
FCAI Response to NTC Discussion Paper: Regulating Government Access to C-ITS and Automated Vehicle Data



Federal Chamber of Automotive Industries
Level 1, 59 Wentworth Avenue
KINGSTON ACT 2604
Phone: +61 2 6229 8217
Facsimile: +61 2 6248 7673

Contacts:
Mr James Hurnall, Technical Director
Mr Tony McDonald, Operations Director
26 November 2018

EXECUTIVE SUMMARY

The Federal Chamber of Automotive Industries (FCAI) is the peak industry organisation representing the importers of passenger vehicles, light commercial vehicles and motorcycles in Australia. The FCAI welcomes the opportunity to comment on the National Transport Commission's (NCT) Discussion Paper on Regulating Government Access to C-ITS and Automated Vehicle Data.

The NTC consider that Australia's current laws and regulations do not recognise automated vehicles or provide assurances for their safe design or operation. Therefore, the NTC's objective is to have an "end-to-end" regulatory system in place by 2020 to support the safe deployment of automated vehicles. As part of the end to end regulatory system, the NTC propose a safety assurance system (SAS) for automated vehicles to support the uptake and safe operation of automated vehicles on Australia's roads.

The technology for automated driving systems to deliver levels 3, 4 and 5 (conditional driving automation, high driving automation and full automation) will continue to evolve rapidly over the next few years. Even with this rapid development, mass market introduction of vehicles with high or full driving automation systems (i.e. levels 4 or 5) are unlikely to be available until at least 2030.

A small number of vehicles with level 4 or 5 systems may be introduced before 2030. However, it is expected that these will be either niche products (e.g. Navya shuttle) and/or in limited numbers as part of a closed fleet. These vehicles will not be "mass market" (i.e. available to be purchased by the general public) and will be operated under restricted conditions.

An important enabler to facilitate the introduction of increasing levels of automated driving systems, and especially high (level 4) and full (level 5) automated driving is the need for widespread compatible communications and road infrastructure. It must be recognised that provision of the necessary infrastructure will require significant financial investment over a very long period of time and will need to be rolled out in conjunction with the introduction of highly and fully automated vehicles. Clearly the wide-spread introduction of the necessary infrastructure in regional and rural areas of Australia will be a challenge which in turn means that operation of connected vehicles with high or full automation system (i.e. levels 4 or 5) in regional and rural areas are also unlikely in the short term.

Road regulations and vehicle regulatory standards will gradually develop on the back of the lead from the international market, and regulatory authorities will develop the necessary regulatory approaches for automated driving over time. Development of both road and vehicle regulations is underway at the international level via the United Nations (UN) Working Party 1 (WP.1) and Working Party 29 (WP.29) with changes to the Vienna Convention and the UN Regulations. The focus to date by WP. 29 has been on automated steering systems (UN R79).

The Discussion Paper proposes that government (the FCAI assumes mainly State/Territory governments' road and traffic authorities and Police [for traffic enforcement activities]) would collect data generated by C-ITS and automated vehicle technology to inform and enhance decision making in:

- Law enforcement.
- Traffic management and road safety as part of network operations to improve network efficiency.

- Infrastructure and network planning as part of strategic planning.

The NTC have identified the following as the privacy challenges from the the collection and use of data generated by C-ITS and automated vehicles:

- New information captured by automated vehicle technology (e.g. in-cabin cameras and bio-metric, biological or health sensors).
- More widespread direct collection of location information by government; i.e. the method and potential volume of data on individual vehicle movement (including speed, location, direction and date/time) collected.
- A greater breadth and depth of information that provides a greater opportunity for data linking by government.

The Discussion Paper presents four options for addressing the privacy challenges of automated vehicle technology, and a further three options to address the privacy challenges of C-ITS technology. The NTC proposed Option 2 for addressing the privacy challenges of both automated vehicle and C-ITS technology.

The FCAI supports the NTC's preferred approach, i.e. Option 2 - broad principles limiting government collection, use and disclosure of automated vehicle and C-ITS information, as this option best addresses the identified challenges while ensuring that governments can appropriately use information from future vehicle technology to benefit the community.

