REGULATING GOVERNMENT ACCESS TO C-ITS AND AUTOMATED VEHICLE DATA DISCUSSION PAPER

September 2018

NTC AUSTRALIA

National Transport Commission

Report outline

Title	Regulating government access to C-ITS and automated vehicle data
Type of report	Discussion paper
Purpose	For public consultation
Abstract	This discussion paper considers the new privacy challenges associated with government collection and use of information likely to be generated by C-ITS and automated technology. It seeks feedback on whether Australia's information access framework is sufficient to address these challenges and whether (and what) reform is necessary.
Submission details	Submissions will be accepted until Thursday 22 November 2018 online at www.ntc.gov.au or by mail to: Attn: Regulating government access to C-ITS and automated vehicle data National Transport Commission Level 3/600 Bourke Street Melbourne VIC 3000
Key words	data, information, C-ITS, automated vehicles, privacy, surveillance, government access, government collection, government use
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

Contents

List of tables

List of figures

Executive summary

The purpose of this paper is to outline and seek feedback on a number of matters relating to the privacy of people using cooperative intelligent transport system (C-ITS) and/or automated vehicle technology. Specifically:

- potential new privacy challenges of government access to information generated by C-ITS and automated vehicle technology
- whether Australia's information access framework[1] is sufficient to address these new privacy challenges
- proposed options for reform if the current framework is not sufficient.

This paper applies Australia's information access framework to government collection and use[2] of information that is likely to be generated by C-ITS and automated vehicle technology.

Context

This paper is derived from two previous recommendations agreed by the Transport and Infrastructure Council in 2016 and the then Standing Council on Transport and Infrastructure in 2013. These recommendations require the National Transport Commission (NTC) to consider options to manage government access to C-ITS and automated vehicle data that provide sufficient privacy protection for users.

This paper is limited to examining whether additional privacy protections for government collection and use of information 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.

This work is a part of the NTC's broader automated vehicle national reform program. As part of these broader reforms, the NTC is considering data recording and sharing obligations on automated driving system entities[3] and new powers for governments to access data, including for law enforcement purposes. Any such obligations and powers will affect the analysis of Australia's information access framework.

We are seeking submissions on this paper by **Thursday 22 November 2018**.

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.

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

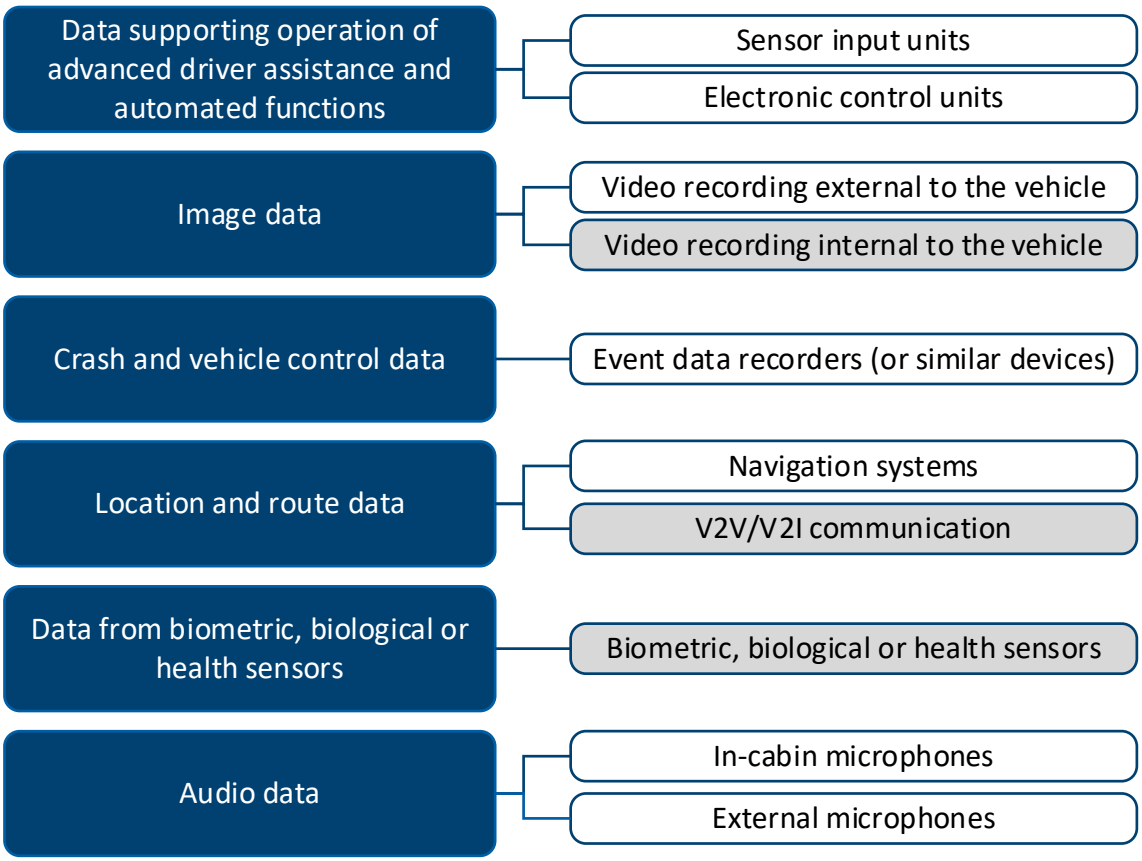
[2] 'Use' is intended to broadly cover use, disclosure and destruction or de-identification of information.

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

Automated vehicle data is derived from a combination of vehicle technology sources that together enable the operation of an automated vehicle.

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. The NTC's overview of technology in vehicles



Need for government access to information generated by vehicle technology

Information generated by vehicle technology will inform and enhance government decision-making. The NTC identified three main categories where information generated by C-ITS and automated vehicle technology could do so:

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

In addition to these three main categories, there may be other applications and benefits from government accessing C-ITS and automated vehicle data, including in delivering value to the public. These include the broad safety, security, environmental and transport efficiency objectives of government.

It is necessary to balance potential improved decision making and public value with sufficient privacy protection 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 identified three categories of potential new privacy challenges of C-ITS and automated vehicle technology:

- **Category 1** – new information 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 information 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 information by government may be in the future. The risk is therefore not linked to the type of information, 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 information.

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

These will be privacy challenges only if the relevant information identifies and impacts on individuals. The NTC considers that data produced by C-ITS and automated vehicle technology will most likely be 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.

The NTC considers that these 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'. 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 surveillance opportunities.
- Road transport laws contain provisions to facilitate information 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.

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, the options focus on limiting the collection, use and disclosure of automated vehicle information to specific purposes.

The NTC proposes separate options for addressing these challenges for C-ITS technology and for automated vehicle technology because the issues and implementation options differ.

The NTC proposes that any automated vehicle recommendations will guide the development of the NTC's broader automated vehicle reforms, rather than be standalone reforms.

This discussion paper presents 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 information (reform option)
- option 3 – limit government collection, use and disclosure of automated vehicle information 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 information to specific purposes (reform option).

The NTC is not completing other C-ITS reform development. Austroads is currently developing a national framework for C-ITS. As such, we propose that issues identified and any recommendations relevant to C-ITS inform Austroads' overall consideration of privacy for the C-ITS framework.

This discussion paper presents 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)
- option 2 – agree broad principles on limiting government collection, use and disclosure of C-ITS information (reform option)
- option 3 – limit government collection, use and disclosure of all C-ITS information to specific parties and purposes (reform option).

NTC's preliminarily preferred option

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

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

While we consider that options for addressing the privacy challenges of C-ITS technology should be separate to those for automated vehicle technology, we recognise that there is a degree of overlap in the issues and principles for both technologies. As such, we have developed a single set of draft principles to address the privacy challenges of both these technologies.

The draft principles are set out in Table 1.

Table 1. Draft principles for addressing the privacy challenges of government access to C-ITS and automated vehicle data

Principle 1	C-ITS information and automated vehicle information must be clearly defined to ensure any additional privacy protections only capture relevant information.
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).
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.
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.
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.
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.
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.
Principle 8	Privacy protections for C-ITS and automated vehicle data should be regularly reviewed to ensure privacy is adequately protected.

Next steps

The NTC is seeking submissions on this paper by Thursday 22 November 2018. Any individual or organisation is welcome to make a submission.

Based on the feedback from this consultation, we will develop recommendations and next steps to implement the recommendations for the Transport and Infrastructure Council meeting in May 2019.

1 Context

Key points

- Australia's transport ministers asked the National Transport Commission to develop options to manage government access to cooperative intelligent transport systems (C-ITS) and automated vehicle data that balances road safety and network efficiency outcomes and efficient enforcement of traffic laws with sufficient privacy protections for vehicle users.
- Our aim is to ensure any privacy challenges of government access to information generated by C-ITS and automated vehicle technology are appropriately addressed.
- We are seeking your feedback on whether:
  - Australia's information access framework is sufficient to address new privacy challenges of government access to information likely to be generated by C-ITS and automated technology
  - reform to address these new privacy challenges is necessary (and what reform is needed).

1.1 Objectives

1.1.1 Purpose of this discussion paper

The purpose of this discussion paper is to:

- outline potential new privacy challenges associated with government collection and use[4] of information generated by cooperative intelligent transport systems (C-ITS) and automated vehicle technology – in particular, considering what is different compared with the information produced by vehicle technology today
- apply Australia's information access framework[5] to government collection and use of information likely to be generated by C-ITS and automated vehicle technology
- seek feedback on whether the information access framework is sufficient to cover any new privacy challenges of government collection and use of information likely to be generated by C-ITS and automated vehicle technology
- seek feedback on whether reform is necessary to address any new privacy challenges, and the proposed options for reform.

1.1.2 Objectives of this work

This National Transport Commission (NTC) is assessing whether Australia's information access framework applying to government collection and use of information is sufficient to protect privacy given the significant developments in transport technology. In particular, we

[4] In this discussion 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.

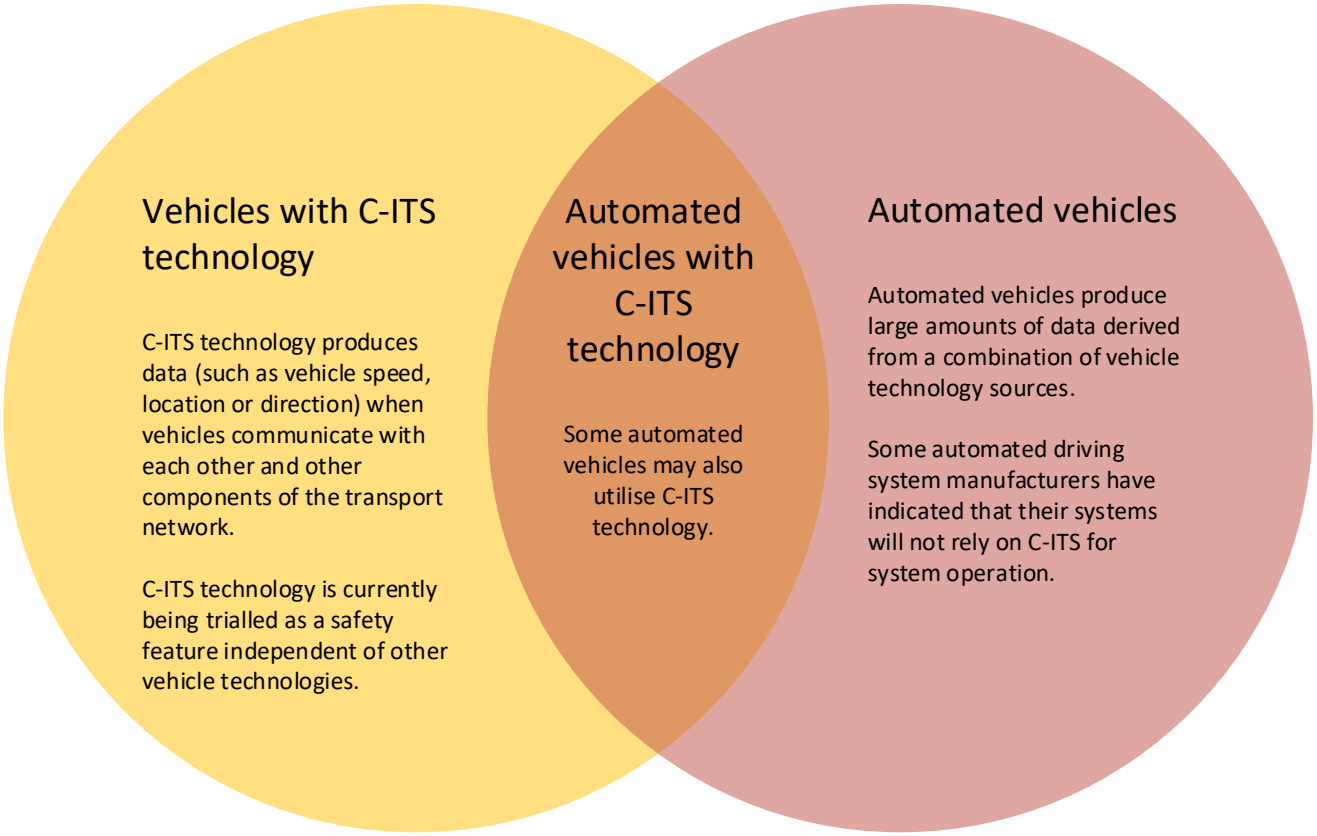
[5] In this discussion paper, 'Australia's information access framework' refers to existing privacy protections, and powers to collect information that collectively provide the framework for governments to access, use and disclose information. This includes legislation at state and federal level. The NTC's overview of the current information access framework is at section 1.5.

need to consider the existing regulations in light of the types and amount of information that future transport systems will be able to produce.

We are focusing 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 information, including information 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 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



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, delaying or impeding the deployment of technology that has the potential to significantly improve road safety. This could arise because consumers are uncomfortable about the amount and type of personal information governments may be able to access, or because government access is inconsistent or unclear.

Australia's existing information access framework was developed when C-ITS and automated vehicle technology did not exist and the breadth, depth and type of information that can be produced by this technology may have been 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.

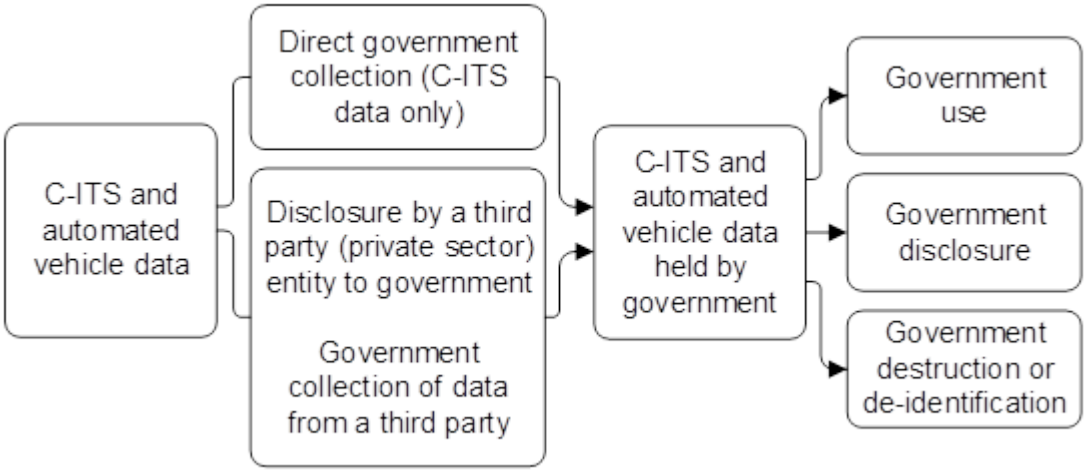
The NTC recognises there may be an additional element to the problem – that individuals take up the technology and continue to use it, but privacy is not sufficiently addressed. However, the NTC has a mandate for transport policy reform and not a broader privacy advocacy role. As such, the NTC is focusing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

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

- **Chapter 3** considers whether information generated by C-ITS and automated vehicle technology presents new privacy challenges when compared with information generated by current vehicle technology. This is considered in light of the type, breadth and depth of information.
- **Chapter 4** builds on the analysis in chapter 3 by considering whether the information identified as raising these new privacy challenges is personal information and sensitive information.
- **Chapter 5** considers government collection of information (both directly and from third parties), and whether the new privacy challenges are sufficiently covered by the information access framework.
- **Chapter 6** considers government use, disclosure and destruction or de-identification of information, and whether the new privacy challenges are sufficiently covered by the information access framework.
- **Chapter 7** outlines options for reform to address new privacy challenges
- **Chapter 8** outlines the next steps following the outcomes of this discussion paper.

Figure 3 represents the possible movement of C-ITS and automated vehicle information from a government access perspective. This figure appears in the other sections of the discussion paper to clarify which part of government access to C-ITS and automated vehicle data the section is discussing.

Figure 3. Movement of C-ITS and automated vehicle information from a government access perspective



1.4 Legal research and consultation

1.4.1 External legal research report

In mid-2018 the NTC engaged academics from the University of New South Wales (UNSW) to prepare a legal research report analysing and briefly explaining how Australia's information access framework applies to data generated by C-ITS and automated vehicle technology.

The UNSW's report, *The privacy and data protection regulatory framework for C-ITS and AV systems* (the UNSW report), informed and supported the NTC's development of issues and analysis in this discussion paper. It is available on the NTC's website.[6] While the UNSW's research and analysis are used throughout, this discussion paper does not reference the UNSW report except when directly quoting from the report or referring the reader to further detail contained in the report on a specific issue.

1.4.2 Initial stakeholder consultation

As part of initial background research and consultation, the NTC engaged with information and privacy commissions, state and territory transport agencies, various industry stakeholders and academics to better understand (among other matters):

- data collected by vehicle technology today and how this may change with the introduction of C-ITS and automated vehicles
- the privacy challenges of C-ITS and automated vehicle technology
- the current privacy frameworks in each jurisdiction, including any potential gaps.

1.5 Background

1.5.1 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.

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

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 (in the event that C-ITS data was deemed to be personal information). SCOTI approved the following recommendation:

> **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 (PIA) 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 PIA concluded, consistent with the position in the European Union (EU)[7], that the broadcast messages exchanged by vehicles are personal information. This meant that the pre-condition in recommendation 4 had been satisfied and further work needed to be done.

