure or roadside units at connected points across the network, C-ITS technology could allow government to (among other things) collect data from the vehicle to:

- analyse and improve the road network, and for congestion analysis
- improve road safety by analysing driver behaviour
- optimise operation of intersections.

Governments could collect a vehicle’s location, speed and type for the vehicle journey. This would most likely require connected points along the whole vehicle route.

In addition, a C-ITS-equipped vehicle may broadcast a unique identification number (that is pseudonymised and rotated periodically) that is received by roadside equipment.

5.3.3 C-ITS and automated vehicle technology will generate a greater breadth and depth of data

The generation and potential storage of data is likely to increase in the future because:

- automated vehicles will rely on more inputs than current vehicles to perform the entire dynamic driving task (for example, to monitor the driving environment)
- C-ITS and automated vehicle technology will collect and broadcast more data about the safety of vehicle occupants and the road environment
- vehicle technology such as navigation systems and event data recorders, or similar devices that capture who is in control, will probably be integral to the operation of automated vehicles and therefore more widespread. Data from event data recorders and similar devices may be stored for longer periods of time, rather than only in the event of a crash
- external camera input units in automated vehicles will probably move from real-time feed to recording and storing.

Because the generation and potential storage of the data is likely to increase, there is also greater opportunity for data linking by government. Data linking involves the combination of two or more data sources that may not independently identify an individual but may do so when linked. For example, data from sensor input units, electronic control units and electronic data recorders may not identify individuals on its own; however, when combined with data from in-cabin and external cameras and microphones, significant personal information may be revealed. Identifiability is a key concept in determining whether data is personal information.

5.4 Is the data 'personal information' or 'sensitive information'?

Potential privacy challenges for C-ITS and automated vehicle users depend on whether the data can be used to identify an individual. This type of data is called 'personal information.' Privacy law only applies to personal information and 'sensitive information'.

The definition of personal information is similar across all Australian states, territories and the Commonwealth. The relevant concept is whether an individual is reasonably identifiable. Identification may be directly obtained from the collected data – for example, if it reveals an individual's name or address – or from the combination of the data with other relevant datasets the collecting entity has access to.

The definition of 'sensitive information' varies substantively across Australian jurisdictions, and not all states and territories have a sensitive information category in their legislation. Broadly, however, it refers to certain types of information about the individual – for example, their race or ethnic origin, sexual orientation, political opinions or health information.[20] The collection, use or disclosure of sensitive information may need to meet higher standards than other types of information.

In the discussion paper we suggested that the following are more likely to generate personal information and sensitive information than current vehicle technology, either on their own or through linking with other datasets:

- data generated by in-cabin cameras and biometric, biological or health sensors
- location data from C-ITS technology

[20] For states and territories that have a sensitive information category, many exclude biometric and genetic information, and some exclude health information. For example, NSW legislation does not include a sensitive information category, and in Victoria sensitive information only includes information that is also personal information. Some states, for example NSW, also have distinct legislation that governs health information.

- the breadth and depth of data generated by C-ITS and automated vehicle technology.[21]

Stakeholder feedback on the extent to which the three categories of privacy challenges relate to personal information is outlined below.

5.4.1 Stakeholder feedback

A number of stakeholders agreed with the NTC's assessment of personal and sensitive information generated by C-ITS and automated vehicle technology (PwC Legal, RACQ, Squire Patton Boggs, Transurban). Other stakeholders agreed generally that C-ITS and automated vehicle technology will generate more personal and sensitive information (Austroads, DoT WA, Law Institute of Victoria, NSW Young Lawyers, OVIC, a state government, a vehicle manufacturer).

The FCAI considered that data generated by operating the vehicle is personal information. The Truck Industry Council similarly considered that operating the vehicle could potentially identify the driver, other occupants and any cargo or freight. Brisbane City Council proposed that all data with the potential to be personal information should be classified as such.

A number of stakeholders considered that all C-ITS and automated vehicle data should be treated as personal information by default (ATA, EROAD, OIC QLD, OVIC, Squire Patton Boggs).[22] A vehicle manufacturer stated that current privacy legislation would treat the data as personal and sensitive information by default.

Some stakeholders agreed that non-identifying data from C-ITS and automated vehicle technology could be linked to other datasets to create personal information or sensitive information (DoT WA, EROAD, iMOVE, NSW Young Lawyers). A state government noted that if a C-ITS framework was built with a 'privacy by design' focus it might not require identifying information; however, data linking could still create privacy risks and challenges.

Austroads considered standards-based C-ITS data might not need to be treated as sensitive information if protections were adopted to restrict future inclusion of sensitive information. The DTMR similarly suggested that C-ITS system design and security specifications may be sufficient to minimise the likelihood that positioning data could be linked with other data to identify individuals.

Some stakeholders considered that in-cabin audio recordings had the potential to generate personal or sensitive information (ATA, IAG, Squire Patton Boggs, a state government). Squire Patton Boggs noted these recordings could capture discussions regarding an individual's sexuality, race, political or philosophical opinions, religious affiliation, association membership, criminal record or health information. Calibre also noted that data from phone calls could generate personal or sensitive information.

A road transport agency considered that each data type should be considered on a case-by-case basis rather than suggesting all C-ITS and automated vehicle data will be personal or sensitive information. The DTMR considered it is not possible to define what data is personal information until we understand the data produced by these technologies and how it would be collected (for example, if it would be aggregated). Another state government noted that Austroads' work on developing a national framework for C-ITS was likely to provide a greater evidence base to assess categories of information.[23] Transurban encouraged analysis of

[21] The categorisation relies on the definition of sensitive information in the Privacy Act. The variation in the states and territories around inclusion and the definition of sensitive information affect whether the analysis is accurate for an individual state or territory.

[22] For a description of the 'privacy by default' principle see discussion in Appendix B at B.2 on the GDPR.

[23] Austroads' work now encompasses a national framework for all intelligent transport systems rather than only C-ITS. Further detail about this work is in Chapter 9.

new sources of data and context for collection, use and disclosure to determine whether it is or is not personal information.

The DITCRD considered government use of data for purposes such as improving network operational efficiency and infrastructure investment decisions would only require aggregated, de-identified information rather than personal information.

The DTMR indicated that it is unlikely that a single government agency would have infrastructure extensive enough to collect personal information or the ability to capture and retain data at this scale. It considered that even if a vehicle is identified the link between the vehicle and its registered operator would only be held by a limited number of entities. The DTMR considered direct access to data stored in the vehicle as the biggest privacy threat because the information is tied to an identifiable vehicle, whereas wireless access can anonymise the vehicle.

In contrast, OVIC submitted that road and law enforcement agencies have access to a wide range of datasets and the technical capacity to analyse that data. It suggested that methods for de-identification of unit-level records may be insufficient to protect this data.

5.4.2 NTC conclusions

Stakeholders expressed differing views about whether the new privacy challenges identified relate to personal information. Overall, there was strong support for the view that the new privacy challenges arising from C-ITS and automated vehicle technology will relate to data that is personal information. We have retained the discussion paper's categorisation of the new privacy challenges relating to personal information and sensitive information. This categorisation is summarised in section 5.5.

We have taken into account views that all C-ITS and automated vehicle data should be treated as personal information by default while balancing this with views that it was not appropriate at this stage to make this assessment. While this is not specifically reflected in the categories summarised in section 5.5, it affects our recommended approach in Chapter 8 and Appendix D. We also note the importance of public trust and have addressed this in the same sections.

We acknowledge views on the importance of use cases to assess whether data generated will be personal or sensitive information, and more generally that a comprehensive review of use cases would be valuable. As noted in Chapter 4, we have engaged with state and territory governments directly on this matter, and ministers have made further decisions, which are outlined in Chapter 9.

5.5 Summary of personal information and sensitive information likely to be generated by C-ITS and automated vehicle data

5.5.1 Data generated by in-cabin cameras and biometric, biological or health sensors

Data from in-cabin cameras is highly likely to be personal information in all circumstances because it can identify the driver and vehicle occupants. This identification can occur in real time if recognition functions exist, or later when video recording is examined.

In-cabin cameras may also reveal sensitive information. For example, an individual's race or ethnic origin may be deduced from a recording of an individual's facial features, dress or behaviour.

Data from biometric, biological or health sensors is less likely to identify an individual on its own; however, it may do so if it encompasses unique or rare traits. Identifiability increases if it can be linked with other relevant data such as that from cameras and microphones and processed through systems such as pattern recognition software. Therefore, context becomes important, including the capacity of the entity holding the data to analyse it and the availability of other data to aid identification. Operators of road infrastructure and law enforcement and intelligence agencies are likely to have access to a wide range of data and the technical capacity to analyse data; this could aid identifiability.

Biometric, biological or health sensors could also generate sensitive information because it could reveal health information about an individual as well as information that could be used for the purpose of biometric identification.

5.5.2 Location data from C-ITS technology

Data from messages broadcast in C-ITS are likely to require identifiers (security certificates) that are pseudonymised and rotated periodically to protect the identifiability of the data. However, entities that can access other relevant datasets, or a very large number of these messages, could identify a vehicle. Once the vehicle is identified, it can be linked back to the driver or vehicle owner by relying on data such as registration records (van Dijk, 2017).

Location information contained in C-ITS data messages broadcast by vehicles and received by road agencies from government-owned infrastructure or roadside units will probably be personal information (van Dijk, 2017, p. 16). This is because road agencies may collect a large number of these messages and have access to vehicle registration records (and other information) to aid identification.

The UNSW report observed that location information ‘potentially enables a deep set of inferences about a person and therefore could assist in identifying an individual’. Location information from C-ITS technology, including the possibility of tracking a vehicle along its whole route, could reveal information such as a person’s home or work address.

This type of data could also reveal a range of sensitive information about an identified individual based on venues the person visits. The UNSW report stated that location data suggesting ‘a person is having an affair, visiting a known brothel, attending political meetings, attending particular religious or faith venues, or visiting a particular medical specialist’ will be sensitive.

5.5.3 Breadth and depth of data generated by C-ITS and automated vehicle technology

The greater breadth and depth of data likely to be generated by C-ITS and automated vehicle technology would facilitate data linking by government and therefore increase the ease of identification. Data from certain vehicle technologies, such as sensor input units and event data recorders, has limited value on its own in identifying individuals. However, when combined with data from other C-ITS and automated vehicle technology, such as in-cabin and external cameras and microphones, such data may reveal significant personal information.[24]

The ability to combine a greater breadth and depth of data is more likely to reveal sensitive information when compared with an individual piece of data. A person who parks their car near a place of worship may do so because they intend to visit. This could reveal information about their religious affiliation. However, the person could just be visiting another venue in the same vicinity. If this information is combined with a video from in-cabin cameras that shows the person wearing religious clothing, then a person’s religious affiliation may be clearer.

[24] The various ways in which different information from C-ITS and automated vehicle technology may be linked to produce personal information is discussed throughout section 3.6 of the UNSW report.