Recognising that modern motor vehicles generate different types of data, and that the data must be used and stored in an appropriate manner to ensure privacy is protected, the FCAI developed *Guiding Principles for Privacy and C-ITS* (Section 2.4). These principles are reflected within the NTC's draft principles.

Therefore, the FCAI supports the draft eight principles for addressing the privacy challenges of government access to C-ITS and automated vehicle data proposed by the NTC.

However, the NTC must treat C-ITS (i.e. connected vehicle) technology and automated vehicle technology as a single entity when considering the privacy implications of government access, collection, storage and use of vehicle data.

A major privacy challenge for consumer (and subsequently FCAI member brands) is the collection and use of C-ITS and automated vehicle data for secondary purposes. For example, use of data transmitted as V2X information in the Basic Safety Message for enforcement of traffic laws (e.g. speeding) could discourage the take-up of the technology leading to a slower introduction and delayed road safety and traffic management benefits. The FCAI considers the draft privacy principles should address this challenge.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	2
1.0 INTRODUCTION	5
2.0 OVERVIEW OF FCAI POSITION	6
2.1 <i>Background</i>	6
2.2 <i>International Harmonisation</i>	7
2.3 <i>Data vs Information.....</i>	8
2.4 <i>Guiding Principles for Privacy and C-ITS.....</i>	9
2.5 <i>Overview of NTC Proposal.....</i>	10
2.6 <i>Conclusion</i>	12
3.0 RESPONSES TO DISCUSSION PAPER	13
3.1 <i>Assumptions</i>	14
3.2 <i>Data generated by vehicle technology and the privacy challenges of C-ITS and automated vehicle technology.....</i>	14
3.3 <i>Is the information that is generated by vehicle technology personal information? ..</i>	15
3.4 <i>Government collection of information generated by vehicle technology.....</i>	15
3.5 <i>Government use, disclosure, de-identification and destruction of information generated by vehicle technology.....</i>	16
3.6 <i>Options to address the privacy challenges.....</i>	16
4.0 CONCLUSION	19
GLOSSARY	20

1.0 INTRODUCTION

The Federal Chamber of Automotive Industries (FCAI) is the peak industry organisation representing the importers of passenger vehicles, light commercial vehicles and motorcycles in Australia.

Modern vehicles¹ are complex machines with a range of sophisticated mechanical and electrical components and electronic modules that are integrated to deliver the performance, safety and emissions expected by customers and governments. Vehicle manufacturers are researching, developing and progressively introducing new technologies to make vehicles more automated and connected.

The technology for automated driving systems to deliver levels 3, 4 and 5² (conditional automated driving, high automated driving and full automation) will continue to evolve rapidly over the next few years. Even with this rapid development, mass market introduction of vehicles with high or full driving automation systems (i.e. levels 4 or 5) are unlikely to be available until at least 2030.

A small number of vehicles with level 4 or 5 automated driving systems may be introduced before 2030. However, it is expected that these will be either niche products (e.g. Navya shuttle) and/or within closed fleets. The vehicle will not be “mass market” (i.e. available to be purchased by the general public) and will be operated under restricted conditions.

Before the safety, environmental and mobility benefits of automated and connected vehicles can be realised several matters need to be considered – including government access to the data generated by the operation of automated and connected vehicles.

The FCAI notes that the NTC Discussion Paper is limited to examining whether additional privacy protections for government collection and use of information generated by connected and automated vehicles is needed.

¹ In this submission, the term ‘vehicle’ refers to light vehicles (passenger cars, SUVs and light commercial vehicles) and motorcycles.

² Levels of automated driving as per SAE J3016, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, Sep 2016

2.0 OVERVIEW OF FCAI POSITION

2.1 Background

There are challenges to achieve the right balance between allowing the introduction of automated vehicle technology and understanding the level of vehicle automation Australia is ready to accept for use on our road network.

The NTC has been reviewing the regulatory system and identifying the reforms required to facilitate the entry of connected and automated vehicles into Australia. This is being done by a range of projects:

- Automated vehicle trial guidelines.
- Automated vehicle exemption powers review.
- Clarifying control of automated vehicles.
- Safety assurance system for automated vehicles.
- Changing driving laws to support automated vehicles.
- Automated compulsory third party insurance review.
- Regulating government access to C-ITS and automated vehicle data.