1.5.2 This work is part of a broader national reform program

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 are:

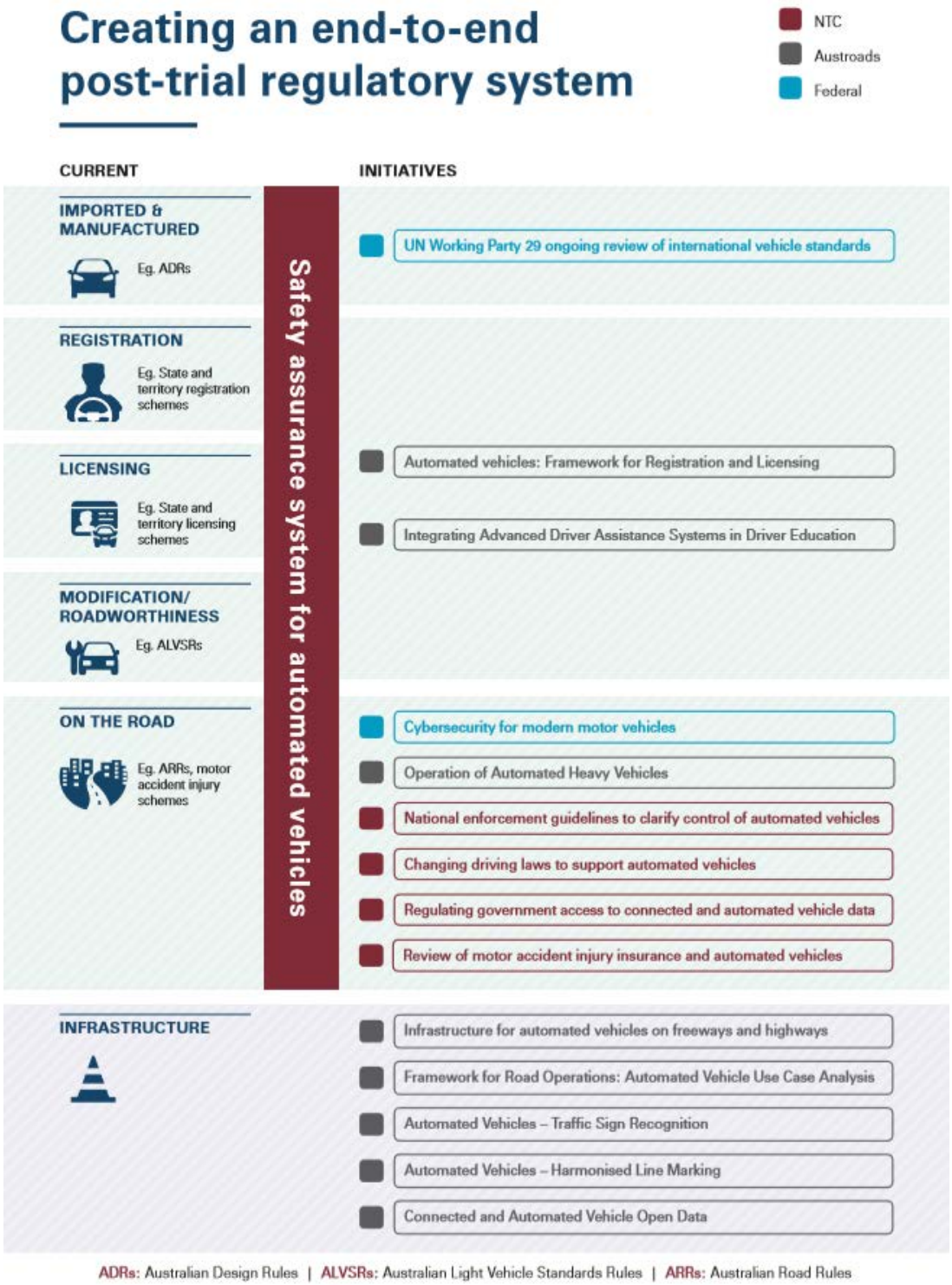
- **Safety assurance system for automated vehicles**: develop a system that sets out how governments regulate the safety of automated vehicles. In November 2017 the Council approved the development of a safety assurance system for automated vehicles based on mandatory self-certification in the interim until international standards are developed. A consultation regulation impact statement (RIS) was released for public consultation in May 2018 seeking the views of interested parties on policy options to address the safety risks associated with deploying vehicles with automated driving systems (ADS). We will submit the RIS to the council for a decision in November 2018.
- **Changing driving laws to support automated vehicles**: develop legislative reform options to clarify the application of current driver and driving laws to automated vehicles and establish legal obligations for ADS entities (ADSEs) and human users. Phase 1 was completed in May 2018 when the Council approved high level reform options including that a uniform approach to driving laws for automated vehicles is taken through the development of a purpose-built national law. Phase 2 will develop more detailed policy recommendations sufficient to enable the development of purpose-built national law to regulate an ADS 'driver'. This will form part of developing more detailed policy across all NTC automated vehicle reforms and be translated into legislation as required.
- **Motor accident injury insurance and automated vehicles**: we are considering options that support the deployment of automated vehicles, with the aim of ensuring that crash victims are no worse off in accidents involving automated vehicles. We will submit recommendations to the council in May 2019.

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

The NTC is collaborating closely with the Commonwealth, Austroads and 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.

Figure 4. End-to-end regulatory process and initiatives



1.5.3 Interdependencies

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. The NTC's safety assurance system for automated vehicles is proposing to introduce data recording and sharing obligations.

One design element of mandatory self-certification agreed by the Council in November 2017 is that ADSEs must submit a Statement of Compliance against safety criteria and other obligations. One such criterion is data recording and sharing.[8] 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 information. The NTC will consider specific legislative powers for government to access relevant automated vehicle information as part of the compliance and enforcement options for automated vehicles. The outcomes from this discussion paper will guide the development of these broader automated vehicle reforms.

1.5.4 Overview of Australia's information access framework

This overview focuses on the main aspects of Australia's information access framework. The discussion paper also touches on other elements not specifically mentioned in this overview.

Privacy regulation

Privacy legislation is found in all jurisdictions excluding Western Australia and South Australia. In South Australia, privacy is covered by an Information Privacy Principles Instruction published as Premier and Cabinet Circular No. 12 of June 2016.

Privacy legislation is based on 'privacy principles'. In many cases, state and territory-based privacy principles (generally referred to as the Information Privacy Principles) are derived from the Commonwealth Australian Privacy Principles (APPs) or their predecessors. However, there are variations in the IPPs of different states and territories. The principles outline how entities must handle, use and manage personal information and sensitive information. The APPs cover private sector organisations (with a turnover of more than $3 million) as well as Commonwealth agencies. State and territory privacy principles focus on state and territory public sector agencies.

Government collection powers

Specific powers for government to collect information relating to C-ITS and automated vehicles are quite narrow. These may include:

- limited and narrow powers to collect data under road transport laws
- access to information with a warrant under road transport laws
- access to data about telecommunications (metadata) without a warrant and to the content of telecommunications with a warrant under the *Telecommunications (Interception and Access) Act 1979*
- generic powers and specific collection powers for law enforcement in state and territory laws.

There may also be potential new powers to collect information considered and developed as part of the NTC's compliance and enforcement approach to automated vehicles.

[8] The NTC consulted on the safety criteria and other obligations as part of its consultation on the May 2018 RIS.

Surveillance device laws

Surveillance device laws are found in all Australian jurisdictions, but there is inconsistency in the types of devices regulated and how they are regulated. Surveillance device laws provide criminal offences for the unauthorised use of up to four categories of device:

- listening devices
- optical surveillance devices
- tracking devices
- data surveillance devices

Surveillance device laws prohibit installing or using surveillance devices except in certain circumstances (generally where there is consent or authorisation). This may protect privacy.

1.6 Scope

This work is limited to examining whether additional privacy protections for government collection and use of information generated by C-ITS and automated vehicle technology are needed.

The following areas are **outside the scope** of this work:

- **Access to automated vehicle data by motor accident injury insurers**. This issue will instead be considered in the NTC's motor accident injury insurance and automated vehicles review.
- **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 control of an automated vehicle). As discussed in section 1.5.3, the NTC will progress this work as part of the safety assurance system for automated vehicles and more broadly when considering compliance and enforcement options for automated vehicles.
- **Australia's information access framework as it applies to the private sector** (for example, consumers' ability to opt out of ADSEs collecting personal information). The NTC acknowledges there may be concerns by individuals about private sector access. In 2016 the NTC found that private sector access to data is a significant societal issue that is much broader than automated vehicle policy and regulation (National Transport Commission, 2016). In the same paper, the NTC found that privacy laws covering the private sector may be sufficiently robust to regulate private sector access to personal information generated by automated vehicles
- **Access to automated vehicle data by consumers for disputing liability** (for example, data showing which party was in control for defending road traffic infringements). The NTC intends to facilitate this access as part of the safety criteria and other obligations. The NTC's proposed data recording and sharing criterion requires ADSEs to explain how they will ensure individuals receive data to dispute liability where the individual makes a reasonable request and the provision of information aligns with privacy regulation. More broadly, '[t]he Australian Government will introduce a Consumer Data Right to allow consumers to access particular data, including transaction, usage, and product data, in a useful digital format' (Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2018, p. 6). While this right is primarily intended to achieve competition benefits, it suggests that the Australian Government is itself considering consumer access to data. The Consumer Data Right is discussed in more detail in Appendix A.

1.7 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.

Automated driving system (ADS) means the hardware and software that are collectively capable of performing the entire dynamic driving task on a sustained basis.[9]

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 together enable the operation of an automated vehicle.

Cooperative intelligent transport system (C-ITS) means 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.

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.

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 information means information 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 information is pseudonymised it is most likely still identifiable when combined with other information.

Personal information means (broadly) information about a reasonably identifiable individual. Definitions of personal information are discussed in more detail in section 4.3.

1.8 Relevant developments in Australia

The NTC has identified developments in Australia relevant to our consideration of the issues. 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
- collection of personal information in C-ITS trials
- privacy protections introduced under the My Health Record system.

[9] 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).

1.9 International approaches to data and information privacy

1.9.1 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)[10] and the *Law Enforcement Directive*[11]. 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 different members states. Some of these variations are discussed in section 8.3 of the UNSW report.

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 3.2) 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 relevance of these principles in the Australian context is discussed in more detail in section 5.4.5.

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*

[10] *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*.

[11] *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*.

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.[12]

1.9.2 United States

The US does not have a comprehensive legal framework for regulating public and private sector privacy. The UNSW reports 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 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'.

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 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.

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.

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

1.9.3 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.

1.10 Assumptions

The NTC adopted the following assumptions in carrying out its analysis in this discussion paper.

1. It is difficult to irreversibly de-identify personal information.

   The NTC's initial stakeholder consultation revealed a range of opinions about whether personal information can be irreversibly de-identified. Some stakeholders considered this could occur through aggregation. However, many stakeholders considered personal information can only be pseudonymised. This means personal information can be de-identified by removing personal identifiers but can often be re-identified by linking it with other information.

   For example, researchers at the University of Melbourne considered de-identified datasets published online and found that 'a few mundane facts taken together often suffice to isolate an individual' (Culnane, et al., 2017, p. 2). The report noted that de-identified data can be linked with other government datasets (or any other known data) to re-identify it; however, re-identification becomes harder where the precision of de-identified datasets decreases.

   Stakeholders also noted it is very difficult for personal information collected by automated vehicles to be de-identified because of the breadth and depth of information collected and because the information most likely contains many identifiers. The NTC is therefore taking a cautious approach at this stage and proceeding on the basis that it is difficult to irreversibly de-identify personal information generated by C-ITS and automated vehicle technology.

2. Internationally, information access frameworks will remain inconsistent with varying standards around data privacy. This is supported by the UNSW report, which highlights the different approaches to data privacy in the EU and the US. These are summarised in section 1.9 and are outlined in more detail in sections 8 and 9 of the UNSW report.

   The NTC is therefore not proposing to follow a particular international approach.

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 information.

   These potential obligations and powers are discussed in section 1.5.3.

Consultation question

1. Are the assumptions the NTC has identified for this discussion paper reasonable?

2 Consultation

Key points

- Any individual or organisation can make a submission to the NTC.
- We are seeking submissions on the paper by Thursday 22 November 2018.

2.1 Questions to consider

1. Are the assumptions the NTC has identified for this discussion paper reasonable?
2. Have we accurately captured current vehicle technology and anticipated C-ITS and automated vehicle technology (and the information produced by it)? Please provide reasons for your view, including whether there are any other devices that are likely to collect information internal and external to the vehicle.
3. Have we accurately captured the new privacy challenges arising from information generated by C-ITS and automated vehicle technology relevant to government collection and use?
4. Based on your assessment, what information generated by C-ITS and automated vehicle technology is 'personal information' and/or 'sensitive information' under current law?
5. Have we broadly identified the key reasons why governments may collect information generated by vehicle technology? Please outline any additional reasons governments may collect this information.
6. Is the current information access framework for government collection sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology? Please provide reasons for your view, including what parties may be affected if there is no change.
7. Is the current information access framework for government use, disclosure and destruction/de-identification sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology? Please provide reasons for your view, including what parties may be affected if there is no change.
8. Are separate options for addressing the privacy challenges of C-ITS technology and of automated vehicle technology reasonable for achieving any future reform? Please provide reasons for your view.
9. Are the criteria for assessing the automated vehicle reform options comprehensive and reasonable?
10. Is there is a need for reform to address the identified problem and the privacy challenges of automated vehicle technology (that is, option 1 is not viable)? At this stage of automated vehicle development, which option best addresses these privacy challenges while recognising the need for appropriate information sharing and why?
11. Are the criteria for assessing the C-ITS reform options comprehensive and reasonable?
12. Is there is a need for reform to address the identified problem and the privacy challenges of C-ITS technology (that is, option 1 is not viable)? At this stage of C-ITS development, which option best addresses these privacy challenges while recognising the need for appropriate information sharing and why?
13. Would the draft principles adequately address the privacy challenges of C-ITS and automated vehicle technology?

2.2 How to submit

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

To make an online submission, please visit www.ntc.gov.au and select 'Submissions' from the top navigation menu.

Or, you can mail your comments to: Attn: Regulating government access to C-ITS and automated vehicle data, National Transport Commission, Level 3/600 Bourke Street, Melbourne VIC 3000.

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

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

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

3 Data generated by vehicle technology and the privacy challenges of C-ITS and automated vehicle technology

Key points

- Automated vehicle technology presents new privacy challenges because of the type of technology and the new information it can collect. In-cabin cameras and biometric, biological or health sensors are the most likely technology to create privacy challenges. Such technology is either unlikely to be contained in current vehicles, or is only used for specific limited purposes.
- 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 information by government may be in the future. The risk is therefore not linked to the type of information, but rather the method and potential volume of collection.
- C-ITS and automated vehicle technology will generate a greater breadth and depth of information. This introduces new privacy challenges as more information is generated and stored and because of increased opportunity for data linking by government.

3.1 Purpose of this chapter

The purpose of this chapter is to:

- provide an overview of, and comparison between, information generated by current vehicle technology and anticipated C-ITS and automated vehicle technology
- outline the new privacy challenges presented by the type, breadth and depth of information generated by C-ITS and automated vehicle technology, focusing on government collection and use.

3.2 Overview of data generated by current and future vehicle technology

When considering any privacy challenges related to government collection and use of information generated by C-ITS and automated vehicle technology, it is relevant to compare information produced by current vehicle technology and C-ITS and automated vehicle technology and note any differences. These differences form the basis of analysing new privacy challenges.

The NTC's overview of technology in vehicles in this chapter covers technology capable of generating and recording information.[13] It is primarily based on information provided by stakeholders during the NTC's initial stakeholder consultation and the NTC's own research.

[13] For example, the NTC has not considered sim cards in vehicles as a separate technology. Rather, they are mentioned as inputs into a vehicle's navigation or infotainment system.

Table 2 provides a summary and highlights the main differences identified by the NTC between current vehicle technology and anticipated C-ITS and automated vehicle technology. A more detailed comparison is contained in section 3.3.

The NTC identified three C-ITS and automated vehicle technologies that may create privacy challenges and are likely to be widespread in future vehicles. **These technologies are highlighted in grey in Table 2**.

Table 2. NTC's 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, 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. Automated vehicles will generally rely on a larger number of higher quality sensors. External cameras are discussed under 'Image data', below.
Electronic control units	Receive and act on information 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 utilise a wider range of sensor inputs, receive and produce a larger volume of data and require more powerful computers and software.
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 number plates of other vehicles in real time.	Likely to be similar to current vehicles, but: ▪ could rely on a greater number of cameras with higher resolution ▪ the information produced by external camera input units could be recorded and stored, rather than just identifying external parties and number plates 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, fatigue and distraction monitoring).	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 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	Collect crash-related data from the vehicle in the seconds	Likely to be broadly similar to current vehicles. May collect additional inputs (for example, who is in control of the vehicle)

similar devices)	before and during a crash.	and store data over a longer period of time (that is, not limited to when a crash occurs).
Location and route data		
Navigations systems	Generally rely on a global navigation satellite system (GNSS) receiver and/or connection to the mobile network (for example, through a sim card installed in the vehicle). Information 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.
V2V/V2I communication	Not contained in current vehicles.	Enables components of the transport network to wirelessly communicate and share real-time information, including data on vehicle movements, traffic signs and road conditions. Such information can be received by roadside equipment.
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) to customise the driving experience.
Audio data		
In-cabin microphones	Allow voice commands (and voice recognition systems) to operate a number of 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.

The diagram at Appendix B illustrates the multiple sources, receivers and broadcasters of C-ITS and automated vehicle data. Some of these sources overlap with current vehicle technology.

3.3 Comparison of the type of data generated by current and future vehicle technology – are there new privacy challenges?

In this section, we analyse whether the type of data generated by C-ITS and automated vehicle technology may present new privacy challenges. The potential privacy challenges identified in this section are summarised in section 3.4. Section 3.4 also analyses privacy challenges associated with the way information may be collected in the future and the breadth and depth (rather than type) of information that may be generated by C-ITS and automated vehicle technology.

3.3.1 Data supporting the operation of advanced driver assistance and automated functions

Sensor input units

Sensor input units include cameras, radars and other devices embedded in the vehicle. They can, among other things, recognise obstacles and line markings and measure the proximity and speed of nearby objects. External cameras are discussed under 'Image data' in section 3.3.2.

Advanced driver assistance systems contained in current vehicles (such as adaptive cruise control and active lane control) rely on a range of sensor input units embedded in the vehicle to operate.

The NTC considers that ADSs contained in future vehicles are likely to rely on broadly similar sensor input units but of a higher number and quality. ADSs are also likely to rely on Lidar technology to assist with detecting and avoiding objects, measuring distance and mapping the environment. Compared with radar, Lidar technology can better detect objects and understand the type of object it is detecting (for example, a person, vehicle or cloud) (Waymo, n.d.).

While Lidar technology can better generate three-dimensional images, it is unlikely to be a step change from current sensor input units, in particular external cameras. Therefore, sensor input units in automated vehicles are unlikely to present new privacy challenges when compared with sensor input units in current vehicles.

Electronic control units

Electronic control units (ECUs) can receive, interpret and act on data generated by sensor input units and can record information about speed, journey distance and driving performance. ECUs are also used for the purposes of vehicle safety to undertake vehicle self-diagnostic checks and provide warnings about vehicle faults.

The NTC considers that ECUs in automated vehicles will be broadly similar to those in current vehicles. However, ECUs in automated vehicles are likely to use a wider range of sensor inputs, receive and produce a larger volume of data, require more powerful computers and software and play a large role in vehicle diagnostic checks.

Noting the use of ECUs in current vehicles, ECUs in automated vehicles are unlikely to present new privacy challenges.

3.3.2 Image data

Video recording external to the vehicle

External camera input units are used by advanced driver assistance systems in current vehicles to aid parking and recognise pedestrians or other obstacles. External cameras may capture the identity of external parties and the numberplates of other vehicles. The NTC understands this currently only occurs in real time, so this information does not get recorded

and stored. In automated vehicles, such information could be recorded and stored, although data storage limitations could prevent this.

While the recording and storing of image data from external cameras may appear to present a step change, other technology currently available performs a similar function. For example:

- Dashboard cameras capture images of vehicles in public places. They may record number plates and parties external to the vehicle. The NTC understands they are unlikely to identify drivers of other vehicles. Research suggests that the popularity and use of dashboard cameras by Australian consumers is steadily increasing (Compare the Market, n.d.; Lynch, 2016).
- Closed-circuit television (CCTV) can record images of individuals in public places. The Australian Institute of Criminology found that the use of CCTV in public spaces in Australia has grown considerably, and 'CCTV systems have become an increasingly common fixture in urban centres, in shopping centres and malls, individual shops and banks, on public transport and in car parks' (Hulme, et al., 2015).[14]

Noting the above, a change in the function of external camera input units from real time feed to recording and storing is unlikely to present new privacy challenges, at least in relation to the type of information. It is, however, relevant to the greater breadth and depth of information privacy challenge discussed in section 3.4.3.

Video recording internal to the vehicle

Some current vehicles may contain in-cabin cameras for monitoring purposes. These can be used for security purposes (for example, in taxis) or safety purposes (for example, for fatigue or distraction monitoring). However, the NTC does not consider this is widespread.