6 Gaps in Australia’s information access framework to manage government access

Key points

- There are likely to be gaps in Australia’s information access framework to manage government access to C-ITS and automated vehicle data, particularly to cover new privacy challenges.
- Identified gaps relate to inconsistency across jurisdictions, potentially broad secondary uses by government and law enforcement exceptions that may facilitate increased surveillance.
- The NTC will consider specific legislative powers for government to collect data relevant to automated vehicle regulation in a subsequent phase of work. Such powers will require the creation of additional privacy protections.
- Further work is necessary to identify gaps in current frameworks that may impede governments accessing C-ITS and automated vehicle data for beneficial public purposes.

6.1 Purpose of this chapter

The purpose of this chapter is to outline gaps in Australia’s information access framework to manage government access to C-ITS and automated vehicle data, particularly to cover new privacy challenges.

6.2 Information access framework

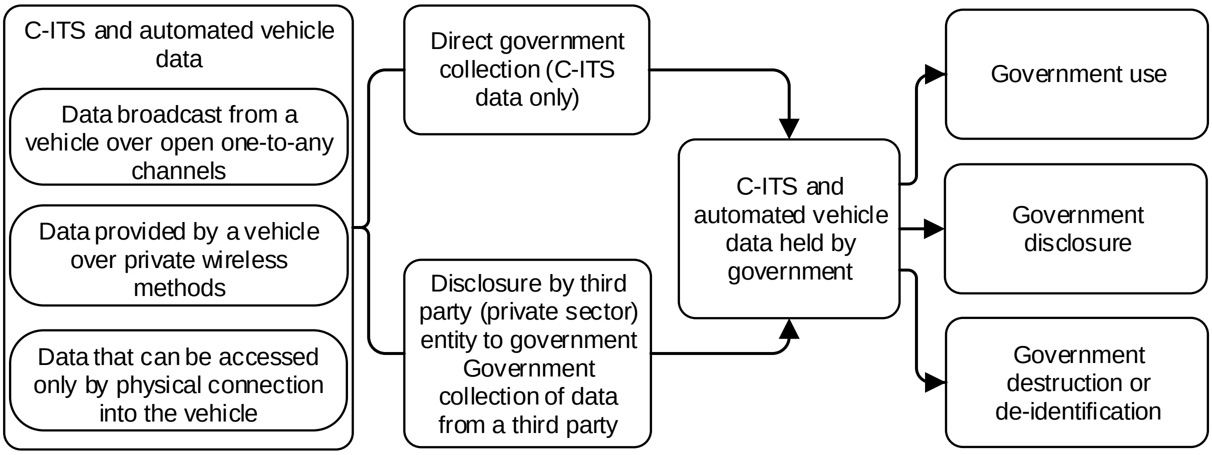
The main elements of Australia’s information access framework are:

- privacy regulation
- government collection powers
- surveillance devices laws.

Collectively, these elements provide the framework for governments to access, use and disclose information. This includes legislation at the state and federal levels.

Figure 5 represents the possible movement of C-ITS and automated vehicle data accessed by government. The NTC provided a detailed analysis of this in Chapters 5 and 6 of the discussion paper.

Figure 5. Movement of C-ITS and automated vehicle data accessed by government


C-ITS and automated vehicle data
Data broadcast from a vehicle over open one-to-any channels
Data provided by a vehicle over private wireless methods
Data that can be accessed only by physical connection into the vehicle
Direct government collection (C-ITS data only)
Disclosure by third party (private sector) entity to government Government collection of data from a third party
C-ITS and automated vehicle data held by government
Government use
Government disclosure
Government destruction or de-identification

As noted in section 3.4.2 we have updated this diagram from the discussion paper to include Austroads' categorisation of data and how it can be accessed in the box. However, we reiterate that the focus of this diagram is whether government can legally collect, use and disclose personal information; this is a separate matter to accessing safeguards within the technology itself.

6.3 Gaps in Australia's information access framework identified in the discussion paper

Chapter 5 of the discussion paper identified gaps in Australia's information access framework to address new privacy challenges arising from C-ITS and automated vehicle technology. We suggested that the key gaps relate to potentially wide allowable, use and disclosure of personal information, especially for law enforcement purposes. Specifically:

- Surveillance device laws are unlikely to place practical restrictions on government collection of personal information.
- While privacy principles do not authorise the collection of personal information, they do not restrict (because they allow/permit) direct collection of personal information by government agencies if it 'is necessary for one or more of its functions or activities'.[25] This facilitates government's increased ability to directly collect C-ITS personal information.
- Law enforcement collection, use and disclosure of C-ITS and automated vehicle data may result in increased opportunities for surveillance.
- Road transport laws in some jurisdictions contain provisions to facilitate information sharing between road agencies and police.[26]
- Requirements to destroy or de-identify personal information may not in practice greatly reduce the amount of personal information held by government. Government may continue to use and disclose the greater breadth and depth of personal information generated by C-ITS and automated vehicle technology once it is collected.

[25] APP 3.1. The circumstances in which collection is allowed and subsequently how it can be used, disclosed, stored and deleted are also explained further in section 5.5.2 of the discussion paper and Chapter 5 of the UNSW report.

[26] This is discussed in section 6.3 of the discussion paper.

We sought feedback on whether the current information access framework is sufficient to cover privacy challenges of government access to data from C-ITS and automated vehicle technology.

6.4 Stakeholder feedback

6.4.1 Sufficiency of current information access framework

Most stakeholders agreed that the existing information access framework would be insufficient to manage government access to C-ITS and automated vehicle data. Specifically:

- There are gaps in Australia's information access framework to sufficiently address new privacy challenges (Maurice Blackburn Lawyers, PwC Legal). Current authorisations for government data collection 'are convoluted and difficult to navigate' (Maurice Blackburn Lawyers). It is not clear to entities requested to supply information what government can collect and for what purpose (Australian Motorcycle Council).
- Existing information access framework may allow government to use personal information for broad secondary uses (Brisbane City Council, RAC WA) Government use of C-ITS and automated vehicle data for secondary purposes could lead to community concerns and delayed uptake (FCAI, OAIC, Truck Industry Council).
- Inconsistency across jurisdictions, including in requirements to destroy or de-identify personal information, means the current information access framework is insufficient (AAA, OIC QLD, RACQ, Squire Patton Boggs). Privacy, road transport and surveillance legislation differs across jurisdictions, and legislative reform would allow automated vehicle users to experience consistent privacy protections (OVIC).
- Additional privacy protections are particularly necessary for sensitive data such as from in-cabin cameras because sensitive information is inconsistently defined and protected between jurisdictions (FCAI, OAIC, Truck Industry Council).
- Law enforcement exceptions may facilitate 'mass surveillance' because of the potential volume of C-ITS and automated vehicle data (AAA, OVIC, Squire Patton Boggs).
- Extra protections are necessary to regulate government access because of the breadth and depth of C-ITS and automated vehicle data (Law Institute of Victoria, NSW Young Lawyers).
- Significant developments in transport technology mean current frameworks are not sufficiently advanced to protect privacy (EROAD, Law Society of New South Wales).
- Generic privacy frameworks are not sufficient for C-ITS and automated vehicle data – end-to-end frameworks such as those in the Heavy Vehicle National Law should be considered (TCA).

Two government agencies submitted that the current framework may not be sufficient, but a more detailed assessment is required before positively concluding this. The NHVR submitted that national consistency is preferable but that it is too early to determine whether there is a need for additional privacy protections.

Squire Patton Boggs raised the GDPR, concluding that it is not relevant to data privacy issues in Australia:

> *While automated and connected vehicle companies will need to comply with the GDPR, for example, when collecting and using information connected with advertising campaigns in Europe, or from vehicle users in the European*

> *Union, they will not have to comply with the GDPR when collecting and processing information from individuals of other jurisdictions, including Australia.*

Some stakeholders considered that existing frameworks in some jurisdictions may be sufficient but recognised the inconsistent application in different states and the need for national consistency (Department of State Growth Tasmania, Transurban, a government agency).

Some stakeholders considered that the current information access framework is probably sufficient to protect privacy:

- Existing privacy policies could be sufficient to cover government access to C-ITS and automated vehicle data (DMTR, WA DoT, a government agency). The key issue with the information access framework is that it does not authorise collection, use and disclosure of C-ITS and automated vehicle data for legitimate government uses. When access provisions are drafted, policymakers will need to consider and create privacy protections at the same time (DMTR).
- The current framework is sufficient, but this may change if governments were able to collect more C-ITS and automated vehicle data (Truck Industry Council).

6.4.2 Data security

Some stakeholders highlighted the links between data security and privacy (AAA, OVIC, RACQ, Squire Patton Boggs). OVIC told us that ‘privacy is closely tied with security’ and ‘both privacy and security protections will be important for encouraging public acceptance’.

RACQ and Squire Patton Boggs submitted that there are gaps in data security requirements in current regulation.

6.4.3 Telecommunications (Interception and Access) Act

Some stakeholders discussed the analysis of the *Telecommunications (Interception and Access) Act 1979* (Cth) in the discussion paper. Some stakeholders considered that there is too much uncertainty to know if or how the Act will apply; specifically, the extent to which the telecommunications network will be utilised for C-ITS communication and who the telecommunications carriers will be.

Telstra considered it is uncertain which parties will be covered by telecommunications legislation, including the Act, because of the various ways in which different information from C-ITS and automated vehicle technology may be linked to produce personal information.

The DITCRD submitted that the application of the Act depends on how the telecommunications network is used, the selection of communications technology and whether ADSEs and C-ITS technology providers are considered carriage service providers.

6.5 NTC conclusions

There are likely to be gaps in Australia’s information access framework to manage government access to C-ITS and automated vehicle data, particularly to address the new privacy challenges. Submissions generally supported this view because Australia’s information access framework:

- is inconsistent across jurisdictions
- may allow broad secondary uses by government
- contains law enforcement exceptions that may facilitate increased surveillance.

Stakeholders who suggested that information access frameworks are currently sufficient generally agreed that some additional protections may be necessary in the future. This included situations where additional government collection powers could allow government to collect more C-ITS and automated vehicle data. Further work is necessary to develop the framework for managing government access to C-ITS and automated vehicle data and the most appropriate privacy protections. This policy paper work is a key step in reviewing whether existing arrangements are appropriate to protect privacy.

The NTC recognises that, to achieve national consistency, reforms for regulating government access to C-ITS and automated vehicle data could, at a high level, incorporate data security protections. This is reflected in Chapter 8 and Appendix D.

The NTC has not considered the applicability of the Telecommunications (Interception and Access) Act in more detail. This is because of uncertainty about the use of the telecommunications network for C-ITS communication, and the unknown and complex roles and obligations of parties in the C-ITS and automated vehicle ecosystem.