The FCAI supported the development of enforcement guidelines to fill the gap between the current road rules (and driver being in control) and the future law that is still to be developed and aligned with international best practice for vehicles with conditional levels of automation (i.e. up to level 2). The FCAI supported national enforcement guidelines that are based on the human driver being in control of a vehicle with conditional automation, even when the automated driving system is engaged in the dynamic driving task.

The FCAI also supported the NTC's review of driving laws to support the introduction of automated vehicles. In our response to NTC Discussion Paper on Changing Driving Laws to Support Automated Vehicles, the FCAI advised that any changes to the driving laws required now should be aimed at facilitating the introduction of new models with automated driving (steering) systems over the next 5 to 10 years. Also, changes to driving laws will need to consider the principles for the development of vehicle regulatory standards (i.e. UN Regulations) that are based on the Vienna Convention.

The FCAI provided a detailed response to the NTC's consultation RIS on a Safety Assurance System for Automated Driving Systems. The FCAI considered that as the Australian government (NTC and DIRDC) were developing a regulatory system for "commercial deployment" of vehicles fitted with high levels (SAE levels 3, 4 or 5) ADS, the existing vehicle certification system (that accepts the international UN Type Approvals) must be utilized to provide the best avenue for early introduction of new technology.

The technology for automated driving systems to deliver levels 3, 4 and 5 (conditional automated driving, high automated driving and full automation) will continue to evolve rapidly over the next few years. Even with this rapid development, mass market introduction of vehicles with high or full automated driving systems (i.e. levels 4 or 5) are unlikely to be available until at least 2030. For example, the German vehicle manufacturers association, VDA, have an estimated timeline for introduction of various automated driving and parking systems (see Figure 2.1) through to 2030.³

³ <https://www.vda.de/en> [downloaded 20 Nov 2017]