Stakeholders informed the NTC that automated vehicles are likely to rely upon inward-facing cameras to monitor human driver alertness and behaviour. The Institute of Electrical and Electronic Engineers has similarly commented on the need for inward facing cameras to measure the driver's state of awareness in automated vehicles (El Dokor, 2016).

Interior cameras (which would, for example, monitor driver attention and head pose) could perceive a driver's lack of attention or drowsiness. If this occurs, system alerts could be designed to wake up the driver or encourage the driver to stop.

Stakeholders informed the NTC that they are developing in-cabin cameras that can detect a human face and judge whether the human is alert, awake and focusing their attention on the road. The camera can also detect indicators of fatigue, including frequency of blinks and prolonged eye closure. Data collected from these cameras is generally held and analysed by private sector entities. For example, in cases of prolonged eye closure, data such as the video (generally a 1–20 second clip), the location of the vehicle and how fast the vehicle was travelling are combined to complete a safety assessment.

In-cabin cameras could also be used for driver recognition. Driver recognition is relevant for security purposes (to ensure only certain parties can operate the automated vehicle) and to set the driver preferences and customise the driving experience. Such information can be combined with data from biometric sensors.

More broadly, in-cabin cameras could be used for security monitoring in fleet vehicles.

In the early stages of development, vehicle cabin recordings in automated vehicles would most likely focus on the driver rather than the rest of the vehicle cabin and its occupants. As technology advances, this will most likely change, especially in vehicles with higher levels of automation. In such vehicles, it is possible that no-one would sit in the driver's seat.

---

[14] For example, from 2005 to 2014, the percentage of local government councils who either have CCTV or who plan to install CCTV rose from 11 per cent to 69 per cent.

Therefore, whole-of-cabin vehicle recordings could detect whether it is safe for the ADS to hand back control to a human (if manual vehicle controls exist).

Some stakeholders noted that taxis already have in-cabin cameras, so where an automated vehicle is owned as part of a fleet, the data collected by these cameras would be the same as that currently collected in taxis. However, in-cabin cameras in automated vehicles present a real step change from current vehicles and therefore raise new privacy challenges for the following reasons:

- There is likely to be a large increase in how continuous and widespread video recording of image data internal to the vehicle is (from limited inclusion in current vehicles to inclusion in most or all automated vehicles)
- There is a key contextual difference between taxis, which would generally be considered a quasi-public space and a personal vehicle, which would generally be considered a private space. More specifically, a vehicle is a private place that functions as an extension of our homes and offices in which individuals engage in intimate conversations and activities (Lawson & Lawton, 2015). It is not certain what automated vehicle ownership will look like. We cannot assume a fleet ownership model, particularly for vehicles with lower levels of automation where a role for the human driver remains
- In-cabin cameras in automated vehicles may collect additional data, such as biometric data, which is not currently collected in taxis.

3.3.3 Crash and vehicle control data

Event data recorders (EDRs) in current vehicles collect crash-related data (including the vehicle's self-diagnostic information) from the vehicle in the seconds before and during a crash. They are triggered by the deployment of airbags or other safety restraint systems. Such information would be collected continually but would be retained temporarily and stored only in the event of a crash.

The NTC considers that EDRs broadly similar to those used in current vehicles will continue to be used for automated vehicles. However, they may collect additional inputs (for example, who is in control and transition demands). These may assist parties to determine whether the ADS or the human was in control at the time of a crash or other safety related event (such as a breach of road traffic laws). To enable the latter, data may be stored for longer periods of time, rather than only in the event of a crash. An international standard on a Data Storage System for Automated Driving is currently under development (OICA, 2018). The system's data will most likely be the key source for determining who is in control of a vehicle at a point in time.

The collection and storage of this additional information by EDRs (or similar devices) relates to system operation at a point in time and is therefore unlikely to present new privacy challenges, at least in relation to the type of information. It is, however, integral to the greater breadth and depth of information privacy challenge discussed in section 3.4.3.

3.3.4 Location and route data

Navigation systems

Navigation systems in current vehicles generally include a GNSS receiver to pick up satellite signals to determine the position of the vehicle; they may also use a connection to the mobile data network. This information allows the vehicle route to be calculated and compared with the vehicle's current location throughout the journey. Past routes can potentially be stored and retrieved later.

Automated vehicles are likely to have more accurate GNSS capability and therefore generate data that could map the location history of the vehicle and its occupants. This is likely to be similar to the location information generated by navigation systems contained in current vehicles.

More broadly, stakeholders noted that speed, location and other related data is already collected by devices installed in current vehicles, and, in terms of location information, there is no real difference between data from automated vehicles and data mobile phones can collect today.

Taking the above into account, the NTC considers that navigation systems in automated vehicles are unlikely to present new privacy challenges.

V2V / V2I communication

C-ITS is a subset of the broader suite of ITS that use wireless communications utilising dedicated short range communication (DSRC) 5.9GHz or the cellular network (4G/upcoming 5G) to share information between components of the transport network. There are a range of communication scenarios that can occur through C-ITS. These include vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle to other devices, such as personal mobile devices.

In January 2018 the Australian Communications and Media Authority released a regulation as a form of ITS radio-communications class licence to allow road authorities, ITS and automotive industries to test or operate ITS stations in Australia in the 5.9GHz frequency ranges (subject to the requirements and conditions in the class licence) (Australian Communications and Media Authority, 2018).

DSRC 5.9GHz will most likely be the relevant communication platform for C-ITS. However, C-ITS could instead (or also) utilise the cellular network (most likely the 5G network under development) to share information. The NTC understands that cellular C-ITS communication may not currently be broadly accepted, and research in the EU will determine the maturity of this technology beginning in 2019. Cellular C-ITS communication may be used for less safety-critical applications.

Data messages broadcast by vehicles over C-ITS include information such as vehicle ITS station ID (unique identification numbers that are pseudonymised and rotated periodically), position, speed, direction, type of vehicle (car or truck) and time as well a more detailed information if there is a specific event or urgent emergency situation such as upcoming fog or an accident. Such information can be received by roadside equipment and used by road operators for traffic management, driver behaviour, intersection optimisation, emergency vehicle pre-emption route and congestion analysis. Roadside equipment could include beacons that monitor passing vehicles for measuring traffic volumes, traffic cameras for monitoring traffic flow and congestion, a traffic signal controller (for signal phasing and timing information) and a motorways/highways cabinet (for traveller information).

The type of data generated by C-ITS technology (speed, location and direction) is broadly similar to that generated by technology contained in current vehicles (for example, ECUs and navigation systems). However, C-ITS technology still presents a new privacy challenge when compared with technology in current vehicles. This is not necessarily linked to the information itself, but rather to how widespread the direct collection of this information by government may be in the future. This is discussed in more detail in section 3.4.

3.3.5 Data from biometric, biological or health sensors

Stakeholders indicated that biological or health sensors can be used to monitor facial temperature, heart rate, breathing rate and glucose and biometric sensors could be used to recognise drivers and occupants to customise the driving experience.

While similar information may currently be collected by wearable devices, the NTC understands that such sensors are unlikely to be contained in current vehicles. However, they are highly likely to be contained in automated vehicles, with some manufacturers suggesting automated vehicles must incorporate health sensors (The Medical Futurist, 2016). Automated vehicles may rely on these sensors to monitor driver alertness and behaviour, including whether a human driver is losing attention or getting stressed. This could assist with determining whether the human driver is ready to take back control of the vehicle. However, they could also collect sensitive health and wellness information about users of automated vehicles (for example, emerging health issues such as a heart attack), including the driver and other occupants.

The data obtained from these sensors therefore represents a real step change from current vehicles and therefore presents new privacy challenges. The type of information collected differs from that collected by current vehicles and may be particularly sensitive because it captures an individual's emotional, cognitive and behavioural attributes and state, as well as health information.

3.3.6 Audio data

In-cabin microphones

In current vehicles, in-cabin microphones allow voice commands (and voice recognition systems) to operate infotainment system functions, such as making hands-free calls or playing music, through a microphone in the vehicle or connected device.

Infotainment systems combine entertainment and information delivery to drivers and passengers. Infotainment systems are generally able to connect to smartphones through Bluetooth or other smartphone mirroring technology, or to a sim card in the vehicle. Once a smartphone or in-vehicle sim is paired with the vehicle's infotainment system, content from the smartphone or in-vehicle sim can be automatically transferred to the infotainment system.

The NTC considers that in-cabin microphones similar in nature to those contained in current vehicles will be used in automated vehicles. Automated vehicles could use audio inputs to, for example, activate automated functions or set destinations. Data from this technology could possibly be accessed in real time, or from a recording of a journey.

Therefore, the NTC considers that in-cabin microphones in automated vehicles are unlikely to present new privacy challenges.

External microphones

The NTC understands that external microphones are unlikely to be contained in current vehicles.

The UNSW report suggests (in section 3.7.5) that automated vehicles could contain external microphones as an additional safety feature. For example, external microphones could allow automated vehicles to respond to someone loudly shouting 'stop', horns or sirens.

It is uncertain whether the use of external microphones will be sufficiently widespread to raise privacy challenges (or whether ADSEs will use such technology at all). Even if such technology is used, the information generated may not raise new privacy challenges. While external microphones may recognise a warning or alert, they may not record this information or even recognise whether it was a human or machine that made the relevant sound because of external background noise.

At this stage, the NTC is unable to find any new privacy challenges from external microphones that may be used in automated vehicles.

3.4 C-ITS and automated vehicle technology presents potential new privacy challenges

The new privacy challenges of C-ITS and automated vehicle technology can be summarised into three general categories. Each of these is considered in detail below.

3.4.1 New information captured by automated vehicle technology

As outlined in section 3.3, automated vehicle technology presents new potential privacy challenges because of the type of technology and the new information it can collect. In-cabin cameras and biometric, biological or health sensors are the most likely technology to create new privacy challenges. Such technology is either unlikely to be contained in current vehicles, or is only used for specific limited purposes. As discussed in section 3.3, the data captured by such technology is not only new information, but may also be particularly sensitive information.

3.4.2 C-ITS technology may allow for more widespread direct collection of location information by government

As discussed in section 3.3, 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 (for example, ECUs and navigation systems). However, C-ITS technology still presents new privacy challenges because, in the future, the government may directly collect this information on a widespread basis. The challenge is therefore not linked to the type of information, but rather the method and potential volume of collection.

The type of data likely to be generated by C-ITS technology is currently directly collected by government in a limited way. The technology utilised for this collection includes road safety cameras, automatic number plate recognition (ANPR), infrared traffic loggers (TIRTLs) and roadside collection devices (including Bluetooth devices).

- Road safety cameras, such as speed and red light cameras, can capture images of traffic offences and calculate the speed of a vehicle. Some cameras are permanently fixed at approved locations (fixed cameras) while others are rotated across approved locations (mobile cameras) (Victoria State Government, 2018).
- Some police vehicles are fitted with ANPR cameras. These cameras photograph a vehicle's number plate so it can be checked against, for example, unregistered or stolen vehicle databases. The number plate is recorded along with the time, date and location. In August 2016, the Queensland Police Service had 60 vehicles equipped with ANPR technology across the state (Queensland Government, 2016). In April 2017, this had increased to 61 vehicles (Fallah, 2017).
- TIRTLs can be used to count, classify and measure the speed of passing vehicles using light based technology (CEOS, n.d.). The NTC understands TIRTLs can collect information for enforcement purposes, but the use of TIRTLs by enforcement in Australia varies.
- Roadside collection devices are generally used by road agencies to collect data for planning and traffic management purposes. For example:
    - VicRoads has installed equipment at limited sites to detect vehicles emitting a Bluetooth signal. VicRoads notes that data from these receivers can be used to calculate travel time and speed between receivers and can be used for origin destination studies (VicRoads, 2018). Such devices have been installed for a similar purpose in Queensland and South Australia.
    - Road & Maritime Services in NSW has around 600 roadside collection device stations that may collect one or more of 'traffic volume counts, speed and

classification (vehicle type) depending on the technology available at each site' (Roads & Maritime Services, n.d.).

The information collected by government using the above technologies is likely to be relatively limited and scattered across the network. Roadside collection devices (such as Bluetooth receivers) may also not receive unique identifiers from vehicles (Austraffic, n.d.). In addition, as outlined in section 3.6.3 of the UNSW report, '[Bluetooth] devices may be ubiquitous and disorganised and thus harder to identify than DSRC, which is customised for specific C-ITS purposes and more well-managed'.

Where C-ITS messages broadcast by a vehicle are received by government-owned infrastructure or roadside units at many points across the network (connected points), C-ITS technology could allow government to (among other things) collect information from the vehicle to:

- analyse, study and improve the road network, and for congestion analysis
- improve road safety by analysing driver behaviour
- achieve intersection optimisation.

As part of this, government 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. The NTC understands that C-ITS trials currently taking place in Australia only have connected intersections over a limited route and a limited number of motorways/highways cabinets. However, the NTC considers this may be more widespread when C-ITS is commercially deployed. This is because the effectiveness of C-ITS in delivering road safety outcomes would most likely rely on connectivity across the network. The allocation of the 5.9GHz band by the Australian Communications and Media Authority for the use of ITS in Australia further supports the intended widespread use of C-ITS in Australia.

In addition, as outlined in section 3.3, a C-ITS-equipped vehicle may broadcast a unique identification number (that is pseudonymised and rotated periodically) that is received by roadside equipment.

3.4.3 C-ITS and automated vehicle technology will generate a greater breadth and depth of information

While only some types of C-ITS and automated vehicle technology (and the information generated by it) may raise new privacy challenges, the breadth and depth of information that will likely be generated may itself present a challenge.

The generation (and potential storage) of information is likely to increase in future vehicles when compared with current vehicles. This will occur for the following reasons:

- Automated vehicles will rely on a greater number of inputs than current vehicles. Unlike advanced driver assistance systems, which can perform only part of the dynamic driving task, automated vehicles will perform the entire dynamic driving task, including monitoring the driving environment. Automated vehicles will therefore require a greater amount of information to operate.
- C-ITS and automated vehicle technology will collect (and broadcast) a greater amount of information relating to the safety of vehicle occupants and the road environment.
- Vehicle technology such as navigation systems and EDRs (or other devices that can capture inputs such as who is in control) will most likely become integral to the operation of automated vehicles. While similar technology is contained in current vehicles, its use is not integral and may therefore not be as widespread. In relation to EDRs and similar devices, data may also be stored for longer periods of time, rather than only in the event of a crash.

- external camera input units in automated vehicles will most likely move from real time feed to recording and storing.

New privacy challenges arise not only because more information is generated and stored, but also because there is 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. Identifiability is a key concept in determining whether information is personal information.

Consultation questions

2. Have we accurately captured current vehicle technology and anticipated C-ITS and automated vehicle technology (and the information produced by it)? Please provide reasons for your view, including whether there are any other devices that are likely to collect information internal and external to the vehicle.
3. Have we accurately captured the new privacy challenges arising from information generated by C-ITS and automated vehicle technology relevant to government collection and use?

Appendix C outlines potential government use cases of C-ITS and automated vehicle data that highlight the new privacy challenges identified in this chapter.

The remaining chapters of this discussion paper focus on the new privacy challenges identified in this chapter. These will only be privacy challenges if the relevant information identifies and affects individuals. This is discussed in detail in chapter 4.

4 Is the information that is generated by vehicle technology personal information?

Key points

- Privacy law only applies to personal information. Personal information is a key concept when assessing new privacy challenges from information likely to be generated by C-ITS and automated vehicle technology.
- Definitions of 'personal information' are similar across all Australian jurisdictions. While there are some variations in wording, these variations are unlikely to be of any real practical effect.
- Definitions of 'sensitive information' differ across Australian jurisdictions, with some variations of practical effect.
- The three general categories of new privacy challenges presented by C-ITS and automated vehicle technology identify and impact on individuals because they relate to personal information and, in some cases, sensitive information. In addition, C-ITS and automated vehicle technology will most likely generate more personal information and sensitive information than current vehicle technology.

4.1 Purpose of this chapter

The purpose of this chapter is to:

- explain why personal information is a key concept
- provide a summary of the definitions of 'personal information' and 'sensitive information' and highlight any substantive differences between jurisdictions
- analyse whether the new privacy challenges identified in chapter 3 relate to personal information and sensitive information.

4.2 Personal information is a key concept

In chapter 3 we identified new privacy challenges based on the type, breadth and depth of information we anticipate will be produced by C-ITS and automated vehicle technology, and how this information may be collected by government in the future.

C-ITS and automated vehicle users would only be affected if the information collected by government identifies an individual. The information collected by government would have to be considered 'personal information'.

As outlined in section 3.1 of the UNSW report:

> *The meaning of [personal information] is critical for both practical and legal reasons. Practically, if a data item or information element is not 'personal information', its disclosure or use will have little specific impact on a given individual. Legally, privacy law will only apply to [personal information].*

Personal information is therefore a key concept when assessing new privacy challenges associated with information likely to be generated by C-ITS and automated vehicle technology.

4.3 Analysis of definitions of personal information and sensitive information

4.3.1 Personal information

The definition of personal information is similar across all Australian jurisdictions (states, territories and the Commonwealth). While there are some variations in wording, these variations are unlikely to be of any real practical effect. These variations are summarised in section 3.2 of the UNSW report.[15]

The *Privacy Act 1988* (Cwlth) (Privacy Act) defines 'personal information' as:

> **personal information** *means information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> *(a) whether the information or opinion is true or not; and*
>
> *(b) whether the information or opinion is recorded in a material form or not.*[16]

Information such as a person's name or address is information 'about an identified individual'. However, in most cases, and particularly for information generated by C-ITS and automated vehicle technology, the relevant concept is whether an individual is reasonably identifiable.[17]

The UNSW report provides (in section 3.4.1) that:

> *Whether an individual is reasonably identifiable…is not solely an intrinsic quality to the information, it is also a feature of the context, and the legal and practical resources available to those who seek to identify.*

The more sources of information and linked data sets an entity has, the more likely it is that an individual is reasonably identifiable. The UNSW report discusses (at section 3.5) the capacity of certain entities to identify individuals. Operators of road infrastructure and law enforcement and intelligence agencies are likely to have access to a wide range of data, and technical capacity to analyse data, that could aid identifiability.

Some definitions of personal information (for example, in Queensland, Victoria and NSW) refer to an individual identifiable 'from the information'. This is arguably more restrictive wording and may suggest an individual is not identifiable from information that needs to be linked with other data. However, as explained in section 3.2.2 of the UNSW report, this wording is unlikely to be of any real practical significance.

Section 3.2.3 of the UNSW report discusses definitions of personal information in state and territory road transport laws. By way of summary, some state and territory road transport laws (including those in the ACT and Queensland) use the term 'personal information' but do not define it in their legislation; others states and territories do not refer to personal information. The Heavy Vehicle National Law includes a definition of personal information that is consistent with definitions in privacy legislation.

4.3.2 Sensitive information

Some information generated by automated vehicle technology may also be 'sensitive information'. Definitions of 'sensitive information' differ across Australian jurisdictions, with some variations of practical effect.

---

[15] The definitions are outlined in full in Appendix B, Table 1 of the UNSW report.

[16] *Privacy Act 1988* (Cwlth) s 6.

[17] A variation on this wording is whether identity is 'reasonably ascertainable'. The UNSW report notes (at section 3.2.2) that '[t]his and related variations in wording exist in states and territories but the differences have little practical impact'.

The Privacy Act defines 'sensitive information' as:

> **sensitive information** *means*:
>
> *(a) information about an individual's:*
>
> *(i) race or ethnic origin; or*
>
> *(ii) political opinions; or*
>
> *(iii) membership of a political association; or*
>
> *(iv) religious beliefs or affiliations; or*
>
> *(v) philosophical beliefs; or*
>
> *(vi) membership of a professional or trade association; or*
>
> *(vii) sexual orientation or practices; or*
>
> *(viii) criminal record;*
>
> *that is also personal information; or*
>
> *(b) health information about an individual; or*
>
> *(c) genetic information about an individual that is not otherwise health information; or*
>
> *(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or*
>
> *(e) biometric templates.*[18]

Government needs to meet higher standards when collecting and using sensitive information as compared with personal information. The above definition also captures information even where it is not personal information (see (b)–(e) in the definition of 'sensitive information' above).