7 Approach for managing government access to C-ITS and automated vehicle data

Key points

- There is a need for reform to manage government access to, and address the privacy challenges of, C-ITS and automated vehicle data.
- At this stage of the reform process the NTC considers it is possible to have a broadly similar approach, and therefore a combined set of options, for both C-ITS and automated vehicle technology.
- We recommend broad design principles for managing government access to, and addressing new privacy challenges of, C-ITS and automated vehicle data, which will guide further work by the NTC and Austroads.
- This approach will provide sufficient flexibility as regulatory frameworks and technologies develop.

7.1 Purpose of this chapter

The purpose of this chapter is to:

- assess the options for managing government access to, and addressing the new privacy challenges of, government access to C-ITS and automated vehicle data
- recommend an approach to managing government collection and use of C-ITS and automated vehicle data.

7.2 Separate options for C-ITS and automated vehicle data

While there is a degree of overlap between C-ITS and automated vehicle technology, automated vehicles can operate independently of C-ITS technology and vice versa.[27] The issues and implementation options differ for C-ITS and automated vehicle technology for the following reasons:

- Government can directly collect C-ITS data but will most likely need to rely on third parties to access automated vehicle data.
- Automated vehicles may generate more sensitive data.
- The NTC is developing end-to-end regulation to support the safe commercial deployment of automated vehicles but is not completing other C-ITS reform development. Austroads is currently developing a national framework for C-ITS.

For these reasons, in the discussion paper the NTC proposed separate options for government access to C-ITS data and to automated vehicle data.

7.2.1 Stakeholder feedback

Stakeholders were divided in their opinions of whether separate options for C-ITS data and automated vehicle data are reasonable for achieving any future reform.

[27] The distinctions and overlaps are illustrated in Figure 2 in Chapter 2.

While acknowledging there may be some overlap between C-ITS and automated vehicle technology, several stakeholders agreed that separate options are warranted for the following reasons:

- The timeframes for deployment and uptake are likely to vary between C-ITS and automated vehicle technology (AAA, Brisbane City Council).
- C-ITS and automated vehicle environments differ. The challenges and risks to individual privacy could differ between the technologies, including because automated vehicle data is likely to be more sensitive (Brisbane City Council, DoT WA, Law Society of NSW, NSW Young Lawyers, OIC QLD, a government agency).
- The technologies can operate independently of each other (AAA, OIC QLD, RACQ).

NSW Young Lawyers considered that a single set of principles cannot address the privacy challenges that arise. The AAA supported separate options but stated that consistent principles should apply to manage C-ITS and automated vehicle data. The RACQ similarly submitted that separate options are reasonable but ‘that the approach used for C-ITS should not be more onerous than that for [automated vehicles]’.

DoT WA suggested that further work is necessary to determine the benefits of separate options.

PwC Legal and a government agency recognised that Austroads is leading work in developing a C-ITS national framework, which will include data privacy considerations.

Several stakeholders submitted that separate options are not necessary or desirable for the following reasons:

- Both technologies can produce personal or sensitive information. Once information is categorised as personal or sensitive information, the relevant protections should not depend on the source of the data (DTMR, EROAD, Squire Patton Boggs, Truck Industry Council).
- While there are differences in the risks and issues between the two technologies, there are also many similarities (PwC Legal).
- C-ITS and automated vehicle technology will most likely both become increasingly integrated into vehicles, especially in highly automated vehicle systems (FCAI, Truck Industry Council).
- A single legislative framework covering C-ITS and automated vehicles needs to be established (TCA).

7.2.2 NTC conclusions

Overall, stakeholder feedback did not provide a clear preference about whether one set of options or separate options for C-ITS and automated vehicle data is preferable.

In the discussion paper the NTC proposed separate options to take account of different issues and implementation options for C-ITS and automated vehicle technology. Stakeholder feedback highlighted similarities in the issues. At this early stage of regulatory framework development, the NTC considers it is possible to have a broadly similar approach for both technologies. We have combined the options analysis for both C-ITS and automated vehicle data in this policy paper.

Once the broad approach is decided, it can be refined to consider variations in timeframes for deployment and uptake, specific challenges and risks of each technology and the differences in implementation paths. The NTC is not suggesting a single legislative framework covering C-ITS and automated vehicles needs to be established.

7.3 Options in the discussion paper

7.3.1 Automated vehicle technology

The discussion paper outlined four options for data generated by automated vehicle technology:

- option 1: rely on the existing information access framework to address the new privacy challenges of automated vehicle technology (no change)
- option 2: agree broad principles on limiting government collection, use and disclosure of automated vehicle data[28] (reform option)
- option 3: limit government collection, use and disclosure of automated vehicle data from in-cabin cameras and biometric, biological or health sensors to specific purposes (reform option)
- option 4: limit government collection, use and disclosure of all automated vehicle data to specific purposes (reform option).

7.3.2 C-ITS technology

The discussion paper outlined three options for data generated by C-ITS technology:

- option 1: rely on the existing information access framework to address the new privacy challenges of C-ITS technology (no change)
- option 2: agree broad principles on limiting government collection, use and disclosure of C-ITS data (reform option)
- option 3: limit government collection, use and disclosure of all C-ITS data to specific parties and purposes (reform option).

7.4 Criteria for assessing the options

In the discussion paper we proposed criteria for assessing the options and sought stakeholder feedback. Details of the stakeholder feedback are provided in Appendix C. The textbox below provides updated criteria to assess the options based on stakeholder feedback.

Updated criteria for assessing the options

Each option will be assessed based on whether it:

a. recognises the identified new privacy challenges of C-ITS and automated vehicle data and the likely inability of Australia’s information access framework to sufficiently address these

b. will most likely reduce the privacy concerns that may be a barrier to uptake

c. encourages and assists the realisation of beneficial future uses of C-ITS and automated vehicle data to achieve outcomes – in particular, road safety and network efficiency

d. provides appropriate flexibility for developing the regulatory frameworks for C-ITS and automated vehicles

[28] Note in the discussion paper we referred to ‘information’ throughout these options instead of ‘data’.

e. can be implemented within the broader information access and privacy landscape in Australia.

7.5 Preferred option for addressing the privacy challenges of C-ITS and automated vehicle data

In the discussion paper we assessed option 2 as preferable for both C-ITS and automated vehicle data because it was the only option that met the assessment criteria.

7.5.1 Stakeholder feedback

Need for reform

Most stakeholders agreed reform is probably needed and that option 1 (no change) is not viable for managing government access to, and addressing the privacy challenges of, C-ITS and automated vehicle data.

DoT WA and the Department of State Growth Tasmania suggested that a no-change option is viable but that there could be some benefit to agreeing broad principles for national consistency. The DITCRD supported no change, suggesting that ‘[a] priority for all Australian governments will be to monitor C-ITS and automated vehicle technology as it evolves and is applied to ensure the existing information access framework is fit for purpose’.

Support for option 2

Many stakeholders supported agreeing broad principles to inform the development of the regulatory frameworks for C-ITS and automated vehicles (option 2). Reasons given in support included that it:

- recognises the need for reform while acknowledging current uncertainties and provides sufficient flexibility for developing the C-ITS and automated vehicle regulatory frameworks (Brisbane City Council, OAIC, OIC QLD)
- currently provides the best approach to balance the achievement of transport and community outcomes with individual privacy (FCAI, NHVR, RACQ, Truck Industry Council)
- ensures that individual privacy is not undermined as technologies evolve while providing sufficient time for the technology to mature (Deloitte, EROAD, Law Institute of Victoria)
- offers the opportunity to move to options 3 and 4 once there is greater certainty about the specific limitations on government access that will need to be imposed (Australian Motorcycle Council, Maurice Blackburn Lawyers, OAIC)
- supports national consistency and is a good starting point for reform (OVIC, a government agency).

While supporting option 2:

- Squire Patton Boggs submitted that reforms must go further to address privacy concerns and suggested specific limitations on government collection and use.
- The RAC WA stated that the principles may not be sufficient to encourage take-up if the reasons for government access to C-ITS and automated vehicle data are not explicitly clear.

Support for options 3 and 4

Calibre, NSW Young Lawyers and the Law Society of NSW submitted that option 2 is not sufficient and that the more prescriptive options 3 and 4 are more appropriate.

- NSW Young Lawyers submitted that agreeing broad principles does not sufficiently protect privacy when considering the breadth and depth of personal information available from C-ITS and automated vehicle data. In supporting the more privacy protective reform option 3 (for C-ITS) and option 4 (for automated vehicles), NSW Young Lawyers stated that the options should be subject to further limitations. These include more narrowly defining the purposes who which C-ITS and automated vehicle data can be collected and used, and only allowing collection and use with a warrant or court order.
- The Law Society of NSW submitted that option 2 is insufficient because 'it does not begin from a privacy-protective presumption, nor is the protection of individuals' data and privacy necessarily embedded within the broad principles approach'. The Law Society of NSW supported option 3 for C-ITS and option 4 for automated vehicles, noting that option 3 for automated vehicles does not sufficiently address all relevant data sources.

No option supported or support for a variation

The DTMR and a government agency stated that they cannot support any of the options at this stage. In stating this:

- The DTMR submitted that, in their current form, the draft principles in option 2 may impede development of the technology but agreed that broad principles could assist in developing the regulatory framework.
- The government agency submitted that further work on the gaps in current information access frameworks should be completed, including by undertaking a privacy impact assessment.

Transurban submitted that rather than agreeing to no change, varying option 1 to ensure the existing privacy framework is applied consistently is the most appropriate response.

PwC Legal submitted that none of the options are adequate to address the identified privacy issues because private sector access is not addressed and broader inadequacies in existing privacy protection laws will remain.

7.5.2 NTC conclusions

Need for reform

We consider that there is a need for reform and that a 'no change' approach (option 1) is not viable. Most stakeholders supported a need for reform for managing government access to, and addressing the privacy challenges of, C-ITS and automated vehicle data.

Adopting a nationally consistent approach is a key element of proposed C-ITS and automated vehicle regulatory frameworks. Unclear or inconsistent government access to C-ITS and automated vehicle data could contribute to privacy concerns becoming a barrier to take-up of the technology in Australia.

Proposed approach

Based on feedback from stakeholders and the NTC's assessment of the options in Table 3, the NTC's proposes agreeing broad design principles to manage government access to C-ITS and automated vehicle data. The principles will inform the development of laws and aligned standards for C-ITS and automated vehicle technologies. This provides a sufficiently flexible approach.

While the language used to describe the NTC's proposed approach differs from the language used to describe option 2 in the discussion paper (which referred to limiting government collection, use and disclosure of C-ITS and automated vehicle data), the intent of the approach is largely the same. The main differences are to the content of the principles themselves, which is discussed in Chapter 8.

Many stakeholders strongly supported agreeing broad principles to inform the development of C-ITS and automated vehicle laws and aligned. Agreeing broad principles is not a commitment to a specific regulatory option but rather a recognition that there is a need to appropriately manage government access to C-ITS and automated vehicle data and agreement to key themes that will guide this access.