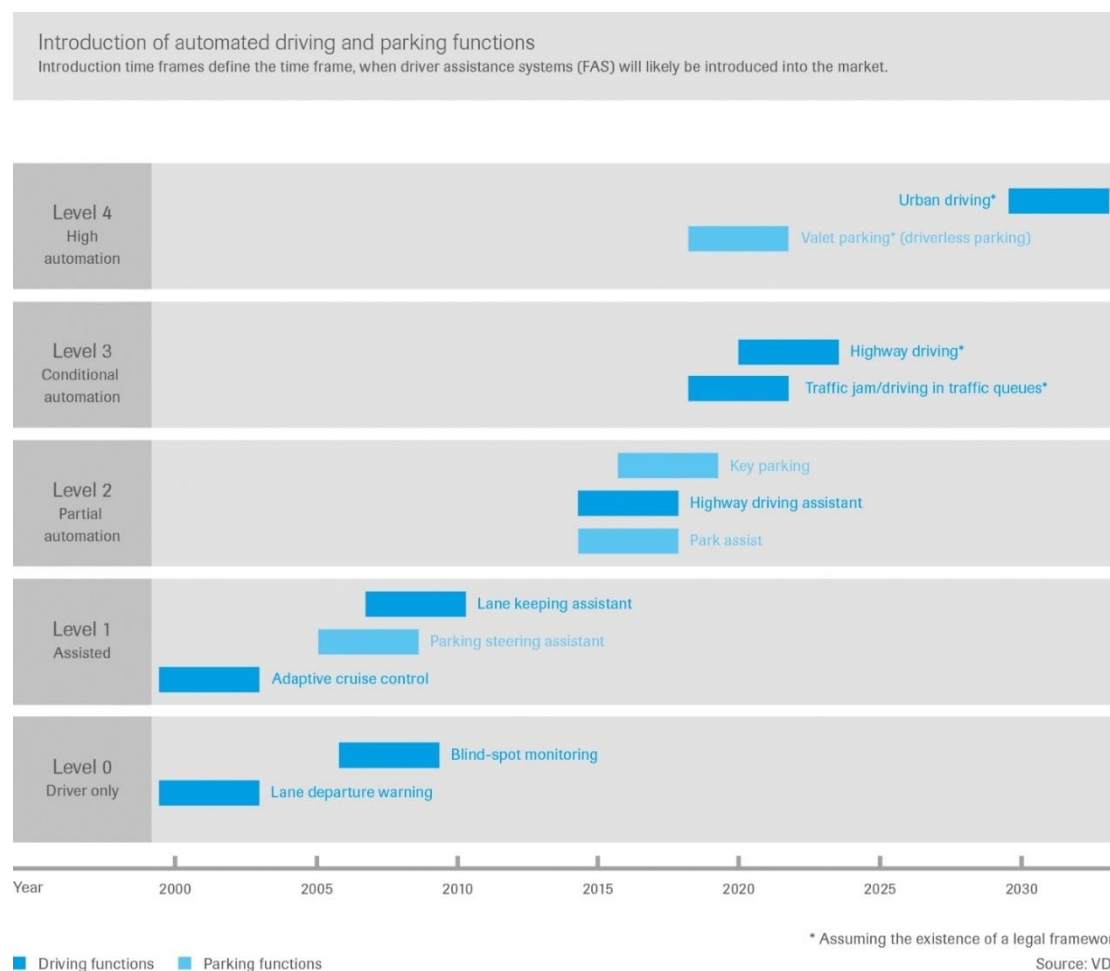


Figure 2.1 Introduction of Automated Driving Systems

With the average age of light vehicles in Australia, at just under 10 years,⁴ there will be a mixed (vehicles with varying levels of automation) in-service fleet for another 15 to 20 years after 2030 (i.e. out to 2045-2050).

A small number of vehicles with level 4 or 5 systems may be introduced before 2030. However, it is expected that these will be either niche products (e.g. Navya shuttle) and/or within closed fleets. The vehicle will not be “mass market” (i.e. available to be purchased by the general public) and will be operated under restricted conditions.

An important enabler in facilitating the introduction of increasing levels of automated driving systems, and especially high (level 4) and full (level 5) automation, is the need for widespread compatible communications and road infrastructure. It must be recognized that provision of the necessary infrastructure will take a significant period of time and will need to be rolled out in conjunction with the introduction of connected and highly/fully automated vehicles.

2.2 International Harmonisation

Australia is a small market, with annual sales of (approx.) 1.2 million new vehicles comprising just over 1% of annual global vehicle production (97 million in 2017). To facilitate the

⁴ Australian Bureau of Statistics, 9309.0 – Motor Vehicle Census, Australia, 31 Jan 2017

adoption of new technology at lowest cost, the FCAI supports harmonisation with international regulations and standards.

The international vehicle regulations (i.e. UN Regulations) are developed under “The 1958 Agreement” of which Australia is a Contracting Party.⁵ This means that any UN Regulation developed, will need to be considered by the Australian Government for adoption under the Australian Design Rules (ADRs). The FCAI supports harmonisation of ADRs with the UN Regulations, where it has been demonstrated the introduction of a vehicle regulatory standard is required.

Development of vehicle regulatory standards for automated vehicle systems is underway at the international level via the United Nations Working Party 29 (WP.29) with changes to the UN Regulation on Steering Systems (UN R79). Similarly, Working Party 1 (WP.1) is reviewing the driving laws and has amended the Vienna Convention, Article 8, to clarify that a human driver is in control of a vehicle, even if a vehicle system (that conforms to UN vehicle regulations or can be overridden or switched off by the driver) influences the way it is driven.⁶

In 2015 WP.29 initially created an Informal Working Group on Intelligent Transport Systems/Automated Driving (IWG-ITS/AD) where representatives from WP.1 participate. The Australian Government (through the Department of Infrastructure, Regional Development and Cities [DIRDC]) was an active participant in WP.29 and the relevant working groups. The global vehicle industry, through the global manufacturer’s association, OICA, participate in WP.29 and are very active in the IWG-ITS/AD to develop the necessary vehicle technical regulatory standards (i.e. UN Regulations) and certification procedures for automated driving systems.

Recently, WP.29 created a dedicated working group on Automated/Autonomous and Connected Vehicles (GRVA), to lead on the development of UN Regulations for the automation aspects of automated vehicles (e.g. UN R79 for automated steering functions). The first meeting of the new working group was held during 25-28 September 2018 and the FCAI expects that the Australian Government will be an active participant on GRVA.