Unlike for personal information, there are substantive variations in the definitions of sensitive information across the Commonwealth, states and territories. These variations are summarised in section 3.8.2 of the UNSW report.[19] Not all states and territories have a sensitive information category in their legislation. 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.

4.4 Information generated by C-ITS and automated vehicle technology will most likely be personal information

In section 3.4 we identified three general categories of new privacy challenges from C-ITS and automated vehicle technology. The extent to which each of these categories relates to personal information is detailed below.

4.4.1 Personal information 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. Such identification can occur in real

[18] *Privacy Act 1988* (Cth) s 6.

[19] The definitions are outlined in full in Appendix B, Table 2 of the UNSW report.

time if the cameras are also used for driver recognition (or if other built-in recognition functions exist, such as biometric sensors). Identification can also occur later when the video recording is examined.

Data from biometric, biological or health sensors is, on its own, less likely to identify an individual; however it may do so if it encompasses unique or rare traits. Its identifiability increases if it can be linked with other relevant data such as that from cameras or microphones, and processed through systems such as pattern recognition software. Context therefore becomes important, including the capacity of the entity holding the information to analyse it and the availability of other data to aid identification. As discussed in section 4.3, government entities such as road operators and law enforcement are likely to have a wider range of data and capacity to analyse the data than other entities may have. In their hands, data from biometric, biological or health sensors is therefore more likely to be personal information. Such data may also aid the identification of other data generated by C-ITS and automated vehicle technology.

4.4.2 Location information from C-ITS technology is most likely personal information

Messages broadcast in C-ITS will most likely require identifiers (security certificates) to verify their authenticity. Each message would broadcast the location of the vehicle on the network at the time the message was sent. If each vehicle has a single identifier, its whole route could be tracked along the network. To mitigate this possibility, '[e]ach vehicle maintains a list of pseudonyms that are rotated periodically' (van Dijk, 2017, p. 15).

The use of pseudonymised identifiers protects the identifiability of the information in the first instance. Therefore, an individual who receives a single message or multiple messages 'would not be able to identify a pattern concerning a single vehicle (with any degree of certainty)' (van Dijk, 2017, p. 15).

However, entities that can access other information, or a very large amount 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 information such as registration records (van Dijk, 2017, p. 15).

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

The UNSW report states (in section 3.6) that location information may in some cases 'be too remote from the individual to assist identification' but in other cases it 'potentially enables a deep set of inferences about a person and therefore could assist in identifying an individual'. Location information from C-ITS technology would most likely fall into the latter category because the possibility of tracking a vehicle along its whole route could reveal information such as a person's home or work address. As discussed in section 4.5, it could also reveal sensitive information.

4.4.3 Combination of data generated by C-ITS and automated vehicle technology increases the ease of identification

As noted in section 3.4, the greater breadth and depth of information 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, ECUs and EDRs – 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.

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

4.5 Information generated by C-ITS and automated vehicle technology may be sensitive information

The extent to which each of the three general categories of new privacy challenges relate to sensitive information is detailed below. Please note that the categorisation below relies on the definition of sensitive information in the Privacy Act. The variations in the states and territories around inclusion and the definition of sensitive information (noted in section 4.3.2) affect whether the analysis below is accurate for an individual state or territory. We consider the impact of these variations in more detail when discussing privacy protections regarding collection, use and disclosure in chapters 5 and 6.

4.5.1 Sensitive information generated by in-cabin cameras and biometric, biological or health sensors

Once data from in-cabin cameras is linked to an individual, it may reveal sensitive information about the individual. An individual's race or ethnic origin, religious affiliation and sexual orientation, among other matters, may in some circumstances be deduced from a recording of an individual's facial features, dress or behaviour.

Data from biometric, biological or health sensors could fall within the definition of sensitive information without identifying an individual because it could reveal health information about an individual, as well as information that could be used for the purpose of biometric identification.

4.5.2 Location information from C-ITS technology may reveal sensitive information

Location information, particularly where a vehicle's location is tracked along its whole route, could reveal a range of sensitive information about an identified individual based on venues the person visits. The UNSW report states (in section 3.8.5) 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.

4.5.3 The breadth and depth of data generated by C-ITS and automated vehicle technology could more easily reveal sensitive information

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.

4.6 C-ITS and automated vehicle technology will generate more personal and sensitive information

Sections 4.4 and 4.5 highlight that the new privacy challenges identified in chapter 3 identify and impact on individuals as they relate to personal information and, in some cases, sensitive information. These sections also highlight that C-ITS and automated vehicle

technology is likely to generate more personal information and sensitive information than current vehicle technology.

Consultation question

4. Based on your assessment, what information generated by C-ITS and automated vehicle technology is ‘personal information’ and/or ‘sensitive information’ under current law?

In chapters 5 and 6, we analyse whether Australia’s information access framework sufficiently covers these new privacy challenges. Chapter 5 focuses on government collection of C-ITS and automated vehicle information.

5 Government collection of information generated by vehicle technology

Key points

- Government may need to collect information generated by C-ITS and automated vehicle technology to inform and enhance decision making in law enforcement, traffic management and road safety, and infrastructure and network planning.
- Surveillance device laws are unlikely to place any practical restrictions on governments collecting 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. This facilitates government's increased ability to directly collect C-ITS personal information.
- Law enforcement collection of C-ITS and automated vehicle data from third parties may result in increased surveillance opportunities. Exceptions to privacy principles for law enforcement purposes could apply in many law enforcement contexts and allow law enforcement to collect the greater breadth and depth of information generated by C-ITS and automated vehicle technology upon request.

5.1 Purpose of this chapter

The purpose if this chapter is to:

- explain why government may wish to collect information generated by vehicle technology
- outline relevant government powers to collect information
- outline the privacy and other protections relevant to government collection of information
- analyse whether Australia's information access framework for government collection sufficiently covers the new privacy challenges of C-ITS and automated vehicle technology.

5.2 Need for government access to information generated by vehicle technology

Information 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, pp. 61-62).

The NTC identified three main categories where information generated by C-ITS and automated vehicle technology 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.

Each of these is discussed in detail below.

In addition to these three main categories, there may be other applications and benefits from government accessing C-ITS and automated vehicle data, including in delivering value to the public. These include the broad safety, security, environmental and transport efficiency objectives of government. For example, for automated vehicle regulation, any entities that will be responsible for the safety assurance system may require access to automated vehicle data to investigate contraventions of an ADSE's obligations or for general compliance monitoring/auditing of an ADSE.

It is necessary to balance potential improved decision making and public value with sufficient privacy protection 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.

5.2.1 Law enforcement

Crash investigations and road traffic law enforcement

To ensure effective administration of road traffic laws and to complete crash investigations, enforcement agencies will need to identify who is in control of an automated vehicle. Where there is crash or breach of a road traffic law (for example, where the automated vehicle goes through a red light), data showing whether the human driver or the ADS was in control at the time of the breach would assist police.

As noted in section 1.5.3, the proposed safety criteria for ADSEs include a criterion requiring the recording of crash data and data about who is in control of a vehicle and provision to parties such as law enforcement. EDRs or similar devices in automated vehicles will most likely collect and store information about who is in control of the vehicle and transition demands at a point in time. This is outlined in more detail in section 3.3.

Vehicle data may also be relevant for enforcing other proposed provisions relevant to automated vehicles. These include requirements on a new party (the fallback-ready user)[20] to remain sufficiently vigilant to respond to ADS requests without undue delay, which were agreed by transport ministers in May 2018 (National Transport Commission, 2018).

Image data internal to the vehicle and data from biometric, biological or health sensors can be used to monitor a driver's level of attention and alertness. Such data can be used for a safety purpose to, for example, determine whether it is safe for the ADS to hand back control to the human driver, or to issue system alerts to wake up the driver. This is outlined in more detail in section 3.3. It can also be used as evidence of a fallback-ready user's vigilance. The proposed requirement for data recording and sharing in the safety criteria does not cover the recording and sharing of such data.

Data from C-ITS and automated vehicle technology can also inform police of, and provide evidence for, current traffic offences such as speeding.

Other law enforcement activities

C-ITS and automated vehicle data may also provide evidence, including for criminal investigations, outside of the transport context. Examples of how enforcement could use the information outlined in section 3.3 include the following:

- location data of a suspect in a terrorism investigation
- video recordings of criminal behaviour occurring inside a vehicle

[20] The 'fallback-ready user' is a term that comes from SAEJ3016. A fallback-ready user means a human in a vehicle with conditional automation who is able to operate the vehicle and who is receptive to requests from the ADS to intervene and is receptive to evident dynamic driving task performance-relevant system failures. The fallback-ready user is expected to respond by taking control of the 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.

5.2.2 Traffic management and road safety as part of network operations

Government, particularly road management agencies, have a role in traffic management. For example, VicRoads states that its Traffic Management Centre delivers real time traffic management to Victorians (VicRoads, 2016). The Traffic Management Centre responds to incidents and events that may affect traffic safety or flow including hazards, vehicle crashes and natural disasters.

Stakeholders explained that road managers could use information from C-ITS to assist with network congestion, traffic management and traffic signal phase timing. When received in real time, such information would enable road operators to manage changing traffic conditions.

The United States Department of Transport found that connected vehicles could assist with managing the road network by providing vital data about the weather and road conditions as well as structural asset information. Once received by road operators and authorities, information relating to the weather and road hazard information could be provided to other road users. In the Australian context, this could mean that data relating to severe weather and emergency conditions such as flooding and bushfires could be received and transferred (Weeratunga & Somers, 2015).

5.2.3 Infrastructure and network planning as part of strategic planning

Government has a role in infrastructure and network planning. This includes making strategic decisions about what investments should be made to improve the road network and infrastructure, and to reduce network congestion.

Stakeholders explained that government could use information from C-ITS to consider vehicle interactions with the road environment and identify blackspots for future road investment.

Consultation question

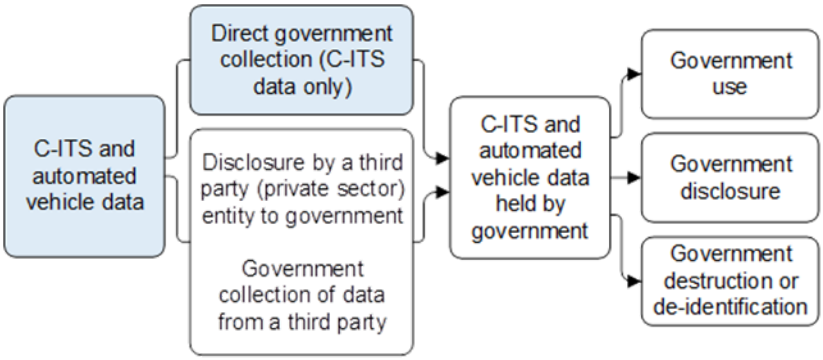
5. Have we broadly identified the key reasons why governments may collect information generated by vehicle technology? Please outline any additional reasons governments may collect this information.

5.3 Direct collection of information by government

In section 3.4.2 we discussed the new privacy challenge of potentially widespread direct collection of C-ITS information by government in the future. We now consider how this risk is addressed by Australia's information access framework covering collection of personal information.

This section focuses on the highlighted part of Figure 5.

Figure 5. Direct collection of C-ITS information by government



5.3.1 Surveillance device laws

Australian surveillance devices laws are relevant to information collection and provide criminal offences for unauthorised use of surveillance devices. There are four categories of such devices: listening devices, optical surveillance devices, tracking devices and data surveillance devices. The definition of each category of surveillance device is similar across all Australian jurisdictions, but not all jurisdictions cover each device. Section 6 of the UNSW report discusses surveillance device laws in detail.

Roadside infrastructure or other devices capturing C-ITS messages may be data surveillance devices[21] or tracking devices[22]. The installation, use and maintenance of a data surveillance device or tracking device without consent (express or implied) or without authorisation or warrant for law enforcement purposes is an offence under most surveillance device laws.

The NTC considers that surveillance device laws are unlikely to prevent state and territory road agencies from directly collecting C-ITS messages, or to provide any nationally consistent collection protections. The reasons for this are outlined below.

The installation, use and maintenance of data surveillance devices is not covered in all states and territories – it is covered in Victoria, South Australia, NSW and the Northern Territory.[23] Only South Australia and NSW include an offence for a person to install, use or maintain a data surveillance device – Victoria and the Northern Territory only regulate law enforcement officers.[24] Therefore, state and territory road agencies would most likely only be covered in South Australia and NSW.

The installation, use and maintenance of tracking devices is not covered in all states and territories – it is covered in Victoria, South Australia, NSW, the Northern Territory and Western Australia.[25] While South Australia covers tracking devices, it allows tracking devices to be installed, used and maintained to measure transport system performance (provided the

[21] A *data surveillance device* means any device program capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device. 'Program' is omitted in the Northern Territory data surveillance device definition.

[22] A *tracking device* means any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object.

[23] Data surveillance devices are also covered in the Commonwealth surveillance devices legislation, but that legislation is not relevant to state and territory road managers.

[24] See: *Surveillance Devices Act 1999* (Vic) s 9; *Surveillance Devices Act 2007* (NT) s 14.

[25] Tracking devices are also covered in the Commonwealth surveillance devices legislation, but that legislation is not relevant to state and territory road managers.

information obtained is de-identified).[26] This exemption is likely to apply to government-owned roadside infrastructure and other devices capturing C-ITS messages.

The following apply to both data surveillance devices and tracking devices:

- Express or implied consent of individuals is sufficient for use of the device to be legal. C-ITS enables components of the transport network to share information, and many C-ITS safety applications require receipt and processing of vehicle position and location information. Therefore, it may be possible to imply consent of individuals for use of C-ITS devices. Road agencies could possibly also ask individuals for express consent to use these devices through registration and licensing processes.
- The intended use of a device may affect its characterisation. For example, the installation, use and maintenance of a tracking device to determine the geographical location of a person or an object is prohibited.[27] The purpose of a C-ITS device is road safety and network efficiency rather than to determine location. Its purpose is therefore not a surveillance purpose. However, the ultimate intent is not an element of the offence, and therefore the role of intent in characterising a device may be limited.
- The UNSW report refers (in section 6.2) to commentary by the Australian Law Reform Commission that there are many gaps in surveillance devices laws when it comes to coverage of wireless devices that could be used for surveillance. This is relevant because C-ITS messages will most likely be sent over DSRC, which is a wireless communication platform. As such, C-ITS devices may fall outside the definition of surveillance devices altogether.

5.3.2 Privacy regulation

Privacy regulation covers both direct collection of information from an individual and collection of information from third parties. The former is discussed in this section and the latter is discussed in section 5.4.

The UNSW report states (in section 5.1.1) that '[p]rivacy principles focus on collection as a key point of control and treat the purpose of collection and whether it is necessary for the collecting entity's functions or activities as critical factors'. Collection covers personal information and sensitive information. As discussed in chapter 4, location information from C-ITS technology may be personal information and reveal sensitive information.

Collecting personal information

Collection privacy principles vary between states and territories, but these variations are generally not significant. One gap is the absence of privacy principles in Western Australia, though this is not specific to data generated by C-ITS and automated vehicle technology and may also not create a large practical gap. Stakeholders indicated that various Western Australian government agencies act within their own privacy policies, which are often informed by the APPs. Western Australian government agencies must also comply with an information sharing policy framework, which expects agency practices to align with privacy standards set out in the APPs (Government of Western Australia, 2017; Wauchope, 2014). In addition, the Western Australian Ombudsman issued a guideline for agencies that includes good practice principles for managing personal information (Ombudsman Western Australia, 2013). These principles cover collection, use and disclosure and include checklists that mirror some of the language in the privacy principles of other states and territories. The Western Australian government is also currently implementing recommendations from a 2017 Service Priority Review, which includes a recommendation that the Department of the

[26] Surveillance Devices Regulations 2017 (SA) reg 11.

[27] See, for example, *Surveillance Devices Act 1999* (Vic) s 8.

Premier and Cabinet 'develop legislation and processes to facilitate information sharing while protecting sensitive personal and other information' (Government of Western Australia, 2017; Department of the Premier and Cabinet, 2018).

While there are no legislative privacy principles in South Australia, South Australia has privacy principles in Cabinet instructions. Cabinet instructions represent policy developed at the highest level of state government and are binding on the public sector (Legal Services Commission of South Australia, 2018).

Most state and territory privacy principles allow public sector organisations or agencies to collect personal information only if it is necessary for one or more of its functions or activities and require collection by lawful means or for a lawful purpose.

Where privacy principles apply, they generally require collection of an individual's personal information from the individual. Collection can be from another party if it is not reasonable or practicable to collect from the individual (in most jurisdictions) or the individual consents to collection from someone other than themselves (in some jurisdictions).

Collection of C-ITS messages from vehicles by government-owned infrastructure or roadside devices can be characterised as direct collection from the individual in certain circumstances. The UNSW report suggests (in section 5.1.2) these circumstances are where 'that individual is in effective control of the vehicle and aware that collection was occurring'. This would most likely require notification, which is also covered by the privacy principles.

Notification provisions in state and territory privacy principles are broadly similar, and require public sector organisations or agencies to notify the individual whose information is collected of the purpose of collection and the intended recipients of the information (among other matters). This may require agencies to also notify about known secondary recipients (for example, if road agencies typically provide certain information to law enforcement). In the ACT, there is a more explicit requirement to notify individuals of 'any other public sector agency or entity … to which the public sector agency usually discloses personal information of the kind collected by the agency'.[28]

Notification must occur before the information is collected, or as soon as practicable after collection. In the context of government direct collection of C-ITS messages, the UNSW report states (in section 5.1.3) that 'the proper channel for notification may need some thought'. Notification at each collection point (beacon, signal controller or motorways/highways cabinet) may not be practical. Providing notification during a registration or licensing process may be a relevant alternative but could be too remote from the collection.

Collecting sensitive information

Only the ACT, the Northern Territory, Victoria and Tasmania have specific requirements for collecting sensitive information. These provisions generally require the individual to consent to the collection or for the collection to be required or authorised by law, which are not requirements for collecting personal information. Each jurisdiction has other grounds for collecting sensitive information, but these are less relevant to the direct collection of C-ITS information by road agencies.

In practice, this may mean road agencies would need individuals to consent to the purposes the information is collected for, rather than just notifying individuals of these purposes.

[28] *Information Privacy Act 2014* (ACT) TPP 5(f).

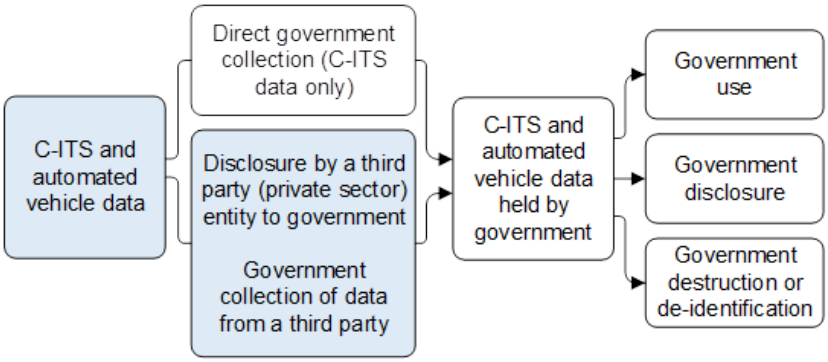
5.4 Government collection of information from third parties

In sections 3.4.1 and 3.4.3, we discussed the new privacy challenges of automated vehicle technology capturing new information, and C-ITS and automated vehicle technology generating a greater breadth and depth of information. These challenges relate to information government could obtain from third parties, such as the ADSE, rather than directly collect itself. We now consider how these risks are addressed by Australia's information access framework covering the collection of personal information by:

- outlining relevant existing and potential government powers to collect information
- explaining the potential for private sector entities to disclose information upon request (without government having a specific power to collect the information)
- analysing the applicability of surveillance devices laws
- considering relevant privacy regulation.