A broad-principles approach may not address all issues, including because some of these are still unknown. As the regulatory frameworks for C-ITS and automated vehicles develop there will be an opportunity to move to reform that may better address the issues and more closely resemble options 3 and 4. The NTC notes that several stakeholders recognised that option 2 allows for this. However, at this stage, options 3 and 4 may impede beneficial future uses and obstruct government goals of road safety and network efficiency.

Reasons for government access to C-ITS and automated vehicle data must be clear to ensure stakeholders take up the technology. The approach to agree broad principles is a starting point to ensure issues such as transparency are adequately addressed.

The NTC acknowledges that the options may not address any broader issues in existing privacy protection laws; addressing broader privacy issues is outside the NTC's scope and mandate.

We have completed a combined assessment of C-ITS and automated vehicle data options against the updated criteria. This assessment is summarised in 0.

To ensure continuity from the discussion paper, we have kept the numbering of the options the same as in the discussion paper but combined options that are similar.

Table 3. Assessment of options against the updated criteria

	Option 1 (automated vehicles and C-ITS) – existing information access frameworks	**Option 2 (automated vehicles and C-ITS) – broad design principles**	**Option 3 (automated vehicles) – limit access to data from in-cabin cameras and biometric, biological or health sensors to specific purposes**	**Option 3 (C-ITS) / Option 4 (automated vehicles) – limit access to all data to specific purposes**
a. Recognises the identified new privacy challenges of C-ITS and automated vehicle data and the likely inability of Australia's information access framework to sufficiently address these	×	✓	✓ (partial – does not recognise all privacy challenges)	✓
b. Will most likely reduce the privacy concerns that may be a barrier to uptake	×	✓ (but will depend on implementation of the principles)	✓ (partial – does not sufficiently address all relevant data sources)	✓
c. Encourages and assists the realisation of beneficial future uses of C-ITS and automated vehicle data to achieve outcomes – in particular, road safety and network efficiency	✓ (partial – while not constraining future uses, it does not recognise benefits of government access)	✓	× (although some beneficial uses are recognised)	× (although some beneficial uses are recognised)
d. Provides appropriate flexibility for developing the regulatory frameworks for C-ITS and automated vehicles	×	✓	×	×
e. Can be implemented within the broader information access and privacy landscape in Australia	✓	✓	Unclear at this stage	Unclear at this stage

Option 1 meets one criterion, partially meets one criterion and does not meet three criteria. This is because it:

- disregards the gaps identified in Australia's information access framework to address the new privacy challenges of C-ITS and automated vehicle technology (criterion a)
- leaves uncertain how privacy issues will be addressed and therefore is unlikely to reduce the privacy concerns that may be a barrier to uptake (criterion b)
- does not explicitly recognise the benefits of government access to C-ITS and automated vehicle data (criterion c)

- does not account for any potential new powers or authorisations that may be considered and developed as part of the regulatory frameworks for C-ITS and automated vehicles (criterion d)
- does not require implementation within the broader information access and privacy landscape (criterion e).

Option 2 meets all five criteria (although some uncertainty does exist in its ability to address criterion b). This is because it:

- recognises that additional privacy protections are most likely necessary to address the new privacy challenges of C-ITS and automated vehicle technology (criterion a)
- signals that governments are proactively addressing privacy concerns; however, success in reducing these concerns that may be a barrier to uptake also depends on implementing the principles as the C-ITS and automated vehicle regulatory frameworks are developed (criterion b)
- recognises the importance of C-ITS and automated vehicles data in realising beneficial future uses by balancing the achievement of transport and community outcomes with individual privacy (criterion c)
- only agrees broad principles and therefore does not restrict further development of the C-ITS and automated vehicle regulatory frameworks (criterion d)
- can be implemented as part of C-ITS and automated vehicle reforms in progress and therefore integrate within the broader information access and privacy landscape similarly to existing legislation such as the Heavy Vehicle National Law (criterion e).

Option 3 (automated vehicles) partially meets three criteria and does not meet two criteria. This is because it:

- focuses on specific types of data, not recognising that the greater breadth and depth of data likely to be generated by C-ITS and automated vehicle technology itself introduces risks (criterion a)
- addresses privacy issues from some data sources but leaves uncertain how remaining privacy issues will be addressed; this may not reduce the privacy concerns that could be a barrier to uptake (criterion b)
- focuses on limiting the purposes for which specific types of data can be used, which may impede the realisation of beneficial future uses (although some are recognised) (criterion c)
- may limit flexibility in developing the C-ITS and automated vehicle regulatory frameworks because it may prematurely determine one element when other related elements have not been fully developed (criterion d)
- is unclear at this stage how it can be implemented within the broader information access and privacy framework in Australia (criterion e).

Option 3 (C-ITS) / Option 4 (automated vehicles) meets two criteria, partially meets one criterion and does not meet two criteria. This is because it:

- recognises that additional privacy protections are most likely necessary to address the new privacy challenges of C-ITS and automated vehicle technology (criterion a)
- proactively addresses the privacy issues of all C-ITS and automated vehicle data, which will increase consumer confidence and therefore reduce the privacy concerns that may be a barrier to uptake (criterion b)

- focuses on limiting the purposes for which C-ITS and automated vehicle data can be used, which may impede the realisation of beneficial future uses (although some beneficial uses are recognised) (criterion c)
- may limit flexibility in developing the C-ITS and automated vehicle regulatory frameworks because it may prematurely determine one element when other related elements have not been fully developed (criterion d)
- is unclear at this stage how it can be implemented within the broader information access and privacy framework in Australia (criterion e).

Recommendation

NOTE the design principles for managing government access to, and addressing new privacy challenges of, C-ITS and automated vehicle data, which will guide further work by the NTC and Austroads.

The design principles are outlined in the next chapter.

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

Key points

- The NTC has developed design principles for regulating government access to C-ITS and automated vehicle data. These principles incorporate feedback provided on the principles proposed in the discussion paper.
- The principles are design principles and not principles that will be included in legislation.
- Among other matters, the principles consider: balancing the benefits of data access with privacy considerations; aligning with existing concepts of personal information; and specifying the data, purposes and parties covered.

8.1 Purpose of this chapter

The purpose of this chapter is to outline broad design principles for regulating government access to C-ITS and automated vehicle data to guide the development of the C-ITS and automated vehicle laws and aligned standards.

8.2 Principles outlined in the discussion paper

In the discussion paper, the NTC proposed eight principles for addressing the privacy challenges of government access to C-ITS and automated vehicle data. We proposed that these principles inform the next stage of our automated vehicle reform development and Austroads' development of the C-ITS national framework.

The principles captured the following high-level themes:

- C-ITS and automated vehicle data is most likely personal information.
- A regulatory framework that supports lawful collection, use and disclosure of C-ITS and automated vehicle data needs to be developed.
- When establishing this framework, additional legislative privacy protections are needed to appropriately limit collection, use and disclosure.
- Additional privacy protections need to specify the C-ITS and automated vehicle data covered, the purposes for which the data can be used and the parties to whom these limitations apply.
- Privacy protections could capture additional elements such as notification, consent, aggregation and destruction.

We sought feedback on whether our proposed principles would adequately address the privacy challenges of C-ITS and automated vehicle technology.

8.3 Stakeholder feedback

Stakeholders provided extensive feedback on the principles proposed in the discussion paper. A detailed summary of stakeholder feedback is provided in Appendix D.

Several stakeholders supported the draft principles (Australian Motorcycle Council, Brisbane City Council, FCAI, Maurice Blackburn Lawyers, Truck Industry Council, a government agency).

Other stakeholders suggested some amendments to the principles or additional principles and provided more general feedback. Key themes in the submissions related to:

- personal information – several stakeholders submitted that C-ITS and automated vehicle data should be treated as personal information by default, while others submitted that a case-by-case assessment is necessary
- consent – several stakeholders submitted that there is a need to obtain explicit informed consent from users. Others submitted that it is difficult to secure meaningful informed consent from users of vehicles producing C-ITS and automated vehicle data, and therefore alternative approaches need to be considered. A road transport agency considered stored vehicle data might be owned by the automotive company or service provider rather than the vehicle owner or driver. This could have implications for consent and notification
- providing different levels of protection for different data categories
- incorporating data security
- aligning with, and being informed by, Australian and international approaches
- ensuring the principles do not introduce inconsistencies with existing mechanisms.

8.4 NTC conclusions – proposed principles to inform future framework development

The NTC has extensively redrafted the principles we proposed in the discussion paper based on stakeholder feedback. These are outlined in Figure 66, with more detailed descriptions of the principles in section 8.4.1. NTC responses to stakeholder feedback are detailed in Appendix D.

The aim of the principles is to guide the development of future C-ITS and automated vehicle regulation. The principles are design principles and not principles that will be included in legislation. This means they will not introduce inconsistencies with existing legislative access and privacy protection frameworks. The NTC recognises that some of the draft principles outlined in the discussion paper may have read as legislative principles. In redrafting the principles, we have made it clearer that each principle is a design principle.

Figure 6. Design principles for regulating government access to C-ITS and automated vehicle data

The laws and aligned standards for 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 provide 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.

8.4.1 Description of principles

Principle 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

Australian governments will need to develop laws and aligned standards that support lawful collection, use and disclosure of C-ITS and automated vehicle data and capture holding, retention and storage of data. As part of this development, additional privacy protections should be included to appropriately limit the collection, use and disclosure of C-ITS and automated vehicle data to specific purposes, in particular safety and network efficiency. This must be balanced with ensuring that the benefits of government access to C-ITS and automated vehicle data, including in delivering value to the public in line with community expectations, can be realised.

This approach recognises and balances the benefits of government access with safeguarding privacy.

Principle 2: Be consistent with, and informed by, existing and emerging Australian and international privacy and data access frameworks

There are broader privacy challenges in different sectors in Australia, and as such it is important to consider data access frameworks in other sectors where appropriate when developing frameworks for C-ITS and automated vehicle technology.

As well, much automated vehicle and C-ITS technology will be developed overseas. Alignment with international data access frameworks, where appropriate, will also be important in order to encourage the deployment of automated vehicle and C-ITS technology in Australia.

Principle 3: Embed access powers and privacy protections for C-ITS and automated vehicle data in legislation, with sufficient flexibility to ensure this can be updated efficiently

To the extent possible, additional access powers and privacy protections for C-ITS and automated vehicle data should be legislative because:

- this ensures appropriate interaction with legislative collection powers and other legislative privacy protections
- this provides a legislative basis for enforcing non-compliance
- guidelines would offer weaker protection.

Non-legislative instruments including guidelines, standards or codes of practice, can be used and updated to support legislative powers and protections.

Principle 4: Clearly define C-ITS and automated vehicle data in inclusive and technology neutral terms

C-ITS and automated vehicle data must be clearly defined to ensure any additional privacy protections only capture relevant data. These definitions should be drafted in inclusive and technology neutral terms.