The FCAI expects that the Australian government will adopt the relevant UN Regulations (as they are developed) as Australian Design Rules and incorporated into the Australian vehicle certification procedures (which accept the UN vehicle regulation type approvals) under its obligations as a signatory to the “1958 Agreement.”

2.3 Data vs Information

The FCAI considers that the NTC Discussion Paper is considering access to data, and not information, even though both words are used throughout the Discussion Paper.

It is important to distinguish between data and information. As outlined in the Productivity Commission’s Inquiry into *Data Availability and Use*⁷, data refers to a collection of material,

⁵Agreement concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations, Revision 3 (including the amendments which entered into force on 14 September 2017).

⁶ NTC Discussion Paper, *Changing driving laws to support automated vehicles*, October 2017, pp. 35-36

⁷ Productivity Commission, *Data Availability and Use*, Productivity Commission Inquiry Report, No, 82, 31 March 2017

which can include characters, text, words, numbers, pictures, sound or video. Data is unorganised material. Information is data that has been transformed by having been organised, collated, analysed and interpreted.

The FCAI developed this response on the understanding that the scope of the NTC's Discussion Paper is focused upon Government Access to 'data', not 'information'.

2.4 Guiding Principles for Privacy and C-ITS

Recognising that modern motor vehicles generate different types of data, and that the data must be used and stored in an appropriate manner to ensure privacy is protected, the FCAI developed the following Guiding Principles:

GUIDING PRINCIPLES:⁸

Data generated by or from motor vehicles can potentially deliver substantial benefits to individual drivers as well as to road users generally. For example, the data can be used to enhance safety, reduce the environmental impacts of vehicles and detect and/or prevent vehicle theft. The FCAI and its members recognise that consumers need to be confident that the data is being generated, used and stored in an appropriate manner and that privacy is properly protected. The principles set out below have been developed to give consumers this confidence.

Data Generation

Modern vehicles will generate different types of data including:

- a) Traffic information: collected by infrastructure owners, aggregated and de-identified data
- b) Owner/driver operation information: developed through use of the vehicle and can include data generated by both OEM and 3rd party systems, e.g. fleet management
- c) Vehicle Systems Operation: this is data contained within the vehicle management modules and is to meet both legislative and non-legislated requirements. This is the OEM intellectual property.

Principles

1. We will be transparent in our treatment or intended treatment of data generated by any of the above methodologies.
2. Where possible, we will give customers choice in the decision as to whether or not they wish to share data and information generated through owner/driver operation of the vehicle.
3. We will maintain data security to protect the personal information about our customers.
4. Where we need to process data generated through the use of the vehicle, it will be done in a manner that is adequate for the intended purpose, is relevant for that purpose, and if it is necessary to consolidate data it will be done so in a manner that de-identifies particular persons.

⁸ Guiding Principles for Privacy and Cooperative Intelligent Transport Systems, 23 February 2017, www.fcai.com.au [downloaded 2 October 2018]

5. Where information has been provided to the OEM/Distributor or their agent by the owner or registered user and that information on its own or in combination with other information identifies a person or elicits contact details, we will provide reasonable means to update or correct that information in instances where the information is held within the vehicle's original equipment.

Note: These principles do not replace nor supersede existing laws, in particular the Privacy Principles contained in the Privacy Act 1988 (Cwlth), nor members' existing privacy arrangements.

2.5 Overview of NTC Proposal

The NTC Discussion Paper is limited to examining whether additional privacy protections for government collection and use of information generated by connected and automated vehicles is needed. The Discussion Paper is clear in defining areas out of scope include:

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

The 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 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).

The NTC considers that Option 2; i.e. agree broad principles on limiting government collection, use and disclosure of automated vehicle and C-ITS information, best addresses the identified challenges (i.e. information from new vehicle technology, more widespread direct collection of location information and a greater depth and breadth) of information collected, while ensuring that governments can appropriately use information from future vehicle technology to benefit the community.