This section focuses on the highlighted part of Figure 6.

Figure 6. Government collection of C-ITS and automated vehicle data from third parties



5.4.1 Government powers to collect information

Collection powers under road transport laws

Some state and territory road transport laws contain provisions about information certain government entities can collect to administer the laws. Some of these powers could potentially cover some data generated by C-ITS and automated vehicle technology, including records relating to vehicle use and performance and location information (though the location information is limited to the current or intended journey of the vehicle).[29] It is not clear whether these provisions are broad enough to capture the provision of C-ITS and automated vehicle data. The collection is also usually limited to a specific purpose.

Passenger transport legislation in some states and territories may provide collection powers broad enough to capture automated vehicle data. For example, the *Point to Point Transport (Taxis and Hire Vehicles) Act 2016* (NSW) imposes a primary duty of care on passenger and booking service providers to ensure, so far as reasonably practicable, the health and safety of drivers and passengers.[30] In the future, operators of automated vehicles could fall into these categories. Data from in-cabin cameras, biometric, biological or health sensors and other safety-related technology in automated vehicles may be relevant to assessing

[29] See, for example, sections 40W and 40X of the *Road Traffic Act 1961* (SA) and sections 569 and 570 of the *Heavy Vehicle National Law*.

[30] *Point to Point Transport (Taxis and Hire Vehicles) Act 2016* (NSW) ss 12 and 13.

compliance with the primary duty of care. The Act provides powers for authorised officers[31] to require a person to produce documents or information.[32] This could include the automated vehicle data described.

Some road transport laws allow authorised officers to obtain a warrant to search premises for records, devices or things.[33] As discussed below, this may not cover intangible things such as data generated by C-ITS and automated vehicle technology.

State and territory law enforcement powers

Outside of road transport laws, state and territory laws contain generic law enforcement functions (or powers) and specific powers to compel information.

An example of the former is in the *Police Act 1990* (NSW), which outlines the general functions of police officers such as to provide police services for NSW.[34] For law enforcement entities wanting to collect information generated by C-ITS and automated vehicle technology, the UNSW report notes (at section 4.5.2) that these generic law enforcement powers 'help define the scope of 'enforcement related activities' for the purposes of federal and state law'. Enforcement related activities are relevant to considering exceptions from privacy principles, and are discussed in more detail below.

There are also more specific powers to compel information in both general police legislation (such as the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW)) and more specific legislation (detailed in section 4.5.2 of UNSW's report).

Certain provisions in the Law Enforcement (Powers and Responsibilities) Act may have some relevance to data generated by C-ITS and automated vehicle technology. For example, the Act creates a general power for a police officer to (without a warrant) stop and search a vehicle and seize and detain 'all or part of a thing that the police officer suspects on reasonable grounds may provide evidence of the commission of a relevant offence'.[35] Relevant offences are generally indictable offences, together with some more specific offences.[36] The UNSW report notes (in section 4.5.2) that '[t]here may be doubt whether 'thing' includes intangible information, as such powers are often read narrowly'. As such, the applicability of this power to data generated by C-ITS and automated vehicle technology is questionable.

The applicability of powers to compel data generated by C-ITS and automated vehicle technology in the more specific legislation is also unclear, and in many cases, requires a warrant or other authorisation.

Access under the *Telecommunications (Interception and Access) Act 1979*

Under the Telecommunications (Interception and Access) Act, telecommunications service providers are required to keep data about telecommunications (referred to as 'metadata') for a minimum of two years.[37] Such data includes the source, destination and time and duration of a communication.[38] Law enforcement agencies can access this data (without a warrant)

---

[31] Authorised officers include a police officer. See *Point to Point Transport (Taxis and Hire Vehicles) Act 2016* (NSW) s 3.

[32] *Point to Point Transport (Taxis and Hire Vehicles) Act 2016* (NSW) s 121.

[33] See, for example, *Road Traffic Act 1961* (SA) s 41B and *Road Safety Act 1986* (Vic) s 128.

[34] *Police Act 1990* (NSW) s 6. The definition of 'police services' is inclusive, and includes prevention and detection of crime and protection of persons from injury and death.

[35] *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) s 36.

[36] See *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) s 20.

[37] *Telecommunications (Interception and Access) Act 1979* s 187C.

[38] *Telecommunications (Interception and Access) Act 1979* s 187AA.

for investigations into criminal offences, offences involving a pecuniary penalty and for the protection of public revenue. Access to the content of communications generally requires a warrant or other authorisation.

The UNSW report notes (in section 4.2) that:

> *The relevance of these provisions to C-ITS and [automated vehicle] data is unclear. The telecommunications data is held by the telecommunications entity and would normally be related to communications from a mobile device or fixed line used by a person.*

If C-ITS messages are sent over the cellular network, they may be captured by the Act even though they may be communications between vehicles devices, rather than people. However, other C-ITS and automated vehicle data is unlikely to be covered by the legislation unless C-ITS and automated vehicle providers are themselves providing a telecommunications service. The UNSW report notes (in section 7.1) that 'ADSEs or C-ITS manufacturers may themselves be relevant entities under telecommunications legislation in the future'. Because this is quite speculative, the NTC has not considered it further at this stage but could address it at a later stage. Section 7 of the UNSW report provides more detail about the potential applicability of telecommunications legislation to C-ITS and automated vehicles.

Noting these uncertainties, the Act may in practice not provide powers for government to collect C-ITS and automated vehicle data.

Powers for specific bodies to compel information

Certain government agencies or bodies may have specific extra powers to compel the provision of information. Such bodies include:

- the NSW Independent Commission Against Corruption and the Victorian Independent Broad-based Anti-corruption Commission, who have anti-corruption roles
- the Australian Taxation Office, which has a role in tax evasion investigations.

A broad range of government agencies or bodies may have specific powers to compel information. Noting the number of entities this may cover, the NTC has not considered these powers or whether they cover C-ITS and automated vehicle data.

5.4.2 Potential new collection powers for automated vehicle compliance and enforcement are still to be developed

Police stakeholders indicated they would need to access certain automated vehicle data to determine whether the system or the human driver was in control of the vehicle in the event of a breach of a road traffic law or crash (discussed in more detail at 5.2.1). Police may require new powers to access this information. The inclusion of such powers will be considered as part of the NTC's compliance and enforcement approach to automated vehicles.

Any entities responsible for the automated vehicle safety assurance system may also require certain information collection powers. What such powers could look like is largely unknown at this stage because institutional arrangements for the safety assurance system have not yet been decided.

The outcomes of this discussion paper will help inform the development of any new collection powers for automated vehicle compliance and enforcement.

5.4.3 Disclosure by private sector entities upon request

For completeness, powers to compel information are often not a pre-requisite to government collecting information from private sector entities. The UNSW report notes (in section 4.6) that '[t]here may be circumstances where compulsory government collection powers do not exist, but third parties still provide information to government, in effect on a voluntary basis.' The UNSW report goes on to provide examples of such circumstances.

Such provision of information must be consistent with the use and disclosure privacy principles. Law enforcement disclosure exceptions in the APPs, which are discussed in section 5.4.5, would often allow private sector entities to disclose information to law enforcement agencies upon request. To develop and maintain consumer trust, private sector entities may not provide personal C-ITS and automated vehicle information to law enforcement unless 'utterly compelled by law' (Camac, 2017, p. 31).

However, stakeholders informed the NTC that entities would likely provide information to police upon request in line with their own privacy policies. An example of such a policy is Tesla's customer privacy policy:

> *With other third parties when required by law*
>
> *Tesla may transfer and disclose information, including information that may or may not personally identify you, to third parties to comply with a legal obligation (including, but not limited to, subpoenas); when we believe in good faith that the law requires it; in response to a lawful request by governmental authorities conducting an investigation, including to comply with law enforcement requirements; to verify or enforce our policies and procedures; to respond to an emergency; to prevent or stop activity we may consider to be, or to pose a risk of being, illegal, unethical or legally actionable; or to protect the rights, property, safety, or security of our products and services, Tesla, third parties, visitors, or the public, as determined by us in our sole discretion* (Tesla, 2018).

Other companies have similar policies about disclosing personal information to government and law enforcement agencies.

These policies suggest entities may disclose information to law enforcement agencies even where they are not legally obliged to do so. Even if this does not occur often, the possibility of disclosure may still impact on consumer willingness to take up C-ITS and automated vehicle technology.

5.4.4 Surveillance device laws and information from third parties

The surveillance devices laws framework is discussed in section 5.3.1. Like government-owned infrastructure or other roadside devices, in-vehicle C-ITS devices or private sector operated roadside C-ITS devices may also be data surveillance devices or tracking devices. Automated vehicle technology may fall within the definition of all four device categories. In-cabin and external cameras may be optical surveillance devices[39] and in-cabin and external microphones may be listening devices[40]. ECUs and navigation systems may be tracking devices. Some automated vehicle technology may also be a data surveillance device.

In this context, it is the ADSE or other private sector entity (rather than government) who will be doing the surveillance (if any). The entity may, however, provide the data generated by

---

[39] A *listening device* means any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing.

[40] An *optical surveillance device* means any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or similar devices used by a person with impaired sight.

the devices to government. If private sector entities collect data by carrying out unauthorised surveillance, the legality of the collection and any subsequent use or disclosure (including to government) of the information may be in doubt. Surveillance device laws could therefore restrict the disclosure by private sector entities to government of information generated by C-ITS and automated vehicle technology. For the following reasons, the NTC considers it is unlikely that surveillance device laws will, in practice, prevent such disclosure:

- Most devices are not covered in all jurisdictions. In section 5.3.1, we discussed that tracking devices and data surveillance devices are not covered in all states and territories. The installation, use and maintenance of optical surveillance devices is not covered in the ACT, Queensland or Tasmania. Listening devices are, however, covered in all jurisdictions.
- Express or implied consent of individuals is sufficient for use of any surveillance device to be legal. To avoid breaching surveillance device laws, private sector entities will likely seek consent (Camac, 2017, p. 30). Most C-ITS and automated vehicle technology captures information about vehicle occupants. Consent of individuals internal to the vehicle could be obtained relatively easily by, for example, including clear signage in the cabin interior.
- External cameras and microphones could capture information about individuals external to the vehicle. However, the use of external cameras and microphones would be unlikely to breach surveillance device laws because laws relating to listening devices and optical surveillance devices focus on listening to private conversations and recording private activities. When parties are external to the vehicle (on or near a public road), they should reasonably expect that their conversations and actions would not be private. [41]

As such, disclosure by private sector entities to government will likely be governed by privacy regulation rather than surveillance device laws.

5.4.5 Privacy regulation – information disclosed by third parties

Disclosure of personal information and sensitive information by the private sector

While private sector privacy regulation is outside the scope of this paper, privacy legislation covering disclosure by private sector entities is relevant to the government's ability to collect information. The UNSW report (in section 2.3) states that 'APPs cover private sector organisations (with turnover over $3m) and may influence their compliance obligations in responding to government requests for information from C-ITS or [automated vehicle] systems'.

The APPs require private sector entities to notify individuals (or to make individuals aware) of the purposes for which the personal information is collected, held, used and disclosed.[42] The NTC understands private sector entities would collect data generated by C-ITS and automated vehicle technology to enable the effective and safe operation of the vehicle. If entities expect to provide such data to government, then the notification provisions may require them to notify individuals of these disclosures. However, where provision of information to government happens infrequently or on an ad hoc basis, specific notification may not be required under the APPs. At the early stages of commercial deployment of C-ITS and automated vehicle technology it may be particularly difficult for entities to gauge whether and when they would disclose data generated by these technologies to government.

---

[41] For example, s 4 of the *Surveillance Devices Act 2007* (NT) provides that: "private activity" means an activity carried on in circumstances that may reasonably be taken to indicate the parties to the activity desire it to be observed only by themselves, but does not include an activity carried on in circumstances in which the parties to the activity ought reasonably to expect the activity may be observed by someone else.

[42] *Privacy Act 1988* (Cwlth) APP 5.

The APPs prohibit disclosure of personal information for a purpose (secondary purpose) that is not the original purpose (primary purpose) of collection, unless the individual consents, or another exception exists.[43] Noting that the likely primary purpose of private sector collection on C-ITS and automated vehicle data is to enable the effective and safe operation of the vehicle, it is likely that the purposes for which government may want to collect the information (outlined in section 5.2) are secondary purposes. In these circumstances, the private sector entity could rely on any consent obtained from the individual. The UNSW report notes (in section 5.6.2) that:

> *Consent may be sought for a wide range of collection, uses or disclosures which are not essential to the provision of a particular service. In some circumstances, the subject may have little practical choice but to consent. For instance, the operators of various systems in the C-ITS or [automated vehicle] environment may insist on a wide range of data uses as a condition for access to a vehicle's software.*

If the person's consent is not sought or obtained, the following exceptions in APP 6.2 are likely to be of most relevance:

- APP 6.2(a) – the individual reasonably expects the secondary purpose disclosure, and the secondary purpose is directly related to the primary purpose (for sensitive information) or related to the primary purpose (for non-sensitive information). The degree of relationship can be ambiguous, so this exception could apply in some circumstances but not others. Any notification provided to the individual would likely be a relevant consideration. Disclosure to government of non-sensitive information, which requires a relatively low threshold of relatedness, may be possible, while disclosure of sensitive information would be less likely.
- APP 6.2(b) – disclosure is required or authorised under law or a court/tribunal order. The current and potential new collection powers discussed in sections 5.4.1 and 5.4.2 respectively are relevant here. Current collection powers may allow limited disclosure of C-ITS and automated vehicle information in certain circumstances, including where the law did not anticipate that this information would be covered when it was drafted. Potential new collection powers may allow greater disclosure of automated vehicle information.
- APP 6.2(e) – the entity reasonably believes that disclosure is reasonably necessary for enforcement related activities of an enforcement body. Both 'enforcement related activity' and 'enforcement body' are broadly defined.[44] An enforcement body includes state and territory police and agencies responsible for administering or performing functions under laws imposing a penalty or sanction. An enforcement related activity includes the prevention, detection, investigation, prosecution or punishment of breaches of a law imposing a penalty or sanction. As discussed in section 5.4.1, the general functions of police officers in police legislation help to define the scope of enforcement related activities. Police functions are often very broadly described and include services to prevent and detect crime and protection from injury, death and property damage whether arising from criminal acts or otherwise.[45] This exception would most likely allow quite broad disclosure of personal information. Unlike APP 6.2(b), it could rely on the private sector entity providing the information upon request where it is not legally obliged to do so. The discussion in section 5.4.3, which considers disclosure by private sector entities upon request, is relevant here.

---

[43] *Privacy Act 1988* (Cwlth) APP 6.1.

[44] Full definitions are contained in *Privacy Act 1988* (Cwlth) s 6.

[45] See, for example, *Police Act 1990* (NSW) s 6(3).

APP 11.2, which requires taking reasonable steps to destroy or de-identify personal information, is also relevant because it could limit the information the private sector entity holds to disclose to government. These requirements do not apply if the entity still needs the information for any purpose for which the information may be used or disclosed, or the entity is required to retain the information under law. The former requirement in particular is relatively vague and broad and, in practice, may not actually limit the personal information the entity holds.

The EU GDPR could also limit the information the private sector entity holds. The UNSW report states (in section 8.1.1) that '[s]ome Australian businesses, including C-ITS or [automated vehicle] manufacturers or their service providers, could be subject to the GDPR if they have an establishment in the EU (irrespective of whether they process personal data in the EU)'. The following GDPR protections are relevant:

- Privacy by Design, under which individuals could customise the technology's ability to collect certain types of personal information, and Privacy by Default, under which individuals may need to opt-in to the collection of personal information by C-ITS and automated vehicle technology.
- Data Minimisation/Data Avoidance, which limits the collection of personal information to what is necessary for legitimate business purposes and requires deletion when the information is no longer necessary for these purposes. In relation to C-ITS and automated vehicle data, the GDPR may only allow collection of data to support vehicle operation and ensure safety. Unless there has been an accident or road traffic offence, this data should be deleted relatively quickly. However, entities could argue the data remains necessary for other related purposes such as for product safety research. This depends on how broadly 'necessity' is interpreted.
- Right to be Forgotten/Right to Erasure, which entitles individuals to require entities to delete their personal information when it is no longer necessary for the purpose for which it was collected or when the individual withdraws their consent and the entity has no other legal ground for holding the personal information. Individuals could argue that data particularly from in-cabin cameras and data from biometric, biological or health sensors is only necessary for a short period. However, this again depends on how broadly 'necessity' is interpreted.

The GDPR most likely offers stronger protections for personal information than the APPs. However, based on the analysis above, it may not in practice greatly reduce the amount of information available to government from private sector entities.

Collecting personal information and sensitive information from the private sector

The framework for government collection of personal information and sensitive information is outlined in section 5.3.2. For this current section, the focus is similarly on state and territory public sector agencies, noting that they are the most likely collectors of vehicle and transport data. However, we focus on a larger category of agencies – law enforcement in addition to road agencies. The privacy principles would generally apply in the same way as outlined in section 5.3.2. There are some differences, which we discuss below.

Where government collects information from a private sector entity, it would not be collecting an individual's personal information from the individual. Government would therefore need to rely either on consent (although this is an alternative only in some jurisdictions) or, more likely, on the fact that collection from the individual is not reasonable or practicable (which is an alternative in most jurisdictions). The UNSW report notes (in section 5.1.2) that:

> *Where C-ITS and particularly [automated vehicle] data is collected by the ADSE and not the individual, the individual will not themselves have access to the data. This may be considered 'unreasonable or impractical', since the individual cannot in practice provide it. If collecting the data is indeed*

necessary, secondary collection will thus most likely not conflict with the obligation in APP 3.6 or state and territory equivalents.

Where a public sector agency collects personal information from someone other than the individual, it must generally still comply with notification requirements (that is, notify individuals about the agency's collection of their personal information).

However, law enforcement agencies may not be subject to most of the collection requirements other public sector agencies are. Where noncompliance is reasonably necessary for the performance of law enforcement functions, state and territory privacy principles generally exempt law enforcement agencies from complying with requirements relating to collecting from the individual and notification. This means individuals may be unaware that their personal information has been collected by a law enforcement agency. Jurisdictions that cover sensitive information also exempt law enforcement agencies from complying with collection requirements specific to sensitive information where noncompliance is reasonably necessary for the performance of law enforcement functions.

5.5 Summary

While information generated by vehicle technology can inform and enhance government decision making, the new privacy challenges of C-ITS and automated vehicle technology mean that careful consideration must be given to balancing potential improved decision making with sufficient privacy protection for users.

5.5.1 Surveillance device laws are unlikely to provide material practical protections

The purpose of surveillance device laws to is to prevent covert surveillance rather than to regulate the collection, use and disclosure of personal information.

The NTC considers that surveillance device laws are unlikely to provide any material practical protections to individuals for government collection of personal information. This is because of the patchwork of surveillance device laws across the country, the uncertainty about which C-ITS and automated vehicle technology may constitute a surveillance device and the sufficiency of express or implied consent of individuals for parties to use these devices.

5.5.2 Privacy regulation may not sufficiently cover the new privacy challenges

As discussed below, privacy principles may not sufficiently address the new privacy challenges.

Privacy principles facilitate broad direct collection of C-ITS information

While privacy principles do not authorise the collection of personal information, they do not restrict (because they allow/permit) the direct collection of personal information by government agencies if the information is necessary for one or more of the agency's functions. This facilitates government's increased ability to directly collect C-ITS personal information. A road agency could collect C-ITS messages from vehicles by government-owned infrastructure or roadside devices for road and traffic management purposes. This collection can be characterised as direct collection from the individual and may legitimately fit within the broad principle of being necessary for one or more of the road agency's functions. While public sector agencies must notify individuals of the purpose of collection and intended recipients, they do not need to seek consent to collect for these purposes.