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

Aligning government entities' approach to managing C-ITS and automated vehicle data with the objectives underlying existing concepts of personal information recognises the new privacy challenges of C-ITS and automated vehicle data, including the potential for the data to identify individuals and affect C-ITS and automated vehicle users.

To allow for this, government entities may need to consider carrying out privacy impact assessments before collecting, using or disclosing C-ITS and automated vehicle data.

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

Additional privacy protections should specify:

a. the C-ITS and automated vehicle data covered. If design and security protocols eliminate data privacy risks, such data could be excluded. Certain data should be considered more sensitive and require stronger protections than other data

b. the purposes for which the data can be accessed. These purpose limitations will be considered in conjunction with any access powers developed as part of broader automated vehicle reform

c. the parties to whom the purpose limitations apply. These parties should include government entities who are authorised or responsible for collecting and managing C-ITS and automated vehicle data.

In developing these additional privacy protections, Australian governments should consider interaction with privacy laws and enforcement powers under existing legislation.

These protections should not impede access to data with a warrant or court order authorising a different use.

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

No further description.

Principle 8: Recognise that meaningful informed consent is important but provide avenues for government entities to balance individuals' expectations of privacy in alternative ways where obtaining such consent is not possible

Meaningful informed consent is a key way to satisfy individuals' expectations of privacy. However, the breadth and depth of C-ITS and automated vehicle data and the extensive purposes for which the data may be used by government entities may make securing such consent difficult. Similar challenges apply to providing genuine avenues for consumers to opt-out of government collection of C-ITS and automated vehicle data.

Where it is not possible or appropriate to obtain meaningful informed consent, alternative avenues for government entities to balance individuals' expectations of privacy should be provided. For example, where a government entity has the legislative authority to collect C-ITS and automated vehicle data, it may not need to rely on consent. This links closely with additional privacy protections specifying the purposes for which data can be collected and used.

Principle 9: Recognise the difficulty of irreversibly de-identifying C-ITS and automated vehicle data in many circumstances

Noting the difficulties of irreversibly de-identifying C-ITS and automated vehicle data in many circumstances, laws and aligned standards should instead incorporate concepts of destruction and aggregation. For example:

- aggregation of C-ITS and automated vehicle data to a statistically valid degree
- destruction of C-ITS and automated vehicle data after a set amount of time has elapsed or as soon as it is no longer necessary for the purpose it was collected for (unless government entities are otherwise required by law to retain the data)

The laws and aligned standards should recognise that the appropriateness and necessity of aggregation or destruction will depend on the circumstances.

Principle 10: Support data security

Data security should be considered alongside privacy. Laws and aligned standards should promote government entities implementing best practice information management for the secure and ethical use, collection and disclosure of C-ITS and automated vehicle data.

Principle 11: Allow for regular review of privacy protections for C-ITS and automated vehicle data

Privacy protections for C-ITS and automated vehicle data should be regularly reviewed so that privacy continues to be adequately protected.

9 Next steps

Key points

- The design principles will guide:
    - the NTC's development of laws to regulate government access to automated vehicle data, in conjunction with a privacy impact assessment
    - Austroads' development of a National ITS Architecture.
- A new piece of work will consider government access and use of C-ITS and automated vehicle data for network efficiency and investment purposes.

9.1 Purpose of this chapter

The purpose of this chapter is to:

- explain how the outcomes from this work will inform the NTC's broader automated vehicle national reform program and the opportunities for stakeholders to be involved in the process
- clarify how the outcomes of this work may inform Austroads' development of the National ITS Architecture.
- outline a new, related piece of work agreed by transport and infrastructure ministers that will be led by the NTC.

9.2 NTC's broader automated vehicle national reform program

The NTC's broader automated vehicle national reform program covers a range of reforms to enable automated vehicles to operate safely on Australian roads once they become ready for commercial deployment (as outlined in Chapter 1).

Ministers have agreed to the framework for a safety assurance system for ADSs at first supply. This included agreement to a set of criteria and obligations that an ADSE must meet before their ADS will be approved. One of these is an obligation to self-certify how an ADS or the ADSE will record data and share it with relevant parties. This is detailed further in Chapter 4.

This system places an obligation on ADSEs to record and share data; however, it does not provide a power for government agencies to access this data. We will consider specific legislative compliance and enforcement mechanisms for government to manage automated vehicles in a later phase of work. The design principles will inform this future work on compliance and enforcement for automated vehicle regulation, which is due to begin at the end of 2019. This will follow current work to develop an approach to the in-service safety of automated vehicles. This work considers the duties a regulator would need to enforce against relevant parties to ensure the safety of automated vehicles on the road.

As part of this work, we will develop a privacy impact assessment. This will assess how our compliance and enforcement proposals will affect the privacy of individuals and set how any impacts will be managed, minimised or eliminated.

9.3 Austroads’ development of a National ITS Architecture

Austroads is currently developing a National ITS Architecture, which will provide a common approach for planning, defining and integrating ITS. This approach is similar to that taken in the EU.

Austroads has completed stages 1 and 2 of this initiative by establishing Australia’s reference National ITS Architecture, its associated Framework and Roadmap for its further development. Stage 3 of the project will establish a governance framework, develop high-priority national architecture content and resources and undertake stakeholder engagement to support and encourage its use – particularly for C-ITS initiatives. The design principles in this policy paper will inform this work.

9.4 New work on government access to data for network efficiency and investment purposes

In Chapter 4 we noted feedback from the DTMR that there should be a comprehensive review of use cases where data can deliver commercial or public value. Following further consultation, all state and territory governments have supported this view. Transport and infrastructure ministers have now directed the NTC to lead a new piece of work, with support from states, territories and Austroads, on government access and use of C-ITS and automated vehicle data, including for network efficiency and investment purposes. We will develop the scope and timing for this work in 2019.

Appendix A Recent developments in Australia

A.1 The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry

In May 2018 the Australian government responded to the Productivity Commission's *Data Availability and Use Inquiry report* (Department of the Prime Minister and Cabinet, 2018). The response outlines policies aiming to achieve economic benefits from better data sharing.

The Australian government has committed to the following:

- A Consumer Data Right (CDR), which aims to give Australians greater control and easier access to their data to achieve choice and competition benefits. The CDR will be designed to ensure strong privacy protections and would allow consumers to securely share their data with third parties such as comparison websites. It will first be rolled out in banking, telecommunications and energy.
- A new data-sharing and release framework supported by a National Data Commissioner to oversee the integrity of Commonwealth agency data sharing and release activities. This aims to increase community trust and confidence in the way government manages and uses its data.
- New laws to improve data sharing and release, subject to strict data privacy and confidentiality provisions. These laws will balance access and secrecy and will not affect current protections covering particularly sensitive data such as national security and law enforcement data.

Treasury is developing the CDR (The Treasury, 2018a). A Consumer Data Right Bill was passed in August 2019 (Parliament of Australia, 2019). The new legislation will first apply to the banking sector, with telecommunications, energy and other sectors rolled out over time (The Parliament of the Commonwealth of Australia, 2019). Strong privacy and information security provisions are a fundamental element of the CDR and consumers will have a range of avenues to seek remedies for breaches of privacy (The Parliament of the Commonwealth of Australia, 2019).

In March 2019 the Office of the National Data Commissioner released a set of best practice guidelines for sharing and releasing agency data; this was an interim measure while a Data Sharing and Release Act is being developed. The Australian government's policy development highlights a move to improved data sharing, including between government agencies. In this policy paper, we are considering reform options for data sharing between government agencies to cover the new privacy challenges of C-ITS and automated vehicle technology. This is consistent with the Australian government's commitments on protecting privacy, introducing safeguards around the sharing of certain data, mitigating the risks associated with sharing personal data and increasing consumer trust in government use of data.

A.2 De-identification

Several recent reports have considered de-identification of personal information. These reports generally consider the release of data to the public, which may have different risks from more targeted use and disclosure of information generated by C-ITS and automated vehicle technology. However, the reports highlight the difficulty of irreversibly de-identifying personal information consistent with the NTC's assumption in this discussion paper. Relevant points from two of these reports are outlined below.

The *De-Identification decision-making framework* provides guidance to organisations on how to de-identify data (O'Keefe, et al., 2017). The report notes that:

- For the purpose of the *Privacy Act 1988* (Cth), information is de-identified if the risk of re-identification occurring is very low (having regard to the relevant release context).
- Whether data is personal information or de-identified information depends on the situation.
- Organisations need to make complex decisions about when data is sufficiently de-identified.
- Measures to reduce the risks of de-identification should be proportional to the risk and its likely impact – zero risk is not possible.
- De-identification only makes sense if it produces useful data.

The *Protecting unit-record level personal information* report broadly covers the limitations of de-identification (Office of the Victorian Information Commissioner, 2018). The report notes that:

- Improvements in technology increase the possibility of publicly released data being re-identified.
- Data could still be personal information even if direct identifiers are removed.
- De-identified data could be linked with another dataset to re-identify the data (where the two datasets have related records).

A.3 Collection of personal information in C-ITS trials

Cooperative Intelligent Transport Initiative (CITI)

Transport for New South Wales (TfNSW) has established CITI, Australia’s first C-ITS testing facility (Transport for NSW Centre for Road Safety, 2017). CITI initially focused on commercial vehicles but expanded into light vehicles. TfNSW established CITI to better understand the safety benefits of C-ITS technology, participants’ experiences and challenges with analysing data from the technology.

Data collected from commercial vehicles in the project is treated as commercially sensitive information rather than personal information, and there is a deed of agreement in place. Participants are informed upfront about what the data will be used for and who it will be provided to (largely for research purposes). Information about who is driving or the vehicle registration number is not collected.

For the CITI light vehicle study, which has been approved by a Human Research Ethics Committee, TfNSW informs participants in writing about how it will collect and use personal information and data; for example:

- The C-ITS equipment records location, vehicle movement and speed information at least 10 times per second.
- Researchers may access participants’ driving history from Roads & Maritime Services during the study and for three years prior to the study.
- Data collected will be used to assess road safety benefits of C-ITS and how user-friendly the system is.

Volunteer participants allow TfNSW to collect and use data and personal information as described by completing detailed consent forms.

The CITI light vehicle study provides a good example of obtaining consumer consent for collecting personal information in the context of C-ITS. Whether such an approach would be feasible when C-ITS technology is commercially deployed would need to be considered further as the number of parties needing to provide consent would be much higher.

Cooperative and Automated Vehicle Initiative C-ITS pilot

The DTMR, the iMOVE Cooperative Research Centre and the Queensland University of Technology are conducting a joint C-ITS pilot project. The pilot will take place on public roads in Ipswich in 2019 (Queensland Government, 2018). Around 500 vehicles will be retrofitted with C-ITS devices, and roadside C-ITS devices will be installed on arterial roads and motorways (Queensland Government, 2017). These devices allow vehicles and infrastructure to share real-time information and provide safety-related warnings messages for drivers.