The NTC have proposed eight broad principles:⁹

- 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 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 protection 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 C-ITS and automated vehicle information collected by an agency will be used, collected 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 practical, 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.

⁹ NTC Discussion Paper, *Regulating Government Access to C-ITS and Automated Vehicle Data*, September 2018, p.5 Table 1

2.6 Conclusion

The FCAI supports the NTC's preferred approach, i.e. Option 2 - broad principles limiting government collection, use and disclosure of automated vehicle and C-ITS information, as this Option best addresses the identified challenges while ensuring that governments can appropriately use information from future vehicle technology to benefit the community.

The FCAI supports the draft eight principles proposed by the NTC. The FCAI's *Guiding Principles for Privacy and C-ITS* (Section 2.3) are reflected within the NTC's draft principles.

3.0 RESPONSES TO DISCUSSION PAPER

This section provides responses to each of the consultation questions raised in the Discussion Paper and is based on the FCAI's positions outlined in Section 2. In particular, this references the 3 types of data identified:

- Type a): Traffic information
- Type b): Owner/driver operation information
- Type c): Vehicle Systems Operation

The Discussion Paper proposes that government (the FCAI assumes mainly State/Territory governments' road and traffic authorities and Police [for traffic enforcement activities]) would collect data generated by C-ITS and automated vehicle technology to inform and enhance decision making in:

- Law enforcement.
- Traffic management and road safety as part of network operations to improve network efficiency.
- Infrastructure and network planning as part of strategic planning.

The FCAI supports the draft principles for addressing the privacy challenges of government access to C-ITS and automated vehicle data (see Section 2.5). The FCAI's *Guiding Principles for Privacy and C-ITS* (see Section 2.4) are reflected within the NTC's draft principles.

However, the Discussion Paper does not define what data will be collected and the FCAI seeks to understand what processes will be put in place by government(s) to determine what data and/or information will be collected and any implications. This is covered by draft principle 5b;

- Additional privacy protections should specify the specific purposes for which the information can be used.

Government collection, access and use of data needs to provide a net public benefit. For example, while it is widely accepted that C-ITS information will provide significant benefits to traffic management (FCAI Type 'a' data) and road safety (FCAI Type 'a' and 'b' data), the same information could be used for law enforcement of traffic laws. Use of the information for traffic law enforcement (e.g. speeding) could discourage the take-up of the technology leading to a slower introduction and delayed road safety and traffic management benefits.

The NTC have identified the following as the privacy challenges from the the collection and use of data generated by C-ITS and automated vehicles:¹⁰

- New information captured by automated vehicle technology (e.g. in-cabin cameras and bio-metric, biological or health sensors).
- More widespread direct collection of location information by government; i.e. the method and potential volume of data on individual vehicle movement (including speed, location, direction and date/time) collected.
- A greater breadth and depth of information that provides a greater opportunity for data linking by government.

¹⁰ NTC Discussion Paper, *Regulating Government Access to C-ITS and Automated Vehicle Data*, September 2018, pp.29-31

3.1 Assumptions

In the Discussion Paper, the NTC outlines the assumptions:

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

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

The FCAI considers assumptions 1 and 2 are reasonable.

As the NTC has only recently released the final policy position on the safety assurance system¹¹ the FCAI has not been able to fully review the final decision and cannot agree with assumption 3, i.e. that the safety assurance system will likely include a data recording and sharing criterion.

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

The NTC considers that the introduction of C-ITS and automated vehicle technology will lead to more data being generated by a greater array of sensors.

Question 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.

The NTC has mostly accurately captured current vehicle technology and anticipated C-ITS and automated vehicle technology.

One area that needs to be expanded is V2V/V2I Communication. The Discussion Paper (p.27) mentions “vehicle to other devices, such as personal mobile devices” however, the Discussion Paper should also recognise that road safety of vulnerable road users (pedestrians, cyclists, etc.) will be one of the benefits of C-ITS technology.

This section should recognise personal mobile devices and the role of digital road infrastructure and therefore, the heading should be changed to “V2X Communication.”

Question 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?