Public sector agencies would most likely need consent if they collect sensitive information. As discussed in section 4.5.2, location information from C-ITS technology may reveal sensitive information. In this case, public sector agencies may need to seek consent to

collect personal information for specific purposes, but it is not actually clear what information must be provided to individuals when seeking consent. In addition, there are other grounds for collecting sensitive information and sensitive information is not covered in all jurisdictions. As such, any additional protections for sensitive information are unlikely to be sufficient.

Law enforcement collection of C-ITS and automated vehicle data from third parties risks allowing a greater level of surveillance

The NTC considers that the main collection risk relates to law enforcement agencies collecting C-ITS and automated vehicle data from third parties. A private sector entity can disclose personal information to law enforcement if it believes disclosure is reasonably necessary for enforcement-related activities. Such enforcement-related activities are very broad and would likely allow disclosure of data generated by C-ITS and automated vehicle technology, including new information captured by automated vehicle technology (in-cabin cameras and biometric, biological or health sensors). Requirements in the APPs and the GDPR could limit the type and amount of information the private sector entity holds, which would limit the information available to government. However, the 'destroy or de-identify' requirements in the APPs are relatively vague and broad, and there is potential for a broad interpretation of what information is 'necessary' for entities to hold under the GDPR. As such, requirements in the APPs and the GDPR may not in practice greatly reduce the amount of information available to government from private sector entities.

On the collection side, law enforcement is exempt from complying with many personal information collection requirements where noncompliance is reasonably necessary for the performance of law enforcement functions. The NTC recognises that these exceptions apply on a case-by-case basis. However, the NTC considers that the 'reasonably necessary' argument could be made in many law enforcement contexts. Exemptions apply to notification requirements and to additional requirements when collecting sensitive information (such as seeking consent from the individual).

The NTC notes that, unless law enforcement bodies have specific collection powers or a warrant or other authorisation, they would need to rely on entities providing the personal information upon request when not legally obliged to do so. The views on whether entities would do so are mixed; however, the relatively broad statements in customer privacy policies leave open the possibility of entities disclosing personal information upon request by law enforcement. This may itself affect consumer willingness to take up C-ITS and automated vehicle technology.

The increased surveillance opportunity for law enforcement arises because law enforcement can collect the greater breadth and depth of information generated by C-ITS and automated vehicle technology, including new information captured by automated vehicle technology. The UNSW report states (in section 4.5.4):

> *A significant unresolved issue is whether data generated by C-ITS and [automated vehicle] technology could facilitate mass surveillance, since it will be produced in large quantities and some components will be potentially quite revealing. It may thus be seen as an opportunity by law enforcement agencies. There is a potential risk that this would allow a greater level of surveillance. To the extent that this develops, it is likely that citizen concerns about this potential will be expressed … and some consumers will avoid these technologies.*

This may be particularly problematic when coupled with individuals being unaware that they are under 'surveillance' (or investigation) because of the exemptions offered to law enforcement from many of the collection privacy principles in certain circumstances.

Consultation question

6. Is the current information access framework for government collection sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology? Please provide reasons for your view, including what parties may be affected if there is no change.

The next chapter considers whether Australia's information access framework is sufficient to cover the new privacy challenges of C-ITS and automated vehicle technology once government has collected the information.

6 Government use, disclosure, de-identification and destruction of information generated by vehicle technology

Key points

- State and territory privacy principles restrict the use of personal information to the purpose it was collected for unless an exception applies. Such exceptions are, in practice, likely to permit a wide range of secondary uses. Exceptions to restrictions on the disclosure of personal information similarly permit a wide range of secondary uses.
- The law enforcement exception to restrictions on the use and disclosure of personal information adds to the risk of increased surveillance opportunities outlined in chapter 5.
- Many state and territory road transport laws restrict the use and disclosure of information gathered in the administration of these laws but may not cover C-ITS and automated vehicle data. In addition, road transport laws themselves authorise many uses and disclosures of the information and contain provisions that facilitate information sharing between road agencies and police.
- Requirements to destroy or de-identify personal information are not consistent across the jurisdictions. Even where such requirements exist, they are unlikely in practice to greatly reduce the amount of personal information held by government.

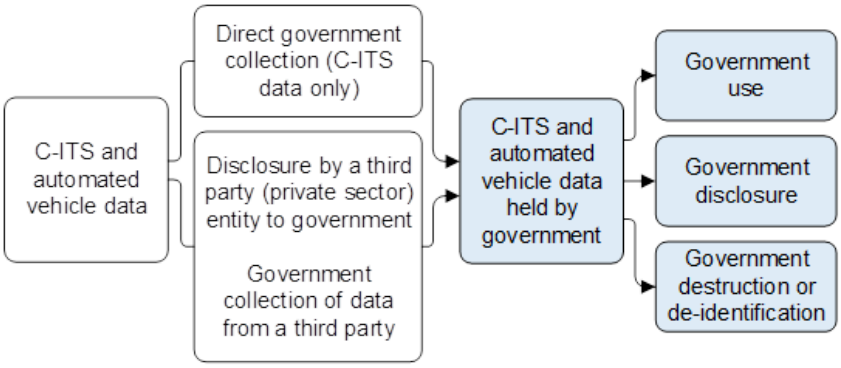
6.1 Purpose of this chapter

The purpose of this chapter is to:

- outline the privacy and other protections relevant to government use, disclosure, de-identification and destruction of information government has collected
- analyse whether Australia's information access framework relating to government use, disclosure, de-identification and destruction sufficiently covers the new privacy challenges from C-ITS and automated vehicle technology.

This chapter focuses on the highlighted part of Figure 7.

Figure 7. Government use, disclosure, destruction or de-identification of C-ITS and automated vehicle information



6.2 Use and disclosure in privacy regulation

Privacy regulations limit the secondary use and disclosure of information collected by government (either directly or from a third party). The purpose of collection is an important consideration because it helps to define acceptable secondary uses and disclosures.

We now consider protections in privacy regulation regarding the use and disclosure of personal information and sensitive information generated by C-ITS and automated vehicle technology. We again focus on state and territory public sector agencies because they are the most likely collectors of vehicle and transport data.

6.2.1 Government use of personal information and sensitive information for a secondary purpose

State and territory privacy principles permit public sector agencies to use personal information for the purpose it was collected (the primary purpose).

As discussed in sections 5.2.2 and 5.2.3, road agencies may collect C-ITS data to assist with network congestion, traffic management, traffic signal phase timing and future road investment. There may also be broader collection purposes, such as the administration of state and territory road transport laws. In the case of direct collection of information by government, the individual will be notified of the purpose of collection.[46] The road agency can then use the information it collects for the notified purpose(s).

Where government collects information from a private sector entity, the primary purpose of collection is likely to remain the purpose(s) notified to the individual by the private sector entity. The UNSW report notes (in section 5.2.3) that '[w]here the recipient third party, who may be government, 'uses' it for a purpose other than that for which it was collected or a related secondary purpose, it may be necessary to examine the basis by which this other use was authorised'.

Use for a purpose other than the purpose for which the information was collected (secondary purpose) is restricted, but, as noted in the UNSW report (in section 5.2.2), 'in practice the restrictions have exceptions substantial enough to permit a wide range of such uses'.

The degree of relationship required between the primary purpose and secondary purpose differs between jurisdictions and differs where information is sensitive information.

- Queensland and NSW allow use of personal information where the secondary purpose is directly related to the primary purpose.
- The ACT, Victoria, the Northern Territory, Tasmania and South Australia allow use of personal information where the secondary purpose is related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose.
- Jurisdictions that cover sensitive information (the ACT, the Northern Territory, Tasmania and Victoria) permit use of sensitive information where the secondary purpose is directly related to the primary purpose and where the individual would reasonably expect the organisation to use the information for the secondary purpose.

There are also other exceptions to the 'use for a secondary purpose' restriction. These vary across the states and territories but all include:[47]

- with the consent of the individual

[46] Notification requirements are discussed in section 5.3.2.

[47] With the exception of Western Australia because Western Australia does not have privacy principles.

- to prevent or lessen a serious threat to the life, health, safety or welfare of the individual or the public
- as authorised under another law
- for law enforcement purposes.

The secondary use exceptions would most likely allow law enforcement to use recordings from in-cabin cameras they may collect from ADSEs originally for automated vehicle compliance and enforcement purposes for secondary law enforcement purposes. In addition, stakeholders explained that law enforcement may collect personal information for broad law enforcement purposes and continue to use it for these broad purposes. In effect, this may mean the secondary purpose exceptions are not even considered.

6.2.2 Government disclosure of personal information and sensitive information

State and territory privacy principles restrict disclosure of personal information and sensitive information but include exceptions similar to the secondary use exceptions. Some differences are:

- In NSW, the 'related purpose' exception is narrower than for use, allowing personal information to be disclosed if 'the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure'.[48]
- In Queensland, there is no 'related purpose' exception for disclosure.

The disclosure exceptions would most likely allow road agencies to disclose for law enforcement purposes any location information revealed from C-ITS messages they collect.

The scenario below covers the law enforcement exceptions for collection, use and disclosure in the APPs and state and territory privacy principles and highlights the possible allowable movement of personal information.

Scenario: Exceptions for law enforcement purposes

Police collect information from XYZ, an ADSE, to determine who was in control of an automated vehicle at the time the vehicle ran through a red light. Having determined it was the human driver in control of the vehicle, police also collect information to determine whether the driver had *proper control* of the vehicle.

XYZ provides police with a video recording of the interior of the vehicle cabin that captures the driver and the vehicle's other occupants. The cameras are also used for driver and occupant recognition, so the video reveals both personal information and sensitive information. XYZ collected this information for the primary purpose of ensuring the effective and safe operation of the vehicle. XYZ can disclose this information to police for a secondary purpose because the exception in APP 6.2(e) applies – disclosure is reasonably necessary for an enforcement body's enforcement-related activities. The video recording assists police with determining whether the driver had his or her eyes on the road.

The video shows the driver potentially in an erratic state (looking frantically from side to side) and a large black bag in the back seat of the vehicle. State and territory privacy principles allow use or disclosure of personal information where it is reasonably necessary for certain law enforcement purposes. Therefore, police share the video with a second police team who they know is investigating a theft in the area where the red light offence

[48] *Privacy and Personal Information Protection Act 1998* (NSW) s 18.

occurred. The second team establishes reasonable grounds for questioning the driver for this theft by reference to the video footage.

If privacy regulation limits parties' ability to hold personal information, their ability to use and disclose personal information is also reduced. We discussed such limits on private sector entities in section 5.4.5 and found they are unlikely in practice to greatly reduce the amount of personal information held. We consider such limits on public sector agencies in section 6.4.

6.3 Use and disclosure in road transport laws

Most (but not all) state and territory road transport laws govern the use and disclosure of information gathered in the administration of these laws. Such information is largely registration and licensing information.[49] Unauthorised use or disclosure of this information is an offence.[50]

The UNSW report states (at section 5.3.5) that these provisions are:

> *…unlikely to cover C-ITS and [automated vehicle] data, unless this data is used for one of the monitoring purposes (such as those in the [Heavy Vehicle National Law], or other safety schemes), not the core registration and licensing purpose.*

In addition, the provisions specifically authorise many uses and disclosures. In Victoria, roads agencies can disclose the information to law enforcement agencies for the prevention, detection, investigation, prosecution or punishment of offences of any kind, and the enforcement of infringement penalties.[51]

There are also provisions governing use and disclosure in more specific road transport laws. These include provisions in the passenger transport legislation we discussed as part of government collection powers in section 5.4.1. The *Point to Point Transport (Taxis and Hire Vehicles) Act 2016* (NSW) prohibits the disclosure of information collected under the Act but provides exceptions to this prohibition. Most notably, it allows disclosure 'with other lawful excuse'.[52]

State and territory road transport laws also contain provisions that facilitate information sharing between road agencies and police. For example, the *Transport Operations (Road Use Management) Act 1995* (Qld) allows the chief executive (of the Department of Transport and Main Roads (TMR)) to enter into a written arrangement about giving and receiving information with the commissioner (of police), including the electronic transfer of information daily.[53] The *Transport Planning and Coordination Act 1994* (Qld) similarly enables the sharing of information between the chief executive (of TMR) and the chief executive officer of an approved agency (which includes the Queensland Police Service) for a law enforcement purpose.[54]

---

[49] See, for example, *Road Safety Act 1986* (Vic) s 90J. This provision also covers information relevant to automated vehicle trials.

[50] *Road Transport Act 2013* (NSW) s 101; *Transport Operations (Road Use Management) Act 1995* (Qld) s 143; *Motor Vehicles Act 1959* (SA) s 139D; *Road Safety Act 1986* (Vic) s 90Q; *Road Traffic (Administration) Act 2008* (WA) s 143A.

[51] *Road Safety Act 1986* (Vic) s 90K(g).

[52] *Point to Point Transport (Taxis and Hire Vehicles) Act 2016* (NSW) s 152.

[53] *Transport Operations (Road Use Management) Act 1995* (Qld) s 17E.

[54] *Transport Planning and Coordination Act 1994* (Qld) s 36I.

6.4 De-identification and destruction

Most states and territories include requirements to destroy or de-identify information after a period of time. These are primarily included in privacy principles.

The privacy principles in Victoria, the Northern Territory, Tasmania and the ACT closely mirror the requirements in APP 11.2 (discussed in section 5.4.5) and require public sector entities to take reasonable steps to destroy or de-identify personal information where it is no longer needed for any relevant purpose. In NSW, the privacy principles require public sector agencies to keep information 'for no longer than is necessary for the purposes for which the information may be lawfully used', after which the information must be disposed of securely.[55] Other jurisdictions do not appear to have such requirements in their privacy principles.

One of the NTC's assumptions when drafting this discussion paper (discussed in section 1.10) is that it is difficult to irreversibly de-identify personal information. Stakeholders noted it is very difficult for personal information collected by automated vehicles to be de-identified because of the breadth and depth of information collected and because the information likely contains many identifiers. In section 4.3.1 we note that identifiability is a feature of context, not just a quality of the information itself. As such, information that has been de-identified by one party (for example, a road agency) could perhaps be re-identified by another party (such as a law enforcement agency) through data linking. This is a relevant risk for C-ITS and automated vehicle data because the breadth and depth of data generated itself facilitates data linking (refer to the discussion in sections 3.4.3 and 4.4.3). The effectiveness of particular methods of de-identification are therefore not clear.

In addition, the circumstances when public sector agencies must destroy or de-identify personal information are relatively narrow and do not include circumstances where the information is still needed for broad relevant purposes (or sometimes 'any purpose'[56]). Some stakeholders explained that, in practice, information obtained for law enforcement purposes may rarely be deleted or disposed of because law enforcement agencies could use it for broad law enforcement purposes.

Consistent with the conclusions for private sector entities, requirements for public sector agencies to de-identify or destroy personal information are unlikely in practice to greatly reduce the amount of personal information held by government.

6.5 Summary

6.5.1 Exceptions to restrictions on secondary use and disclosure of personal information adds to the risk of greater surveillance

While state and territory privacy principles include restrictions on the use and disclosure of personal information, exceptions to these restrictions are, in practice, likely to permit a wide range of secondary uses.

The law enforcement exception is particularly broad. The scenario in section 6.2.2, which focuses on the privacy challenge of automated vehicle technology capturing new information, highlights the broad uses and disclosures the law enforcement exception may allow of personal information and sensitive information. It shows that once information is collected for a law enforcement purpose, government may continue to use and disclose it for other law enforcement purposes. This adds to the risk of greater surveillance identified in chapter 5, which focused on the initial collection of information by government. Specifically, the increased surveillance opportunity for law enforcement arises because law enforcement

[55] *Privacy and Personal Information Protection Act 1998* (NSW) s 12.

[56] See, for example, *Privacy and Personal Information Protection Act 1998* (Vic) IPP 4.2.

could use and disclose the greater breadth and depth of information generated by C-ITS and automated vehicle technology.

Any requirements to destroy or de-identify personal information are unlikely to reduce the risk of greater surveillance. Such requirements do not appear to greatly reduce the amount of personal information held by government because the circumstances requiring de-identification or destruction are narrow and not all states and territories include requirements. In addition, it is difficult to irreversibly de-identify personal information, especially personal information collected by automated vehicles. This means government can 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.

6.5.2 Road transport laws will most likely facilitate rather than restrict the disclosure of personal information

While many state and territory road transport laws restrict the use and disclosure of information gathered in the administration of these laws, these provisions may not cover C-ITS and automated vehicle data. In addition, road transport laws themselves authorise many uses and disclosures of the information. For example, similar to the exceptions in privacy regulation, information can be disclosed to law enforcement agencies for relatively broad law enforcement purposes.

Stakeholders have informed the NTC that road agencies would generally disclose information to police upon request, which further highlights the privacy challenge of C-ITS technology allowing for more widespread direct collection of location information by government. This is because government may be more willing to disclose information to police or other government agencies than private sector entities. Such disclosure of information by government is supported by provisions in state and territory road transport laws that facilitate information sharing between road agencies and police.

Consultation question

7. Is the current information access framework for government use, disclosure and destruction/de-identification sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology? Please provide reasons for your view, including what parties may be affected if there is no change.

Noting the issues identified in chapters 5 and 6, chapter 7 outlines options to address the new privacy challenges.

7 Options to address the privacy challenges

Key points

- This discussion paper presents 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 information (reform option)
  - option 3 – limit government collection, use and disclosure of automated vehicle information 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 information to specific purposes (reform option).
- This discussion paper presents 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)
  - option 2 – agree broad principles on limiting government collection, use and disclosure of C-ITS information (reform option)
  - option 3 – limit government collection, use and disclosure of all C-ITS information to specific parties and purposes (reform option).
- At this stage of C-ITS and automated vehicle development, the NTC considers that option 2 best addresses the identified problem and new privacy challenges for both C-ITS and automated vehicle technology.

7.1 Purpose of this chapter

The purpose of this chapter is to:

- summarise why Australia's information access framework does not sufficiently address the new privacy challenges of government collection and use of information generated by C-ITS and automated vehicle technology
- present options to address these new privacy challenges
- present the NTC's preliminary preferred option for C-ITS and for automated vehicle technology.

7.2 The new privacy challenges are not sufficiently addressed

Chapters 5 and 6 outline the NTC's analysis of why Australia's information access framework does not sufficiently address the new privacy challenges of government collection and use of C-ITS and automated vehicle technology.

The gaps identified primarily relate to potentially wide allowable collection, 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 because their purpose is to prevent covert

surveillance rather than to regulate the collection, use and disclosure 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. This facilitates government's increased ability to directly collect C-ITS personal information. Collecting C-ITS messages from vehicles via government-owned infrastructure or roadside devices can be characterised as direct collection from the individual. A road agency could collect this information for road and traffic management purposes, and this collection may legitimately fit within the broad principle of being necessary for one or more of its functions.
- Law enforcement collection, use and disclosure of C-ITS and automated vehicle data may result in increased surveillance opportunities:
    - Entities can disclose this information to law enforcement where they believe disclosure is reasonably necessary for enforcement-related activities.
    - Law enforcement is exempt from complying with many collection, use and disclosure privacy principles where such noncompliance is reasonably necessary for the performance of law enforcement functions. While the NTC recognises that these exceptions apply on a case-by-case basis, the argument that noncompliance is reasonably necessary could be made in many law enforcement contexts.
    - The increased surveillance opportunity for law enforcement arises because law enforcement could collect, use and disclose the greater breadth and depth of information generated by C-ITS and automated vehicle technology, including new information captured by automated vehicle technology.
- Road transport laws contain provisions to facilitate information sharing between road agencies and police. This supports road agencies disclosing information to police upon request.
- Requirements to destroy or de-identify personal information may not in practice greatly reduce the amount of personal information held by government because the requirements are narrow and are not included by all states and territories. In addition, stakeholders have noted it is very difficult for personal information collected by automated vehicles to be de-identified because of the breadth and depth of information collected and because it likely contains many identifiers. This means government could 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.