The C-ITS pilot will use dedicated short-range communications (DSRC) and cellular communication. DSRC will generally be used for safety and time-critical message transmissions (for example, emergency brake lights). Cellular may be used for less time-critical message transmissions.

The pilot has several vendors. One vendor will manage all participant interaction by collecting personal information (such as the participant’s identity) and managing consent. To participate in the pilot, participants must complete a consent form to authorise the collection of their personal information. Participant identity is not shared with TMR, but TMR will have access to C-ITS device identifiers. TMR has completed a privacy impact assessment to consider the potential impacts of the pilot on privacy, and reviews this on a quarterly basis.

Like the CITI light vehicle study being conducted by TfNSW, the C-ITS pilot manages privacy by obtaining consumer consent. Individuals do not become trial participants unless they consent to their personal information being collected.

A.4 Privacy protections under the My Health Record system

The My Health Record system is the Commonwealth government’s digital health record system. It contains online summaries of an individual’s health information such as medicines they are taking, any allergies they may have and treatments they have received.

The *My Health Records Act 2012* limits when and how health information included in a My Health Record can be collected, used and disclosed. Unauthorised collection, use or disclosure of My Health Record information is both a breach of the My Health Records Act and an interference with privacy.

On 26 November 2018, the Australian Parliament passed the My Health Records Amendment (Strengthening Privacy) Bill 2018. The measures allow Australians to opt in or out of having a My Health Record at any time during their life. Records will be created for every Australian who wants one after 31 January 2019. After this date, a person can delete their record permanently at any time. Under the Australian Digital Health Agency’s official operating policy, no information within My Health Record can be released without an order from a judicial officer (Australian Digital Health Agency, 2018).

The amendments recognise that there may be privacy concerns associated with certain information that is not sufficiently covered by Australia’s existing information access framework. They introduce specific restrictions on the collection, use and disclosure of this information by certain parties. This is consistent with our findings in this policy paper.

Appendix B International approaches to data management and privacy

B.1 Overview of approaches in the European Union and the United States

European Union

The relevant legal framework for collection, use and disclosure of personal information in the EU is broadly governed by two main parts: the *General Data Protection Regulation* (GDPR)[29] and the *Law Enforcement Directive*.[30] Government powers to compel access to third party C-ITS and automated vehicle data are found in the national legislation of EU member states. These vary between member states. Some of these variations are discussed in section 8.3 of the University of New South Wales' *The privacy and data protection regulatory framework for C-ITS and AV systems* ('the UNSW report').

United States of America

The US does not have a comprehensive legal framework for regulating public and private sector privacy. The UNSW report states (in section 9.3) that:

> *US law and federal legislation does not generally regulate the collection and use of personal data derived from C-ITS and [automated vehicles] by the private sector. Some limited protections do however exist preventing the government from unrestrained access to personal data derived from C-ITS and [automated vehicles].*

There is no uniform definition of personal information. Federal and state statutes in the US use three different approaches to define 'personal data' or 'personally identifiable information'. This means that the same information may be personal information under some statutes and not others. The UNSW report states (at section 9.1) that personally identifiable information in the US is 'largely limited to instances where data refers to an actually *identified* individual'.

Comparison between EU and US data protection

The EU framework provides a single definition of personal information, whereas the US system provides for different definitions in different statutes. The US definitions focus on data that identifies an individual. This is narrower than the EU definition of personal information, which covers any information that could reasonably be linked to an individual.

The EU legal framework offers significantly greater privacy protections compared with the US legal framework. The EU framework comprehensively regulates the activities of both the private and public sectors with respect to privacy. By comparison, the US framework is fragmented with different sectoral laws. It does not generally regulate private sector collection of personal information and only offers limited protections for government access to personal information.

[29] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[30] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

B.2 European Union

The GDPR applies to both public and private sector entities and regulates how these entities handle personal information. The GDPR defines 'personal data' as any information relating to an identified or identifiable natural person. As outlined in the UNSW report (in section 8.2), 'data related to C-ITS and [automated vehicles] qualifies as "personal data" for any party that may be able to link such data to a specific individual with reasonable and legal means available to them'. All data generated by C-ITS and automated vehicle technology (described in section **Error! Reference source not found.**) could be personal data under EU law.

The following principles (which the GDPR requires data controllers to comply with) are relevant in the context of government access to C-ITS and automated vehicle data:

- 'privacy by design' and 'privacy by default' – the former aims to ensure privacy protections are built into designing and developing new technologies and services; the latter aims to ensure an 'opt-in' approach to collecting personal information
- 'data minimisation' and 'data avoidance' – these require the collection of personal information to be limited to what is necessary, and deleted when no longer necessary
- 'right to be forgotten' or 'right to erasure' – these entitle individuals to require that their data is deleted when no longer necessary for its collection purposes or when the individual removes their consent.

The GDPR explicitly excepts the handling of personal information for criminal law enforcement purposes. In the law enforcement context, the *Law Enforcement Directive* (a standalone piece of legislation) regulates the handling of personal information.

- Law enforcement purposes for processing personal information are formulated broadly and extend beyond the prevention, investigation, detection and prosecution of criminal offences to developing an understanding of criminal activities.
- The UNSW report states (in section 8.5.1) that:

  > *… vague formulations render most information sharing between C-ITS and [automated vehicle] manufacturers or operators and law enforcement (or between government and law enforcement agencies; or between two or more law enforcement agencies), for broadly defined 'criminal purposes' capable in principle of falling within processing under the* Law Enforcement Directive*, and not the GDPR. Therefore, crash investigations and traffic law enforcement could fall under the* Law Enforcement Directive*.*

- The *Law Enforcement Directive* provides significantly less privacy protection than the GDPR.[31]

B.3 United States of America

Generally, the US legal system does not directly authorise ongoing government access to personal information. Individuals may be compelled to provide electronic communications under the *Electronic Communications Privacy Act of 1986* or the *Stored Communications Act of 1986*. These provide law enforcement agencies with tools such as subpoenas, court orders and search warrants. In specific circumstances, law enforcement is authorised access to third-party data under national security laws.

[31] See also section 8.6 of the UNSW report, which discusses the ability of law enforcement authorities to share C-ITS and automated vehicle personal information on an EU-wide accessible database.

Protections for government access to personal information comprise of constitutional protections and protections in federal and state legislation.

- The Fourth Amendment to the US Constitution, which prohibits unreasonable search and seizure, is the primary limitation. US courts have recognised that GPS tracking of vehicles without a warrant contravenes the Fourth Amendment. However, in circumstances where individuals voluntarily disclose information to third parties (which may be the case for some C-ITS and automated vehicle information), the 'Third Party Doctrine' allows law enforcement agencies to access this information without a warrant. The Fourth Amendment may therefore not provide any real privacy protection from law enforcement collection of personal information held by a third party.
- The US Congress has enacted several statutes covering federal government agencies and state road agencies that provide privacy protections for government access and use of personal information. The applicability of these statutes to C-ITS and automated vehicle data is not clear. These statutes are detailed in section 9.3.2 of the UNSW report.

Recently, the State of California passed the *California Consumer Privacy Act of 2018*. The new privacy rules, to come into effect in 2020, include several obligations on business with respect to privacy and data collection. These include requiring businesses to disclose to consumers any personal information collected and allowing consumers to opt out of businesses selling their data to a third party.

There is some regulatory activity at the federal level. The US Department of Transportation works closely with the Federal Trade Commission to support the protection of consumer information and provide resources relating to consumer privacy (US Department of Transportation, 2018). The department suggests that any exchanges of data respect consumer privacy and proprietary and confidential business information.

B.4 International Conference of Data Protection

The OAIC noted in their submission the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC) 2017 *Resolution on Data Protection in Automated and Connected Vehicles*. The resolution calls on all relevant parties (including public authorities, vehicle and equipment manufacturers, and providers of data driven-services) to 'fully respect the users' rights to the protection of their personal data and privacy'. The resolution has 16 action items and urges parties to, among other things:

- provide granular and easy-to-use privacy controls for vehicle users enabling them to, where appropriate, grant or withhold access to different data categories in vehicles
- provide technical means for vehicle users to restrict the collection of data
- develop and implement technologies for cooperative intelligent transportation systems in ways that enable vehicle users to inhibit the sharing of positional and kinematic data while still receiving road hazard warnings
- provide vehicle users with privacy-friendly driving modes with default settings
- respect the principles of privacy by default and privacy by design.

Appendix C Criteria for assessing the options

C.1 Criteria for assessing the options

The discussion paper outlined three criteria against which the options were for automated vehicles were assessed; specifically, whether the option:

a. recognises the identified new privacy challenges of automated vehicle information and the likely inability of Australia's information access framework to sufficiently address these

b. ensures that beneficial future uses of automated vehicle information are not restricted

c. provides appropriate flexibility for developing the overall automated vehicle legislative framework (such as new powers for government to collect automated vehicle information). This includes ensuring that artificial barriers are not created at this stage of automated vehicle reform development.

The discussion paper also outlined three criteria against which the options for C-ITS were assessed; specifically, whether the option:

a. recognises the identified new privacy challenges of C-ITS information and the likely inability of Australia's information access framework to sufficiently address these

b. ensures that beneficial future uses and applications of C-ITS information are not restricted

c. recognises that the C-ITS framework in Australia is in the early stages of development and provides appropriate flexibility for its development.

We sought feedback on the criteria for assessing the options.

C.2 Stakeholder feedback

Most stakeholders agreed that the assessment criteria are comprehensive and reasonable for both C-ITS and automated vehicle data. Some stakeholders specifically commented that the criteria recognise the potential for C-ITS and automated vehicle data to maximise benefits for society (Brisbane City Council, DTMR, a government agency).

Stakeholders suggested the following amendments to the criteria:

- removing references to ensuring future uses of C-ITS and automated vehicle data are not restricted, and instead referring to encouraging and assisting the realisation of beneficial future uses of the data (Austroads)
- including an assessment of how well each option protects privacy relative to the other options (PwC).

Some stakeholders submitted that the NTC should include additional criteria:

- a criterion to 'ensure that it is possible to implement possible reform options within the broader information privacy landscape in Australia' (DTMR)
- a criterion that 'aligns the ongoing development of the framework for managing government access to automated vehicle data within the wider direction of change of the Australian privacy framework' (EROAD)
- a criterion assessing whether the option reduces the privacy concerns barrier to uptake (DoT WA)
- a criterion covering whether the option minimises the risk of a 'patchwork approach to privacy protection laws' (PwC Legal).

Transurban submitted that the first criterion (criterion a) assumes a new framework is necessary to cover C-ITS and automated vehicle data. Transurban also submitted that the third criterion (criterion c) for assessing the automated vehicle reform options focuses on new access powers, which appears at odds with arguments that there are currently insufficient protections from government access. Transurban suggested new access powers could instead be considered as part of examining law enforcement requirements.