¹¹ NTC Decision Regulation Impact Statement, *Safety Assurance for Automated Driving Systems*, November 2018

A major privacy challenge for FCAI member brands is the collection and use of C-ITS data transmitted as V2X information in the Basic Safety Message (BSM in accordance with SAE J2735). As noted above, use of the BSM for enforcement of traffic laws (e.g. speeding) could discourage the take-up of the technology leading to a slower introduction and delayed road safety and traffic management benefits.

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

The NTC Discussion Paper (p.32) identifies “personal information” as the key concept when assessing the privacy challenges from data that will be generated by C-ITS and automated vehicle technology.

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?

As outlined in Section 2.3, the FCAI considers that data generated by the operation of the vehicle is personal information (FCAI Type ‘b’ data).

3.4 Government collection of information generated by vehicle technology

This section of the Discussion Paper outlines that 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 network and planning.

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.

The FCAI considers that the NTC should more accurately identify which parts of “government” will require access to data generated by the vehicle technology and for what purpose. Austroads have also recognised there may be a range of reasons that governments (as road infrastructure owners/operators) may wish to access, store and use C-ITS data.¹²

As outlined in Section 2.3, the FCAI has no objection to the use of traffic information (FCAI Data Level 1) that is collected, deidentified and used by government infrastructure owners to improve network efficiency and safety. However, the NTC needs to consider the privacy and ownership of any data collected and any subsequent sale/use by third parties. This is especially important considering the the identified challenges (i.e. information from new vehicle technology, more widespread direct collection of location information and a greater depth and breadth) of information collected.

¹² Austroads Research Report AP-581-18, August 2018, *Connected and Automated Vehicles (CAV) Open Data Recommendations*

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.

An important issue raised in Section 5.4.5 of the Discussion Paper (p.48) is collection of data by 3rd parties;

“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, the notification provisions may require them to notify individuals of these disclosures.”

The NTC has recognised that the data generated will be owned by vehicle owner/operator and cannot be disclosed without their approval and have included this the draft Principle 7b;

“Where government directly collects C-ITS information, governments should consider;

b. Obtaining consent from users.”

This same principle is reflected by the FCAI’s *Guiding Principles for Privacy and C-ITS* (Section 2.3).

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

In this section, the NTC outlines that current privacy regulations limit the secondary use and disclosure of information collected by government (either directly or from a third party). The purpose of the collection helps define acceptable secondary uses and disclosures. The NTC’s focus is on those state and territory public sector (government) agencies who will most likely collect and use C-ITS and automated vehicle data.

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.

The FCAI considers that C-ITS and automated vehicle data should only be used for the specific purpose it was collected for, and then deleted, rather than stored for any subsequent (or secondary) use.

As noted elsewhere in this submission, the use of C-ITS and automated vehicle data for other than immediate use (including traffic management and safety) could discourage the take-up of the technology leading to a slower introduction and delayed road safety and traffic management benefits.

3.6 Options to address the privacy challenges

The NTC considers that Australia’s information access framework does not sufficiently address the privacy challenges of government collection, storage and use of C-ITS and automated vehicle data. The NTC have identified gaps that relate to potentially allowing

wide collection, storage and use of personal information for secondary purposes including law enforcement.

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.

The FCAI considers that modern vehicles will be both connected and automated vehicles (CAV). This will be an evolutionary process with increasing levels of connectedness and automation as new systems are developed and new models with these systems are released to the market. Highly automated vehicle systems (levels 4 or 5) will be equipped with C-ITS technology and will require the necessary communication and road infrastructure to be connected and safely operate high or fully automated driving level systems.

Therefore, the NTC must treat C-ITS (i.e. connected vehicle) technology and automated vehicle technology as a single entity when considering the privacy implications of government access, collection, storage and use of vehicle data.

Question 9. Are the criteria for assessing the automated vehicle reform options comprehensive and reasonable?

Question 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?

The Discussion Paper presents four options for addressing the new privacy challenges of automated vehicle technology.

The FCAI supports the NTC's preferred approach, i.e. Option 2 - broad principles limiting government collection, use and disclosure of automated vehicle information, as this Option best addresses the identified challenges while ensuring that governments can appropriately use information from future vehicle technology to benefit the community.

Question 11. Are the criteria for assessing the C-ITS reform options comprehensive and reasonable?