7.3 Separate options for C-ITS and automated vehicle technology

The NTC proposes separate options for addressing:

- the new privacy challenges of C-ITS technology
- the new privacy challenges of automated vehicle technology.

The NTC recognises there is a degree of overlap between C-ITS and automated vehicle technology. Certain vehicles may be equipped with both technologies, and some information produced by C-ITS technology (location, speed) will also be produced by automated vehicle technology. However, as indicated by Figure 2 (in section 1.1), automated vehicles can operate independently of C-ITS technology and vice versa. In addition, C-ITS technology and automated vehicle technology raises different risks and issues:

- The production of data by automated vehicle technology is self-contained (that is, data is produced when the automated vehicle operates). By contract, C-ITS technology is developed to communicate with one or more external C-ITS devices (including devices operated by government). Because of this difference, government can directly collect data generated by C-ITS technology but will most likely need to rely on third parties such as the ADSE to access data generated by automated vehicle technology.
- Automated vehicle technology can generate what may be considered as more sensitive information (particularly in-cabin video recordings and health information) which C-ITS technology cannot generate.

C-ITS information and automated vehicle information would need to be clearly defined to deal with any potential overlap.

The implementation options for C-ITS technology and for automated vehicle technology also differ.

- The issues identified and any recommendations relevant to automated vehicles arising from this paper will inform the NTC's broader automated vehicle reform development, rather than be standalone reforms.
- The NTC is not completing other C-ITS reform development. Austroads is currently developing a national framework for C-ITS. In 2013 SCOTI agreed broad recommendations requiring Austroads to consider privacy in developing the C-ITS framework (National Transport Commission, 2013).[57] The NTC understands that Austroads is currently developing a project brief and proposal for a major C-ITS platform project, and that 'data protection and privacy' would be a subproject. This approach is similar to that taken in the EU. As such, the issues identified and any recommendations relevant to C-ITS arising from this paper should further inform Austroads' overall consideration of privacy for the C-ITS national framework.

Consultation question

8. Are separate options for addressing the privacy challenges of C-ITS technology and of automated vehicle technology reasonable for achieving any future reform? Please provide reasons for your view.

7.4 Options for data generated by automated vehicle technology

7.4.1 Option 1 – Rely on the existing information access framework to address the new privacy challenges of automated vehicle technology (no change)

Option 1 is suitable if governments are satisfied that Australia's information access framework sufficiently covers the new privacy challenges of automated vehicle technology. This option:

- disregards the gaps identified in Australia's information access framework

[57] SCOTI agreed the following recommendations:

- That Austroads adopt privacy by design principles, including the undertaking of a privacy impact assessment, in the development of the C-ITS operational framework.
- That in the development and implementation of a C-ITS operational framework, in particular regarding standards for the data messages broadcast by C-ITS stations, Australian governments seek the highest possible level of anonymity for drivers and that this be a key focus for Austroads in developing the C-ITS operational framework.

- does not account for any potential new powers or authorisations that may be considered and developed as part of the NTC's broader automated vehicle reform development. Such powers or authorisations may further expand the scope of law enforcement purposes relevant to the exceptions in the privacy principles and therefore potentially expand law enforcement's ability to collect, use and disclose information.

7.4.2 Legislative reform options (options 2–4)

Options 2–4 (the reform options) all propose legislative reform placing limitations on the collection, use and disclosure of automated vehicle information to limit it to specific purposes. They are based on the NTC's analysis that:

- additional privacy protections are most likely needed to address the gaps identified in the information access framework
- privacy protections should be legislative to ensure they interact appropriately with legislative collection powers and other legislative privacy protections, and because guidelines would offer weaker protection.

The options do not propose amendments to privacy legislation (where it exists); rather, any additional privacy protections would be included as part of automated vehicle regulation.[58]

Common features of all reform options

The options focus on limiting the collection, use and disclosure of automated vehicle information to specific purposes. This is because 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.

All reform options consider four elements:

(1) a reference to automated vehicle information as **personal information**

(2) the **information we want to limit collection, use and disclosure of**. Each option would rely on, or build on, a definition of 'automated vehicle information'. Any definition of automated vehicle information should capture the categories of information likely to be generated by automated vehicles and be inclusive enough to capture emerging automated vehicle technology. This approach has been used previously in legislation such as the Heavy Vehicle National Law (HVNL) and state and territory road transport acts[59]

---

[58] A similar framework is included in the HVNL and state and territory road transport Acts. An example are provisions in the HVNL that cover electronic work diary (EWD) information.

- EWD protected information can only be used for an EWD authorised use. EWD protected information and EWD authorised use are defined in the HVNL.
- Authorised officers cannot obtain EWD protected information for a purpose other than the enforcement of a driver fatigue provision unless the information is authorised to be seized under a warrant.

[59] Examples of similar definitions include:

- s 727 HVNL: electronic work diary information means information generated, recorded, stored, displayed, analysed, transmitted or reported by an approved electronic recording system that constitutes an electronic work diary, or of which an electronic work diary is a part
- s 90J(1) *Road Safety Act 1986* (Vic): This Part applies to information that is collected or received by the Corporation in relation to its registration or licensing functions and activities and that identifies an individual or from which an individual's identity can be reasonably ascertained.

(3) the **specific purposes** for which automated vehicle information could be collected, used and disclosed.[60] These specific purposes could vary depending on the option chosen

(4) the **parties** to whom the specific purpose limitations apply. These could be parties who will most likely have compliance and enforcement responsibilities for automated vehicles – road agencies, agencies with law enforcement functions, the National Heavy Vehicle Regulator and agencies with responsibilities under the safety assurance system.[61] Parties that are not specified can collect, use and disclose information under standard privacy principles.

Additional elements of the reform options to cover other identified gaps

All the reform options could encompass the following elements, which have been identified as gaps in the ability of Australia's information access framework to cover the new privacy challenges of automated vehicles:

- requirements to destroy 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 (these requirements could be more specific than the current requirements to destroy or de-identify personal information)[62]
- requirements to notify individuals that their automated vehicle information has been collected.

The detail of each option is outlined below.

7.4.3 Option 2 – Agree broad principles on limiting government collection, use and disclosure of automated vehicle information

This option would seek agreement on broad principles. It recognises that:

- more detail around the overall automated vehicle legislative framework (including any new powers for government to collect automated vehicle information) is required before agreeing a clearer direction for limiting government collection, use and disclosure of automated vehicle information
- more detail and exploration is needed around the potential applications and benefits derived from government access to automated vehicle data, including in delivering value to the public.

These principles would form the agreed basis on which the NTC would progress the next stage of automated vehicle reform development.

These principles cover the following:

- Automated vehicle information is most likely personal information.

---

[60] For example, s 426 of the HVNL provides that Transport Certification Australia (TCA) may collect and hold intelligent access program (IAP) information for the exercise of its functions mentioned in section 425 or for law enforcement purposes.

'Law enforcement purposes' are relevantly defined in s 403 of the HVNL as 'the purposes of investigating or prosecuting an offence against an Australian road law'. This is much narrower than the law enforcement purposes provided in the privacy principles.

[61] For example, Chapter 7 of the HVNL contains provisions restricting the collection, use and disclosure of information by TCA and IAP auditors.

[62] For example, s 437 of the HVNL requires TCA to destroy IAP information or to remove personal information from it generally one year after collection.

- When establishing a regulatory framework that supports lawful access, use and disclosure, additional privacy protections are likely needed to appropriately limit the collection, use and disclosure of automated vehicle information to specific purposes.
- These privacy protections should be legislative.
- The privacy protections will need to specify:
    - the automated vehicle information covered (all automated vehicle information or a subset), noting that more sensitive automated vehicle information may warrant stronger protections than other automated vehicle information
    - the specific purposes this information can be used for (for example, automated vehicle compliance and enforcement). This will be considered in conjunction with any access powers developed as part of broader automated vehicle reform
    - the parties to whom the specific limitations apply (for example, road agencies, agencies with law enforcement functions, agencies with responsibilities under the safety assurance system).
- Privacy protections could cover additional elements (destruction, notification) to address other identified gaps. See 'Additional elements of the reform options to cover other identified gaps' above.

The detail of the draft principles is contained in Table 5 in section 7.6.

The NTC notes that options 3 and 4 would also inform the NTC's broader automated vehicle reform but provide a clearer direction for this development.

7.4.4 Option 3 – Limit government collection, use and disclosure of automated vehicle information from in-cabin cameras and biometric, biological or health sensors to specific purposes

This option could provide privacy protection for what may be the more sensitive information collected by automated vehicle technology. However, it does not necessarily address the issue that a greater breadth and depth of information likely to be generated by automated vehicles itself introduces risks. As such, it does not cover the third category of privacy challenge and is therefore less comprehensive than options 2 and 4.

Under this option:

- Automated vehicle information is expressly presumed to be personal information.
- Additional legislative privacy protections are introduced.
- 'Automated vehicle information' would include a subset to cover information from in-cabin cameras and biometric, biological and health sensors and the collection, use and disclosure of this information would be limited.
- The parties to whom the limitations apply would be road agencies, agencies with law enforcement functions, the National Heavy Vehicle Regulator and agencies with responsibilities under the safety assurance system.
- The specific purposes for which the information can be collected, use and disclosed would be for automated vehicle compliance and enforcement. This would include who was in control of an automated vehicle. It could also include enforcement of fallback-ready user provisions. These purposes would be refined as part of the NTC's broader automated vehicle reform development.
- The information could not be used for other purposes such as general road traffic law enforcement or criminal investigations unless:

- the party seeking the information has a warrant or court order authorising a different use, or
- the individual to whom the information relates provides written consent.

- Additional elements (destruction, notification) to cover other identified gaps are included. See 'Additional elements of the reform options to cover other identified gaps' above.

7.4.5 Option 4 – Limit government collection, use and disclosure of all automated vehicle information to specific purposes

Under this option:

- The features are similar to option 3, but the collection, use and disclosure of all automated vehicle information would be limited.
- The purposes for which the information can be collected, used and disclosed would vary, with stronger protections for some automated vehicle information and lesser protections for other automated vehicle information.
  - All automated vehicle information can be collected, used and disclosed for automated vehicle compliance and enforcement.
  - Information that is potentially less sensitive, such as information from electronic control units and event data recorders (or similar devices) can also be collected and used by road agencies for road and traffic management and strategic planning purposes provided it is aggregated.

This option may not be viable at this stage of automated vehicle reform development in Australia. This is because:

- specific privacy protections need to be considered as part of the overall automated vehicle legislative framework (including any new powers for government to collect automated vehicle information) without creating artificial barriers at this stage
- careful consideration needs to be given to ensure beneficial future uses of automated vehicle information are not limited.

A key challenge for this option is to ensure only relevant information is captured when defining automated vehicle information.

The potential problems of this law interacting with other laws that may allow collection of automated vehicle information (such as duplication and unintentional overriding of one law over another) also presents a challenge. The NTC notes that these other laws are likely limited and indirect.

7.4.6 The NTC's preliminarily preferred option

The NTC's preliminarily preferred option is **option 2**. The reasons for this are outlined below.

Based on the NTC's analysis and initial stakeholder consultation, the NTC considers that the options should be assessed against three criteria; 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.

Table 3 summarises the extent to which we consider each of the four options addresses the assessment criteria.

Table 3. Assessment of automated vehicle options against the criteria

	Option 1	Option 2	Option 3	Option 4
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	×	✓	✓ (partial – does not recognise all privacy challenges)	✓
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	×	✓	×	×

Option 1 meets one criterion but does not meet the other two criteria. This is because:

- it disregards the gaps identified in Australia's information access framework to address the new privacy challenges of automated vehicle technology
- it ensures that beneficial future uses of automated vehicle information are not restricted because it does not propose to impose any restrictions
- does not account for any potential new powers or authorisations that may be considered and developed as part of the NTC's broader automated vehicle reform development.

Option 2 meets all three criteria. This is because:

- it recognises that additional privacy protections are likely necessary to address the new privacy challenges of automated vehicle technology
- while recognising that government collection, use and disclosure of automated vehicle information should be appropriately limited, it does not require agreement on what these specific purposes are at this stage. As such, it ensures beneficial future uses are not restricted
- only agrees broad principles and therefore does not restrict further development of the overall automated vehicle framework, including new powers for government to collect automated vehicle information.

Option 3 only partially meets one criterion and does not meet the other two criteria. This is because:

- by focusing on specific types of automated vehicle information, it does not recognise that a greater breadth and depth of information likely to be generated by automated vehicles itself introduces risks
- it may restrict beneficial future uses of automated vehicle information because it specifies the purposes for which specific types of automated vehicle information can be used

- it may limit flexibility in developing the automated vehicle framework because it may prematurely determine one element of the framework when other related elements have not been fully developed.

Option 4 meets one criterion and does not meet the other two criteria. This is because it:

- recognises that additional privacy protections are likely necessary to address the new privacy challenges of automated vehicle technology
- may restrict beneficial future uses of automated vehicle information because it specifies the purposes for which automated vehicle information can be used
- may limit flexibility in developing the automated vehicle framework because it may prematurely determine one element of the framework when other related elements have not been fully developed.

Consultation questions

9. Are the criteria for assessing the automated vehicle reform options comprehensive and reasonable?
10. Is there is a need for reform to address the identified problem and the privacy challenges of automated vehicle technology (that is, option 1 is not viable)? At this stage of automated vehicle development, which option best addresses these privacy challenges while recognising the need for appropriate information sharing and why?

7.5 Options for data generated by C-ITS technology

All options will inform the development of the overall C-ITS framework, rather than be standalone reforms.

The C-ITS framework for Australia is currently being considered by Austroads. Any privacy considerations will likely be an element of this framework. As such, the NTC proposes that any option agreed inform Austroads' overall consideration of privacy for the C-ITS framework.

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

Option 1 is suitable if governments are satisfied that Australia's information access framework sufficiently covers the new privacy challenges of C-ITS technology.

Option 1 disregards the gaps identified in Australia's information access framework.

7.5.2 Reform options (options 2 and 3)

Options 2 and 3 (the reforms options) propose reform placing limitations on the collection, use and disclosure of C-ITS information to limit it to specific purposes.

The NTC considers these protections should be legislative to ensure they interact appropriately with legislative collection powers and other legislative privacy protections, and because guidelines would offer weaker protection. However, noting the NTC's proposal that the options only inform Austroads' consideration of privacy for the C-ITS framework, this is not a specific feature of the options.

Common features of both reform options

The gaps identified in the information access framework primarily relate to potentially wide allowable collection, use and disclosure of personal information, especially where

information is directly collected by government infrastructure or roadside devices, or for law enforcement purposes.

For these reasons, the options focus on limiting the collection, use and disclosure of C-ITS information to specific purposes and explicitly incorporating privacy by design elements where government directly collects C-ITS information.

Both reform options consider four elements:

(1) a reference to C-ITS information as **personal information**

(2) the **information we want to limit collection, use and disclosure of**. Each option could rely on a definition of 'C-ITS information' (for example, information broadcast and received by C-ITS devices). The NTC considers that a definition of C-ITS information should capture the categories of information likely to be generated by C-ITS technology and be inclusive enough to capture any future information not currently anticipated

(3) the **specific purposes** for which C-ITS information could be collected, used and disclosed. These purposes would likely differ depending on whether government directly collects C-ITS information or whether government collects information from third parties.

(4) the **parties** to whom the specific purpose limitations apply. Again, this could differ depending on whether government directly collects C-ITS information or whether government collects information from third parties.

Additional elements of the reform options to cover other identified gaps

All options could encompass the following elements, which were identified as gaps in the information access framework's ability to cover the new privacy challenges of C-ITS technology:

- requirements to destroy 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 (these requirements could be more specific than the current requirements to destroy or de-identify personal information). Where government directly collects C-ITS information, there could be a further requirement to instantly aggregate any information collected
- requirements to notify individuals that their personal C-ITS information has been collected
- where government directly collects C-ITS information, requirements for government to seek express consent of individuals or for individuals to be given the option to opt-out of government collecting their personal information. Whether these consent requirements are workable in all C-ITS deployment scenarios will need to be considered further.

While both options 2 and 3 only inform Austroads' overall consideration of privacy for the C-ITS framework, option 3 provides a clearer direction for this consideration. The detail of each option is outlined below.

7.5.3 Option 2 – Agree broad principles on limiting government collection, use and disclosure of C-ITS information

This option would seek agreement on broad principles. It recognises that:

- more detail and exploration is needed around the potential applications and benefits derived from government access to C-ITS data, including in delivering value to the public

- the C-ITS framework in Australia is in the early stages of development and more detail around the overall framework is required before agreeing a clearer direction.

These principles cover the following:

- C-ITS information is likely personal information
- When establishing a regulatory framework that supports lawful access, use and disclosure, additional privacy protections are likely needed to appropriately limit the collection, use and disclosure of C-ITS information to specific purposes.
- These privacy protections need to consider:
  - the C-ITS information covered
  - the specific purposes this information can be used for (for example, to assist with network congestion, traffic management, traffic signal phase timing; broader purposes if necessary)
  - the parties to whom the specific limitations apply (for example, road agencies, agencies with law enforcement functions, agencies with responsibilities under the C-ITS framework).
- Privacy protections could cover additional elements (destruction, aggregation, notification, consent and opt-out mechanisms) to address other potential gaps. See 'Additional elements of the reform options to cover other identified gaps' above.

More detailed draft principles are outlined in Table 5 in section 7.6.

7.5.4 Option 3 – Limit government collection, use and disclosure of all C-ITS information to specific parties and purposes

Under this option:

- C-ITS information is expressly presumed to be personal information.
- Additional privacy protections are introduced.
- Collection, use and disclosure of C-ITS information would be limited.
- The parties to whom the limitations apply would be road agencies, agencies with law enforcement functions and the agencies with responsibilities under the C-ITS framework.
- The specific purposes for which C-ITS information can be collected, used and disclosed would be by road agencies for network operations and strategic planning (including to assist with network congestion, traffic management and traffic signal phase timing). Law enforcement purposes would be explicitly excluded, except in relation to any C-ITS-specific compliance and enforcement functions. These purposes would be refined as part of considering the C-ITS compliance framework (particularly in relation to any functions of the agencies with responsibilities under the C-ITS framework).
- The information could not be used for other purposes such as general road traffic law enforcement or criminal investigations unless:
  - the party seeking the information has a warrant or court order authorising a different use, or
  - the individual to whom the personal information relates provides written consent.
- Additional elements (destruction, aggregation, notification, consent and opt-out mechanisms) to cover other identified gaps are included. See 'Additional elements of the reform options to cover other identified gaps' above.

This option may not be viable at this early stage of the development of a C-ITS framework in Australia. This is because careful consideration needs to be given to ensure beneficial future uses of C-ITS information are not limited. For example, C-ITS data may need to be collected by government to ensure the security of C-ITS communications. In addition, C-ITS could perhaps be used by government for road pricing. While this is likely to fall within network congestion and traffic management purposes, it may also have law enforcement elements.

The potential problems of this option interacting with laws that may allow collection of C-ITS information (such as duplication and unintentional overriding of one law over another) also presents a challenge. The NTC notes that these other laws are most likely limited and indirect.

7.5.5 The NTC's preliminary preferred option

The NTC's preliminarily preferred option is **option 2**. The reasons for this are outlined below.

Based on the NTC's analysis and initial stakeholder consultation, the NTC considers that the options should be assessed against three criteria; 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.

Table 4 summarises the extent to which we consider each of the three options addresses the assessment criteria.