C.3 NTC conclusions

As discussed in section 7.2.2, we have combined the criteria for assessing the options for C-ITS and automated vehicle data.

Based on feedback from stakeholders, the NTC has:

- included a criterion focusing on whether the options address the identified problem
- included a criterion covering whether the options can be implemented within the broader Australian information privacy landscape
- amended the criterion referring to ensuring beneficial future uses are not restricted to instead focus on encouraging the realisation of beneficial future uses
- removed the specific reference to new access powers from the criterion referring to flexibility for developing the regulatory framework. This ensures the criterion is more general because new access powers for law enforcement are only one part of the regulatory framework the NTC is continuing to develop.

An assumption for this policy paper is that the NTC may propose specific legislative powers to access relevant automated vehicle information as part of in-service safety reform. We will consider new access powers in a subsequent phase of work. Arguments that there are currently insufficient protections from government access have been developed with this assumption in mind.

Appendix D Stakeholder feedback on draft principles

D.1 Draft principles outlined in the discussion paper

Table 4. Stakeholder feedback on draft principles in the discussion paper

Principle	Stakeholder feedback	NTC response
Principle 1 C-ITS information and automated vehicle information must be clearly defined to ensure any additional privacy protections only capture relevant information.	▪ Include definitions for the identified 'new information' (IPC NSW). ▪ C-ITS and automated vehicle data should be defined in technology-neutral terms (Squire Patton Boggs). ▪ Definitions should be inclusive (TCA). ▪ Privacy challenges are not sufficiently unique to warrant protections for only C-ITS and automated vehicle data (PwC Legal).	▪ Noting that the technology is still developing, it is too early to include considered definitions for the 'new information'. ▪ The principles have been updated to refer to drafting inclusive and technology-neutral definitions. ▪ Addressing broader privacy issues is outside the NTC's scope and mandate.
Principle 2 Government entities should err on the side of caution and consider treating C-ITS and automated vehicle information as personal information (unless there are legitimate reasons not to do so).	▪ C-ITS and automated vehicle data should be treated as personal information by default (ATA, EROAD, OIC QLD, OVIC, Squire Patton Boggs). ▪ Need a pragmatic and case-by-case assessment rather than a collective view (DTMR, a government agency). ▪ Difficult to determine if data is personal (iMOVE). ▪ Classifying data as personal information provides consumers with control over their data, which is a positive (IAG). ▪ May be desirable to introduce protections irrespective of where it is personal information (a government agency).	▪ To balance differing stakeholder views about how to treat C-ITS and automated vehicle data, the principles have been updated to recognise the potential for this data to be personal information. ▪ The principles now refer to aligning government entities' treatment of C-ITS and automated vehicle data with the objectives underlying existing concepts of personal

Principle	Stakeholder feedback	NTC response
	▪ Parties seeking to access data should complete a privacy impact assessment (OIC QLD, OAIC, OVIC, a government agency). ▪ Nationally agreed definition of personal information (DoT WA).	information, rather than treating the data as such. ▪ The principles suggest that regulation could provide for government entities to consider carrying out privacy impact assessments before collecting, using or disclosing C-ITS and automated vehicle data. ▪ Developing a nationally agreed definition of personal information is outside the NTC's scope and mandate.
Principle 3 Australian governments will need to develop a regulatory framework that supports lawful collection, use and disclosure of C-ITS and automated vehicle information. As part of this development, additional privacy protections will likely be needed to appropriately limit the collection, use and disclosure of C-ITS and automated vehicle information to specific purposes, in particular safety and network efficiency. This must be balanced with ensuring that the benefits of government access to C-ITS and automated vehicle data, including in delivering value to the public, can be realised.	▪ Recognise and balance the benefits of government access with safeguarding privacy and community acceptance standards and expectations (AAA, Austroads, Brisbane City Council, OIC QLD, OVIC, RACQ). ▪ The regulatory framework should be based on the Australian Privacy Principles, with additional protections (OAIC, Squire Patton Boggs). ▪ Need to capture 'holding, retention and storage' (IPC NSW).	▪ The principles have been updated to: ○ more clearly emphasise recognising and balancing the benefits of government access with safeguarding privacy ○ incorporate reference to community expectations ○ capture holding, retention and storage of data. ▪ A new principle has been added to note that regulation should be consistent with, and informed by, existing Australian privacy frameworks.

Principle	Stakeholder feedback	NTC response
Principle 4 To the extent possible, additional privacy protections for C-ITS and automated vehicle information should be legislative. This will ensure they interact appropriately with legislative collection powers and other legislative privacy protections, and because guidelines would offer weaker protection.	▪ Need to consider the legislative basis and enforcement body to monitor and enforce noncompliance (EROAD, IPC NSW, OAIC). ▪ Privacy protections should be set in legislation and supported by mandatory guidelines as relevant (TCA). ▪ Flexibility is still important in the regulatory approach – a range of instruments can be used (two government agencies).	▪ The principles have been updated to capture the need to provide a legislative basis for enforcing noncompliance while still maintaining some flexibility.
Principle 5 Additional privacy protections should specify: a. the C-ITS and automated vehicle information covered. More sensitive information may warrant stronger protections than other information b. the specific purposes for which the information can be used. These specific purpose limitations will be considered in conjunction with any access powers developed as part of broader automated vehicle reform c. the parties to whom any specific purpose limitations apply.	▪ Recognise that different levels of protection are necessary for different data categories and emphasise stronger protections for more sensitive data (ATA, EROAD, Law Institute of Victoria, OVIC, Squire Patton Boggs, TCA). ▪ General law enforcement powers should not be impeded, such as access to data with a warrant for serious criminal offences (DITCRD, DTMR). ▪ Regulating access outside existing data access frameworks risks introducing inconsistencies with existing mechanisms (DITCRD). ▪ Unclear how additional protections will interact with existing privacy laws and enforcement powers (OAIC). ▪ Place appropriate privacy protections on all entities collecting and managing C-ITS and automated vehicle data, including industry (DTMR, TCA). ▪ Clarify secondary uses, specific reasons for use and circumstances where access is reasonable (OVIC, RAC WA). ▪ Specify agencies or entities that have access to the data (Law Society of NSW, RAC WA).	▪ The principles have been updated to: ○ more clearly recognise that certain data would require stronger protections ○ recognise that safeguards in technical architecture may sufficiently protect privacy ○ recognise the need to consider interaction with existing privacy laws and enforcement powers ○ ensure privacy protections will not impede data access with a warrant. ▪ Noting that a more detailed examination of government uses of C-ITS and automated vehicle data needs to occur, it is too early to specify the reasons for use and relevant agencies

Principle	Stakeholder feedback	NTC response
	▪ Personal information should be collected for a specific purpose and used for that purpose. Where de-identified, personal data can be collected for law enforcement purposes or to meet other state legal responsibilities (DoT WA). ▪ Incorporate privacy by design, such as safeguards in technical architecture (DTMR, OAIC, TCA).	covered. The principles recognise the need for this to be specified when laws and aligned standards are developed. ▪ Private sector privacy is outside the scope of this work.
Principle 6 Noting that government access to C-ITS and automated vehicle information will likely present privacy challenges, governments should consider: a. notifying users of how the C-ITS and automated vehicle information collected by an agency will be used, disclosed and stored b. destroying C-ITS and automated vehicle information after a set amount of time has elapsed or as soon as it is no longer necessary for the purpose it was collected for.	▪ Notification ○ Plain-English notice that is simple to read and understand (Squire Patton Boggs). ○ Notice about government collection and use is critical and must be provided to both drivers and passengers (OVIC). ○ Clear and meaningful notices about data handling would build public trust (OAIC). ○ May not always be practical/feasible to notify users of how C-ITS and automated vehicle data will be collected, used, disclosed and stored (DTMR, a government agency). ▪ Destruction ○ Support destruction over de-identification (OVIC). ○ Support rights for consumers to eventually have their data erased (IAG). ○ May need to retain some data for legitimate purposes (DTMR). ○ The need to retain information will vary based on the purposes for which it is collected, used and disclosed (a government agency). ○ De-identification may be appropriate (DoT WA, OAIC, RAC WA).	▪ The principles have been updated to refer to a plain-English notice. ▪ While it may not be practical to notify users at each point of C-ITS and automated vehicle data collection, it is necessary to recognise notification as a key way to build public trust. The most appropriate way to provide notification in the context of C-ITS and automated vehicle data could be considered further. ▪ There may be some limited circumstances where de-identification is appropriate. However, because of the potential for data linking, it is difficult to irreversibly de-identify personal information in most circumstances (especially C-ITS and automated vehicle data).

Principle	Stakeholder feedback	NTC response
		▪ The principles have been updated to focus on the difficulty of irreversibly de-identifying C-ITS and automated vehicle data while noting the importance of both aggregation and destruction.
Principle 7 Where government directly collects C-ITS information, governments should consider: a. instantly aggregating any information collected b. obtaining consent from users c. where practicable, providing users with the option to opt out of government collection of their personal information**.**	▪ Aggregation ○ Aggregate to a statistically valid degree (TCA). ○ Aggregation is beneficial for promoting efficient transport and developing transport policy (Brisbane City Council). ○ May not be possible/beneficial to aggregate for some C-ITS use cases (DTMR). ▪ Consent ○ Need to obtain explicit informed consent from users (EROAD, FCAI, RAC WA). ○ Difficult to secure meaningful informed consent from all users of vehicles producing C-ITS and automated vehicle data. Where the key elements of consent cannot be satisfied, individuals' expectations of privacy need to be balanced in alternative ways (OAIC, OIC QLD, OVIC). ○ Support ability of users to provide consent to individual uses; do not support bundled consent or holistic requests for consent (IPC NSW). ○ Obtaining consent from uses by multiple road authorities is challenging and could prevent effective deployment of C-ITS (Austroads).	▪ The principles no longer refer to instantly aggregating any information collected. Rather, the principles recognise that aggregation to a statistically valid degree could achieve similar aims to destroying the data. ▪ To balance differing stakeholder views about whether explicit informed consent must be sought, the principles recognise that such consent cannot be sought in all circumstances involving C-ITS and automated vehicle data. The principles note there should be avenues for government entities to balance individuals' expectations of privacy where obtaining consent is not possible. • The principles have been updated to recognise collecting

Principle	Stakeholder feedback	NTC response
	○ Challenging to seek consent through registration and licensing processes (a government agency). ○ Collect legally (DoT WA). ○ Rely on a legislative authority to collect rather than seeking explicit consent from users (DTMR, OVIC). ▪ Opt out ○ Allowing consumers to opt out may limit road safety benefits and affect the integrity of the data that agencies rely on for traffic management and planning (DTMR, OVIC, a government agency). ○ Opt in and out is more appropriate for non-government data collection and use (DoT WA). ○ Degrees of 'opt in' should be offered to users (IAG). ○ Opt out should be available whenever practicable (Law Society of NSW).	with legislative authority as one possible alternative to seeking consent. ▪ The principles recognise that challenges similar to obtaining meaningful informed consent also apply to providing genuine avenues for consumers to opt out of government data collection of C-ITS and automated vehicle data.
Principle 8 Privacy protections for C-ITS and automated vehicle data should be regularly reviewed to ensure privacy is adequately protected.	▪ Support regular review of privacy protections (DoT WA, OVIC, a government agency). ▪ Include oversight by the OAIC (Law Society of NSW).	▪ General support. ▪ The specific parties overseeing the protections will be considered at a later stage

D.2 Additional principles suggested

Several stakeholders submitted that data security is a key consideration alongside privacy (AAA, DoT WA, OAIC, OVIC, Squire Patton Boggs). The NTC recognises that data security should be considered alongside privacy, and we have included a new principle to reflect this.