Question 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?

The Discussion Paper presents three options to address the privacy challenges of C-ITS technology. The NTC proposed Option 2 for addressing the privacy challenges of C-ITS technology.

The FCAI supports the NTC's preferred approach, i.e. Option 2 - broad principles limiting government collection, use and disclosure of C-ITS information, as this Option best

addresses the identified challenges while ensuring that governments can appropriately use information from future vehicle technology to benefit the community.

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

The FCAI supports the draft eight principles for addressing the privacy challenges of government access to C-ITS and automated vehicle data proposed by the NTC.

The FCAI's *Guiding Principles for Privacy and C-ITS* (Section 2.4) are reflected within the NTC's draft principles.

4.0 CONCLUSION

The Federal Chamber of Automotive Industries (FCAI) is the peak industry organisation representing the importers of passenger vehicles, light commercial vehicles and motorcycles in Australia. The FCAI welcomes the opportunity to comment on the National Transport Commission's (NTC) Discussion Paper on Regulating Government Access to C-ITS and Automated Vehicle Data.

The Discussion Paper presents four options for addressing the new privacy challenges of automated vehicle technology, and a further three options to address the privacy challenges of C-ITS technology. The NTC proposed Option 2 for addressing the privacy challenges of both automated vehicle and C-ITS technology.

The FCAI supports the NTC's preferred approach, i.e. Option 2 - broad principles limiting government collection, use and disclosure of automated vehicle and C-ITS information, as this Option best addresses the identified challenges while ensuring that governments can appropriately use information from future vehicle technology to benefit the community.

Similarly, the FCAI supports the draft eight principles for addressing the privacy challenges of government access to C-ITS and automated vehicle data proposed by the NTC.

However, the NTC must treat C-ITS (i.e. connected vehicle) technology and automated vehicle technology as a single entity when considering the privacy implications of government access, collection, storage and use of vehicle data.

A major privacy challenge for consumer (and subsequently FCAI member brands) is the use collection and use of C-ITS and automated vehicle data for secondary purposes. For example, use of data transmitted as V2X information in the Basic Safety Message for enforcement of traffic laws (e.g. speeding) could discourage the take-up of the technology leading to a slower introduction and delayed road safety and traffic management benefits. The FCAI considers the draft principles for addressing the privacy challenges are appropriate.

GLOSSARY

Abbreviation	Term	Description
1958 Agreement		Agreement concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the basis of the United Nations Regulations, Revision 3 which entered into force on 14 September 2017
ACL	Australian Consumer Law	
ADR	Australian Design Rule	
ADS	Automated Driving System	NTC Discussion Paper; The hardware and software that are collectively capable of performing the entire dynamic driving task on a sustained basis. SAE J3016; The hardware and software that are collectively capable of performing the entire dynamic driving task (DDT) on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD); this term is used specifically to describe a level 3, 4 or 5 driving automation system.
ADSE	Automated Driving System Entity	NTC discussion Paper; 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	NTC Discussion Paper; derived from a combination of vehicle technology sources that together enable the operation of an automated vehicle.
CAV	Connected and Automated Vehicles	
C-ITS	Cooperative intelligent transport system	NTC Discussion Paper; 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		NTC Discussion Paper; 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.
DIRDC	Federal Government Department of Infrastructure, Regional Development and Cities	Responsible for administering the vehicle certification type approval system under Motor Vehicle Standards Act (to be replaced by the Road Vehicle Standards Act).
OICA	Organisation Internationale des Constructeurs d'Automobiles	International organisation of motor vehicle manufacturers and represents the industry at international forums such as WP. 29.
RVSA	Road Vehicle Standards Act	
SAE	Society of Automotive Engineers	
SAE J3016		SAE Surface Vehicle Recommended Practice, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, J3016, June 2018.
SAS	Safety Assurance System	
UN R	United Nations Regulation	UN Regulations contain provisions (for vehicles, their systems, parts and equipment) related to safety and environmental aspects. They include performance-oriented test requirements, as well as administrative procedures.
WP. 1		The UNECE Global Forum for Road Traffic Safety
WP. 29		The UNECE World Forum for Harmonization of Vehicle Regulations