Table 4. Assessment of C-ITS options against the criteria

	Option 1	Option 2	Option 3
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 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	×	✓	×

Option 1 meets one criterion and does not meet the other two criteria. This is because it:

- disregards the gaps identified in Australia's information access framework to address the new privacy challenges of C-ITS technology
- ensures that beneficial future uses of C-ITS information are not restricted because it does not propose to impose any restrictions
- may inadvertently limit the ability to include additional privacy protections as the C-ITS framework develops.

Option 2 meets all three criteria. This is because:

- it recognises that additional privacy protections are likely necessary to address the new privacy challenges of C-ITS technology
- while recognising that government collection, use and disclosure of C-ITS information should be appropriately limited, it does not require agreement on what these specific purposes are at this stage. As such, it ensures beneficial future uses are not restricted
- it only agrees broad principles and therefore provides appropriate flexibility for the development of the C-ITS framework.

Option 3 meets one criterion and does not meet the other two criteria. This is because it:

- recognises that additional privacy protections are most likely necessary to address the new privacy challenges of C-ITS technology
- may restrict beneficial future uses of C-ITS information because it specifies the purposes for which C-ITS information can be used
- may limit flexibility in developing the C-ITS framework because it may prematurely determine one element of the framework when other significant elements have not been developed.

Consultation questions

11. Are the criteria for assessing the C-ITS reform options comprehensive and reasonable?
12. Is there is a need for reform to address the identified problem and the privacy challenges of C-ITS technology (that is, option 1 is not viable)? At this stage of C-ITS development, which option best addresses these privacy challenges while recognising the need for appropriate information sharing and why?

7.6 Conclusion

At this stage of C-ITS and automated vehicle development, the NTC considers that option 2 best addresses the identified problem and new privacy challenges for both C-ITS and automated vehicle technology. This approach would help guide further development of the regulatory framework for C-ITS and automated vehicle technologies, whilst providing a sufficient degree of flexibility as the technology develops.

While we consider (for the reasons outlined in section 7.3) that options for addressing the privacy challenges of C-ITS technology should be separate to those for automated vehicle technology, we recognise that there is a degree of overlap in the issues and principles for both technologies. As such, we have developed a single set of draft principles to address the privacy challenges of both these technologies, noting that some principles may apply differently depending on whether we are considering C-ITS or automated vehicle technology. These principles are outlined in Table 5.

Table 5. Draft principles for addressing the privacy challenges of government access to C-ITS and automated vehicle data

Principle 1	C-ITS information and automated vehicle information must be clearly defined to ensure any additional privacy protections only capture relevant information.
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).
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.
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.
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.
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.
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.
Principle 8	Privacy protections for C-ITS and automated vehicle data should be regularly reviewed to ensure privacy is adequately protected.

The NTC proposes that these principles inform the next stage of our automated vehicle reform development, and Austroads' development of the C-ITS national framework.

Consultation question

13. Would the draft principles adequately address the privacy challenges of C-ITS and automated vehicle technology?

8 Next steps

Based on the outcomes of this discussion paper, the NTC will develop recommendations and next steps to implement the recommendations for the Transport and Infrastructure Council meeting in May 2019.

We expect that any recommendations relevant to automated vehicles agreed at the May 2019 meeting will inform our broader automated vehicle national reform program, including any compliance and enforcement options.

We also expect that any recommendations relevant to C-ITS agreed at the May 2019 meeting will inform Austroads' development of the C-ITS national framework.

Appendix A Relevant developments in Australia

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

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

The Commonwealth government has committed to:

- 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 data sharing and release activities of Commonwealth agencies. 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.

The Consumer Data Right is being developed by the Treasurer (The Treasury, 2018). The Department of Prime Minister and Cabinet has begun consulting on the implementation the other commitments by releasing an issues paper (Department of the Prime Minister and Cabinet, 2018).

The Commonwealth government's policy development highlights a move to improved data sharing, including between government agencies. In this discussion paper, the NTC is 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 Commonwealth 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* (Cwlth), 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 NSW (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 because the number of parties needing to provide consent would be much higher.

Cooperative and Automated Vehicle Initiative (CAVI) – C-ITS Pilot

The Department of Transport and Main Roads (TMR), the iMOVE Cooperative Research Centre and the Queensland University of Technology are conducting a 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 utilise both DSRC and cellular communication. DSRC will generally be used for safety and time-critical message transmissions (for example, emergency brake light). 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 is completing a privacy impact assessment to consider the potential impacts of the pilot on privacy.

Like the CITI light vehicle study, 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 My Health Records, which are online summaries of an individual's health information such as medicines they are taking, any allergies they may have and treatments they have received.

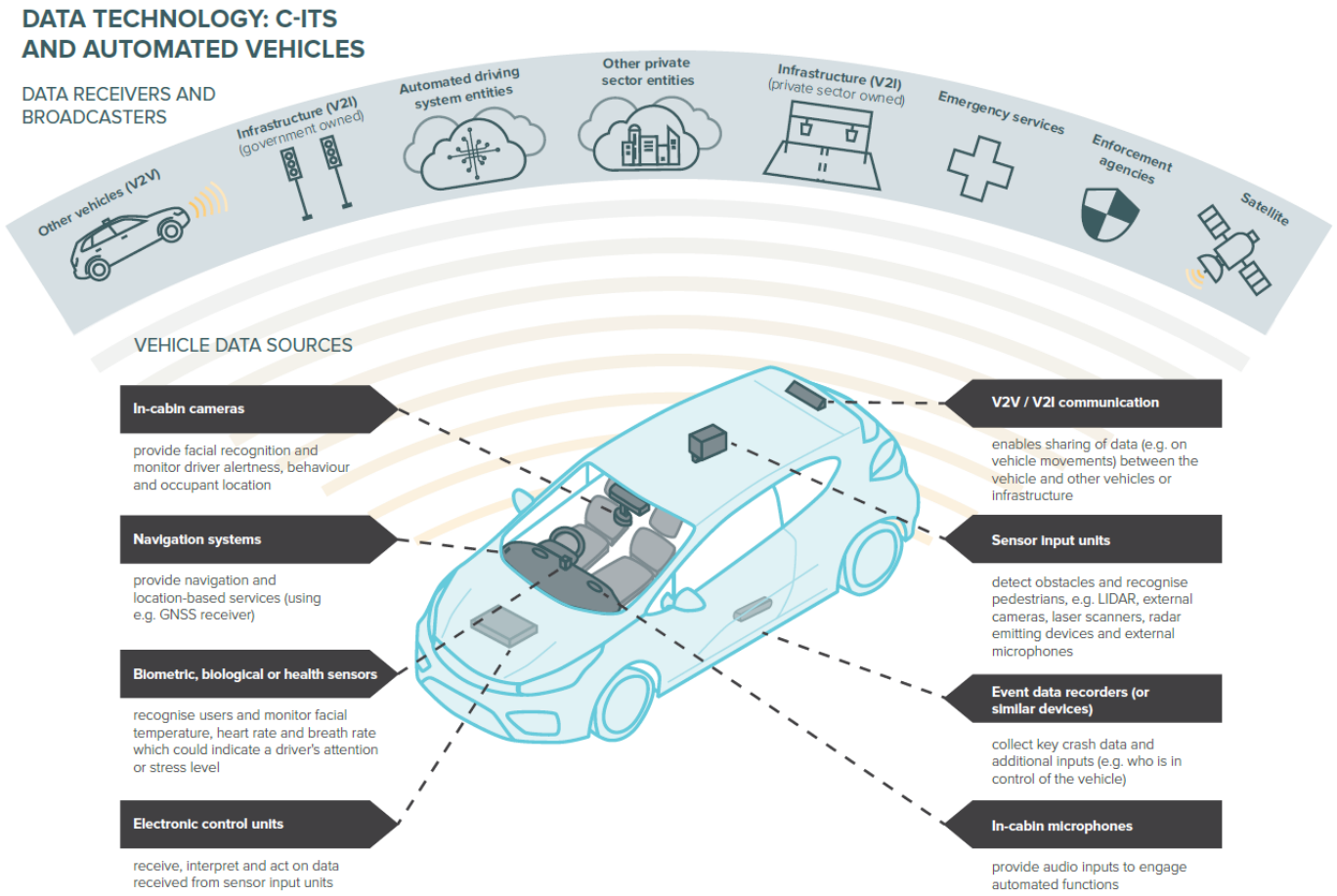
The *My Health Records Act 2012* limits when and how health information included in a My Health Record can be collected, used and disclosed. Unauthorised collection, use or disclosure of My Health Record information is both a breach of the My Health Records Act and an interference with privacy.

In July 2018 the Commonwealth government announced it will amend the My Health Records Act to strengthen the privacy provisions. The proposed amendments will require a court order to release a person's My Health Record information without consent and 'will ensure that no record can be released to police or government agencies, for any purpose, without a court order' (Hunt, 2018).

The proposed amendments appear to recognise that there may be privacy concerns associated with certain information that are not sufficiently covered by Australia's existing information access framework, and introduce specific restrictions on the collection, use and disclosure of this information by certain parties. This is consistent with the findings and options identified by the NTC in this discussion paper.

Appendix B Data technology: C-ITS and automated vehicles

Figure 8. Data technology: C-ITS and automated vehicles



Appendix C Potential use cases for government access to C-ITS and automated vehicle data

Table 6 outlines potential use cases that highlight the new privacy challenges of government access to C-ITS and automated vehicle data identified in chapter 3 of the discussion paper.

Table 6. Potential use cases for government access to C-ITS and automated vehicle data

Area	Use case	Likely data accessed
Roadside enforcement	(1) A vehicle is stopped by an enforcement officer for a random breath test of the driver. The enforcement officer conducts a random inspection of the vehicle.	Unclear what data will be relevant or how it will be accessed at the roadside.
	(2) A vehicle is stopped by an enforcement officer due to an observed traffic offence or on the suspicion of a traffic offence.	Various data may need to be accessed, depending on the traffic offence. Unclear how this data will be accessed at the roadside.
	(3) A vehicle is stopped by an enforcement officer due to suspicion of involvement in a crime other than a traffic offence.	Various data may need to be accessed, depending on the crime investigated. Unclear how this data will be accessed at the roadside.
Crash investigation	(4) A first responder is at the scene of a crash seeking information about the scene.	Unclear what automated vehicle information would be necessary.
	(5) An agency is undertaking a crash investigation and seeks to recover data from the vehicle post-crash.	Data from ECU (speed), EDR (or similar device) (including to determine who was in control at the time of the crash), in-cabin cameras and biological or health sensors (to gauge the driver's level of engagement). Large volume of various types of automated vehicle data could be relevant.
Investigation of an ADSE	(6) Entities responsible for automated vehicle safety assurance (ADS regulator(s)) seek vehicle data as part of an investigation into a suspected contravention of an ADSE's obligations.	Various automated vehicle information. The type of information needed would depend on the contravention. Large volume of various types of automated vehicle data could be relevant.
	(7) ADS regulator(s) seeks vehicle data as part of general ADSE compliance monitoring/auditing	Various automated vehicle information. The type of information needed would depend on what is needed for monitoring and auditing purposes. Large volume of various types of automated vehicle data could be relevant.

Area	Use case	Likely data accessed
Road traffic law enforcement	(8) Police seek access to vehicle data to determine who was in control of the vehicle at the time of a red-light offence caught by a traffic camera.	Various automated vehicle information. Likely information from ECUs and from devices similar to EDRs. Possibly also information from navigation systems.
	(9) Police seek access to vehicle data to enforce requirements on a fallback-ready user to remain sufficiently vigilant.	Image data internal to the vehicle and data from biometric, biological or health sensors can be used to monitor a driver's level of attention and alertness.
	(10) Police seek access to road agency data collected through C-ITS infrastructure as evidence of a speeding offence.	Vehicle speed.
Other criminal investigation	(11) Police seek access to vehicle data as part of a criminal investigation that is not a traffic offence (e.g. a theft in a particular area).	Various, depending on the crime investigated such as: location data of a suspect; in-cabin camera recordings of criminal behaviour occurring inside a vehicle; in-cabin camera recordings and data from health sensors (such as indicators of stress) as evidence of an individual's state of mind.
	(12) Police seek to access road agency data collected through C-ITS infrastructure to determine the travel history of a person of interest.	Vehicle position and direction as it travels on the road network.
	(13) Police seek real-time C-ITS information from a road agency to determine the current location of a vehicle suspected of being in the process of committing a crime.	Vehicle position on the network in real time.
Traffic management	(14) A road agency collects C-ITS information through roadside gantries to optimise signal phase and timing systems.	Various, but likely vehicle speed, direction and position on the network.
Infrastructure planning and research	(15) A road agency collects and analyses C-ITS data collected from a range of C-ITS devices (e.g. roadside gantries) for infrastructure planning or road safety research (e.g. to identify blackspots for future road investment).	Various data covering vehicle interactions with the road environment – including traffic flows and trip times.

Glossary

Term	Definition
automated driving system (ADS)[63]	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, on road conditions) between vehicles and infrastructure.
V2V	Vehicle-to-vehicle communication. The wireless exchange of data messages (for example, on vehicle movements) between vehicles.

[63] 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

Austraffic, n.d. *BlueTooth Based Technology.* [Online]
Available at: https://austraffic.com.au/projects/bluetooth-based-technology
[Accessed 18 June 18].

Australian Communications and Media Authority, 2018. *ACMA introduces new regulations to support intelligent transport systems.* [Online]
Available at: https://www.acma.gov.au/Industry/Spectrum/Spectrum-planning/About-spectrum-planning/acma-introduces-new-regulations-to-support-intelligent-transport-systems
[Accessed 1 June 2018].

Camac, N. T., 2017. *Autonom[y]ous: Australian Privacy Law and the Advent of Connected and Automated Vehicles,* Adelaide: s.n.

CEOS, n.d. *TIRTL.* [Online]
Available at: http://www.ceos.com.au/index.php/products/tirtl?id=10
[Accessed 18 June 2018].

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

Compare the Market, n.d. *3 ways dash cams are changing the world.* [Online]
Available at: https://www.comparethemarket.com.au/blog/car/3-ways-dash-cams-are-changing-the-world/
[Accessed 1 June 2018].

Culnane, C., Rubinstein, B. & Teague, V., 2017. *Health Data in an Open World,* Melbourne: The University of Melbourne.

Department of the Premier and Cabinet, 2018. *Service Priority Review.* [Online]
Available at:
https://www.dpc.wa.gov.au/ProjectsandSpecialEvents/ServicePriorityReview/Pages/default.aspx
[Accessed 24 September 2018].

Department of the Prime Minister and Cabinet, 2018. *New Australian Government Data Sharing and Release Legislation,* Canberra: Department of the Prime Minister and Cabinet.

El Dokor, T., 2016. *Autonomous Vehicles Need In-Cabin Cameras to Monitor Drivers.* [Online]
Available at: https://spectrum.ieee.org/cars-that-think/transportation/self-driving/autonomous-vehicles-need-incabin-cameras-to-monitor-drivers
[Accessed 20 June 2018].

Fallah, A., 2017. *Automatic Number Plate Recognition In Detail: We Go On Patrol With Queensland Police.* [Online]
Available at: https://www.caradvice.com.au/539545/automatic-number-plate-recognition-in-detail-we-go-on-patrol-with-queensland-police/
[Accessed 18 June 2018].

Government of Western Australia, 2017. *Policy Framework and Standards - Information Sharing Between Government Agencies.* [Online]
Available at: http://www.department.dotag.wa.gov.au/_files/Info_sharing_policy.pdf
[Accessed 4 July 2018].

Government of Western Australia, 2017. *Service Priorty Review - Blueprint for Reform,* s.l.: Government of Western Australia.

Hulme, S., Morgan, A. & Brown, R., 2015. *CCTV used by local government: Findings from a national survey,* Canberra: Australian Institute of Criminology.

Hunt, G., 2018. *Strengthening privacy protections for My Health Record.* [Online]
Available at: http://www.health.gov.au/internet/ministers/publishing.nsf/Content/health-mediarel-yr2018-hunt100.htm
[Accessed 31 July 2018].

Lawson, P. & Lawton, E., 2015. *The Connected Car: Who is in the driver's seat?,* Vancouver: British Columbia Freedom of Information and Privacy Association.

Legal Services Commission of South Australia, 2018. *Privacy (South Australian Government).* [Online]
Available at: https://www.lawhandbook.sa.gov.au/ch34s01s02.php
[Accessed 21 August 2018].

Lynch, C., 2016. *Dashcams prove popular for Aussie drivers.* [Online]
Available at: https://www.slatergordon.com.au/blog/dashcams-prove-popular-aussie-drivers
[Accessed 1 June 2018].

National Transport Commission, 2013. *Cooperative Intelligent Transport Systems,* Melbourne: National Transport Commission.

National Transport Commission, 2016. *Regulatory reforms for automated road vehicles - Policy paper,* Melbourne: National Transport Commission.

National Transport Commission, 2018. *Changing driving laws to support automated vehicles - Policy paper,* Melbourne: National Transport Commission.

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

OICA, 2018. *Data Storage System for Automated Driving (DSSAD).* [Online]
Available at: https://wiki.unece.org/pages/viewpage.action?pageId=56591466
[Accessed 27 June 2018].

O'Keefe, C. M. et al., 2017. *The De-Identification Decision-Making Framework,* s.l.: CSIRO.

Ombudsman Western Australia, 2013. *Guidelines for Agencies - Management of Personal Information.* [Online]
Available at: http://www.ombudsman.wa.gov.au/Publications/Documents/guidelines/MPI-Guidelines.pdf
[Accessed 4 July 2018].

Productivity Commission, 2017. *Data Availability and Use,* Canberra: Productivity Commission.

Queensland Government, 2016. *Automatic Number Plate Recognition rolled out to more QPS vehicles.* [Online]
Available at: http://statements.qld.gov.au/Statement/2016/8/12/automatic-number-plate-recognition-rolled-out-to-more-qps-vehicles
[Accessed 18 June 2018].

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].

Roads & Maritime Services, n.d. *Traffic Volume Viewer.* [Online]
Available at: http://www.rms.nsw.gov.au/about/corporate-publications/statistics/traffic-volumes/index.html#Howisdatacollected?
[Accessed 18 June 2018].

Tesla, 2018. *Legal - Customer Privacy Policy.* [Online]
Available at: https://www.tesla.com/en_AU/about/legal?redirect=no
[Accessed 6 July 2018].

The Medical Futurist, 2016. *The Driverless Car Is a Great Opportunity for Healthcare.* [Online]
Available at: https://medicalfuturist.com/the-driverless-car-for-healthcare
[Accessed 10 September 2018].

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

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].

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

VicRoads, 2016. *Traffic Management Centre.* [Online]
Available at: https://www.vicroads.vic.gov.au/traffic-and-road-use/traffic-management/traffic-management-centre
[Accessed 2 July 2018].

VicRoads, 2018. *Bluetooth Sites.* [Online]
Available at: http://data.vicroads.vic.gov.au/metadata/Bluetooth_sites.html
[Accessed 18 June 2018].

Victoria State Government, 2018. *Speed cameras.* [Online]
Available at: https://www.camerassavelives.vic.gov.au/how-cameras-work/camera-types/speed-cameras
[Accessed 18 June 2018].

Wauchope, M. C., 2014. *Policy Framework and Standards for Information Sharing Between Government Agencies.* [Online]
Available at: https://publicsector.wa.gov.au/sites/default/files/documents/2014-02_policy_framework_and_standards_for_information_sharing_between_government_agencies.pdf
[Accessed 4 July 2018].

Waymo, n.d. *Fact Sheet: LiDAR, the "eyes" of our self-driving car.* [Online]
Available at: https://storage.googleapis.com/sdc-prod/v1/press/Waymo_Lidar_Fact_Sheet.pdf
[Accessed 30 May 2018].

Weeratunga, K. & Somers, A., 2015. *Connected Vehicles: Are we ready?,* Perth: Main Roads Western Australia.