Several stakeholders submitted that the NTC should look to other regimes, such as the Heavy Vehicle National Law, the *Telecommunications (Interception and Access) Act 1979* and data-sharing legislation for developing our approach to regulating government access (NSW Young Lawyers, Squire Patton Boggs, TCA, a government agency). The NTC has considered relevant parts of comparable legislation in developing the proposed approach and has included a new principle to reflect the importance of ensuring that further work is informed by existing and emerging Australian data access frameworks.

Several stakeholders commented that the principles should address alignment to international approaches (AAA, Austroads, DTMR, a government agency). The OAIC referred to the 2017 *Resolution on Data Protection in Automated and Connected Vehicles* as a relevant international development. The resolution calls on parties including public authorities to ‘fully respect the users’ rights the protection of their personal data’ and urges them to take certain actions (International Conference of Data Protection and Privacy Commissioners, 2017). The NTC recognises the importance of aligning with international approaches, and we have included a new principle to reflect this. The NTC’s revised principles also reflect many of the concepts in the resolution referred to by the OAIC, including appropriate notification, deleting data after a specific period, ensuring meaningful and informed (not bundled) consent, designing C-ITS in a way that eliminates data privacy risks and completing privacy impact assessments.

The DTMR suggested two additional principles. One is captured in stakeholder feedback on draft principle 5 in Table 4. The second is that ‘[a]s much as reasonably possible, privacy protections and legislative frameworks should allow CAV [connected and automated vehicles] data to be used in cases that deliver common good or societal benefit, by both government and industry’. The NTC notes that the principles capture the need to balance benefits of government access with appropriate privacy protections. However, as private sector privacy and access is outside the scope of this work, the principles do not specifically extend to capturing private sector uses.

EROAD suggested two additional principles:

- Restrain government’s direct C-ITS and automated vehicle data gathering capabilities. While the NTC acknowledges that direct government collection of C-ITS data is one of the new privacy challenges identified, our focus is not on the ease from a practical perspective of initial access to the data but rather whether government can legally collect, use and disclose the data. The purposes for which governments can access C-ITS and automated vehicle data would be the same irrespective of the method of collection.
- Provide a sustainable commercial market for creating and supplying C-ITS and automated vehicle data. The NTC considers this is beyond the scope of this work, which is focusing on managing government access to C-ITS and automated vehicle data.

The TCA suggested additional principles covering: minimise harm; proportionality of protection and responsibility; aggregation and de-identification where possible; clarity of purpose in use; and design of data management. The NTC notes that the revised principles generally capture these concepts.

D.3 Other feedback

EROAD, OVIC and the RAC WA submitted that the principles need to be more firmly stated and should be a requirement, not just a consideration. The NTC notes that the principles have been substantively rewritten to only focus on key design elements of future laws and aligned standards, rather than principles to guide regulated parties. We therefore no longer discuss what regulated parties need to consider.

The OAIC submitted that risks associated with accuracy and access to, and correction of, information are not addressed. The NTC notes it has not specifically considered these risks at this stage because they do not necessarily relate to the specific new privacy challenges of C-ITS and automated vehicle data.

Appendix E Public submissions

Name of organisation	Abbreviation	Description
Australian Automobile Association	AAA	National peak body representing automobile clubs
Australian Logistics Council	ALC	Peak body representing major and national companies in the heavy vehicle, freight transport and logistics supply chain
Australian Motorcycle Council	–	Consumer group
Australian Trucking Association	ATA	Peak body representing trucking operators
Austroads	–	Peak organisation of Australasian road transport and traffic agencies
Brisbane City Council	–	Local council
Calibre	–	Professional services firm
Deloitte	–	Professional services firm
Department of Infrastructure, Transport, Cities and Regional Development	DITCRD	Commonwealth government department
Department of State Growth Tasmania	–	State government department
Department of Transport (WA)	DoT WA	State government department
Department of Transport and Main Roads (Queensland)	DTMR	State government department
EROAD	–	Telematics provider
Federal Chamber of Automotive Industries	FCAI	National peak body representing manufacturers and importers of passenger vehicles, light commercial vehicles and motorcycles in Australia
iMOVE CRC	iMOVE	Collaborative transport research and development consortium
Information and Privacy Commission NSW	IPC NSW	Independent statutory authority
Infrastructure Victoria	–	Independent statutory authority
Insurance Australia Group	IAG	Insurance company
Intelligent Transport Systems Australia	ITS Australia	Independent not-for-profit incorporated membership organisation
Law Institute of Victoria	–	Peak body for Victorian legal professionals
Law Society of NSW	–	Professional association

Maurice Blackburn Lawyers	–	Law firm
National Heavy Vehicle Regulator	NHVR	Independent regulator
NSW Young Lawyers	–	Largest body of young and newly practising lawyers, and law students, in Australia
Office of the Australian Information Commissioner	OAIC	Independent statutory agency
Office of the Information Commissioner (Queensland)	OIC QLD	Independent statutory body
Office of the Victorian Information Commissioner	OVIC	Independent regulator
PricewaterhouseCoopers Legal	PwC Legal	Professional services firm
Royal Automobile Club of Queensland	RACQ	Automobile club and insurance company
Royal Automobile Club of WA	RAC WA	Automobile club and insurance company
Squire Patton Boggs	–	Law firm
Telstra	–	Telecommunications company
Transport Certification Australia	TCA	Government body
Transurban	–	Manager and developer of urban toll road networks in Australia and the United States
Truck Industry Council	–	Peak industry body representing truck manufacturers, importers and major component suppliers

Glossary

Term	Definition
automated driving system (ADS)[32]	The hardware and software that are collectively capable of performing the entire dynamic driving task (steering, accelerating, braking and monitoring the driving environment) on a sustained basis.
automated driving system entity (ADSE)	The legal entity responsible for the ADS. This could be the manufacturer, operator or legal owner of the vehicle, or another entity seeking to bring the technology to market in Australia.
cooperative intelligent transport system (C-ITS)	A technology platform that enables components of the transport network (vehicles, roads and infrastructure) to wirelessly communicate and share real-time information including data on vehicle movements, traffic signs and road conditions.
data linking	A process for combining individual records from two or more data sources. Datasets that may not independently identify an individual may do so when linked.
Lidar	A sensor input unit that detects the position or motion of objects using laser radiation.
radar	A sensor input unit that detects the presence, direction, distance and speed of objects using radio waves.
safety assurance system	A regulatory mechanism for governments to assess the safety performance of an automated vehicle to ensure if can operate safely on the network.
V2I	Vehicle-to-infrastructure communication. The wireless exchange of data messages (for example, about road conditions) between vehicles and infrastructure.
V2V	Vehicle-to-vehicle communication. The wireless exchange of data messages (for example, about vehicle movements) between vehicles.

[32] This term has been paraphrased from Society of Automotive Engineers (SAE) International Standard J3016, *Taxonomy and definitions for terms related to driving automation system for on-road vehicles* (SAE J3016).

References

Australian Competition and Consumer Commission, 2018a. *Consumer Data Right rules outline,* Canberra: Commonwealth of Australia.

Australian Competition and Consumer Commission, 2018b. *Digital Platforms Inquiry preliminary report,* Canberra: Commonwealth of Australia.

Australian Digital Health Agency, 2018. *Australian Parliament passes legislation to strengthen My Health Record privacy.* [Online]
Available at: https://www.myhealthrecord.gov.au/news-and-media/my-health-record-stories/legislation-strengthens-privacy
[Accessed 13 March 2019].

Department of the Prime Minister and Cabinet, 2018. *The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry,* Canberra: Australian Government.

International Conference of Data Protection and Privacy Commissioners, 2017. *Resolution on Data Protection in Automated and Connected Vehicles.* [Online]
Available at: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf
[Accessed 25 January 2019].

Office of the Victorian Information Commissioner, 2018. *Protecting unit-record level personal information,* Melbourne: Office of the Victorian Information Commissioner.

O'Keefe, C. M. et al., 2017. *The de-identification decision-making framework,* Canberra: CSIRO.

Parliament of Australia, 2019. *Treasury Laws Amendment (Consumer Data Right) Bill 2019.* [Online]
Available at:
https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6370
[Accessed 2 August 2019].

Productivity Commission, 2017. *Data availability and use,* Canberra: Productivity Commission.

Queensland Government, 2017. *CAVI components.* [Online]
Available at: https://www.qld.gov.au/transport/projects/cavi/cavi-components
[Accessed 21 August 2018].

Queensland Government, 2018. *TMR announced as first project in new national cooperative research centre.* [Online]
Available at: https://www.qld.gov.au/transport/news/features/cavi-imove
[Accessed 21 August 2018].

The Parliament of the Commonwealth of Australia, 2019. *Treasury Laws Amendment (Consumer Data Right) Bill 2019 - Explanatory Memorandum,* Canberra: Commonwealth of Australia.

The Treasury, 2018a. *Consumer Data Right.* [Online]
Available at: https://treasury.gov.au/consumer-data-right/
[Accessed 8 August 2018].

The Treasury, 2018b. *Treasury Laws Amendment (Consumer Data Right) Bill 2018 (second stage) and Designation Instrument for Open Banking.* [Online]
Available at: https://treasury.gov.au/consultation/c2018-t329327/
[Accessed 13 March 2019].

Transport for NSW Centre for Road Safety, 2017. *Cooperative Intelligent Transport Initiative.* [Online]
Available at: http://roadsafety.transport.nsw.gov.au/research/roadsafetytechnology/cits/citi/index.html
[Accessed 31 May 2018].

US Department of Transportation, 2018. *Preparing for the Future of Transportation Automated Vehicles 3.0,* Washington, DC: US Department of Transportation.

van Dijk, P., 2017. *Privacy Impact Assessment (PIA) for Cooperative Intelligent Transport Systems (C-ITS) data messages,* Sydney: Austroads.

Weeratunga, K. & Somers, A., 2015. *Connected Vehicles: Are we ready? Internal report on potential implications for Main Roads WA,* Perth: Main Roads Western Australia 2015.