22nd November, 2018

The Automated Vehicle Team
National Transport Commission
Level 3, 600 Bourke Street,
Melbourne, VIC, 3000
Submissions to: www.ntc.gov.au

Subject: TIC submission to the National Transport Commission's – Regulating Government Access to C-ITS and Automated Vehicle Data Discussion Paper, released September 2018

The Truck Industry Council (TIC) is the peak industry body representing manufacturers and distributors of heavy commercial vehicles (that is, with Gross Vehicle Mass above 3.5 tonne) or trucks in Australia. TIC members are responsible for producing or importing and distributing 17 brands of truck for the Australian market, totalling more than 32,000 units sold each year. In 2017, TIC members supplied to market over ninety-nine (99) per cent of all new on-highway trucks above 4.5 tonne Gross Vehicle Mass (GVM) sold in Australia. Additionally, TIC members also included two dedicated engine manufacturer members and two dedicated driveline manufacturer members who supply major engine and driveline systems for both on highway and off highway truck applications.

In this submission TIC will respond only to issues that relate to heavy road transport vehicles (that is, with GVM above 3.5t), however TIC believes that a united and uniform approach must be taken for both light vehicle and heavy vehicle regulation for Connected and Automated Vehicles, including data access and as such, the details contained in this submission should apply for any on-road Connected and/or Automated Vehicle.

Typically, and unlike light vehicles, many heavy vehicles have been using connected vehicle technologies for a number of years now to monitor such items as vehicle and driver performance, driver fatigue, cargo/freight condition (such as temperature), vehicle and cargo location, etc. These systems either store information/data on the vehicle for subsequent download and/or transmit the information/data (usually in "real-time") to a database, organisation, or person. The vast majority of these telematic systems are privately owned and monitored by the owner of the vehicle, or their authorised telematics system provider. However some systems are "owned" by a third party organisation, for example the customer of the freight goods, who may require location and/or condition monitoring of their cargo during the journey. The other common use for current telematics data is for government mass management schemes such the Intelligent Access Program (IAP), a scheme that monitors the location, time and in some cases speed of a heavy vehicle, allowing additional mass to be carried on specific routes at specific times and in some cases at specific maximum vehicle speeds. While IAP is a government scheme, the telematics system certification and data monitoring is provided by a third party provider. In these existing telematics use cases, an individual's (usually the vehicle's driver) information/data is governed by an agreement between the vehicles driver and the vehicle owner, or in the case of IAP type systems, the scheme details the rights and

obligations of the driver, vehicle owner, IAP information/data gatherer and the government authority who is administering the program. In most cases these "agreements" detail the rights of a person, or organisation, with respect to the information/data that is gathered and/or stored and what will be the use of this information/data, as well as what protection exists for an individual's privacy. As many of these "agreements" are typically work place agreements, or employment contracts, the protection and rights of an individual may vary.

Many of these existing connected vehicle telematics systems are retrofitted to a vehicle, though moving forward, such systems are more likely to be integrated into the vehicle and supplied by the vehicle manufacturer (OEM). It is important to recognise that any principals, or regulations, that control the access to information/data that is developed by these advanced technology systems and/or an automated vehicle, will have to deal with information/data that is generated from more than one legal "entity", or "source", within a vehicle. Both OEM and aftermarket retrofit connected and automated vehicle technologies may exist within a heavy vehicle, or heavy vehicle combination.

Definitions:

The above brief comments highlight that clear and concise definitions are essential when discussing issues about information, data, monitoring systems and technologies, telematics, connected and automated vehicles. TIC believes that the NTC Discussion Paper did not specifically define many of these terms concisely and at times used terms "interchangeably", or "generally", when a specific term, or definition, was required/appropriate. At this point TIC will define the use and definition/understanding of terms used in this submission. These TIC definitions may vary from the intent in the NTC's Discussion Paper, however the following must be used when reviewing this TIC submission.

Information: Is data that has been transformed by having been organised, collated, configured, manipulated, analysed and interpreted. Information is a "higher" level of data. TIC's responses below do not consider the term "information".

Data: Is a collection of material, which can include characters, text, words, numbers, pictures, sound or video. Data is unorganised, non-manipulated material and is the "lowest" level of material available. TIC's submission is based on the understanding that the NTC's Discussion Paper is focused upon government access to "data" and not "information".

Connected Vehicle: Is a vehicle that can be connected to any form of external device, or medium, for the transmission of data. This data transfer may happen at a specific point in time (such as a stationary download), or may take place in, or close to, a "real time" transfer of data. The data transfer may come from multiple separate systems in a single vehicle, or single vehicle combination. The data transfer may, or may not, be a function of an OEM system. The data transfer may, or may not, be a function of an aftermarket/retrofitted system. The data transfer may be from an onboard telematics system that monitors functions that a vehicle's OEM systems cannot determine (for example, driver fatigue).

Automated Vehicle: Is a vehicle that features advanced automated/autonomous driving features/functions that can operate to control some, or all, functions that would normally be conducted by the human driver. These automated/autonomous driving features/functions may operate automatically and without intervention by the human driver (for example ESC, ABS, AEB), or they may only operate once the human driver has made a conscious decision to deploy these features/systems.

Government: This term does not appear to be defined in the Discussion Paper. TIC has taken the term "government" to mean Federal, State and Territory government only and NOT lower levels, such as local government.

International Harmonisation:

Australia is a small market, with new heavy vehicle sales accounting for approximately 1% of annual global heavy vehicle production. To ensure the adoption of new vehicles and technology at lowest cost, TIC supports harmonisation with international regulations and standards.

Approximately 80 percent of new trucks sold in Australia derive their regulatory certification from Japan or Europe (both regions aligning with UN vehicle regulations), while 19 percent originate from an USA base and are certified to Australian Design Rules (ADR's) that are a mix of Australian, Euro and USA regulations. Australia is a Contracting Party under "The 1958 Agreement" to UN Regulations. This means that any UN Regulation developed, will need to be considered by the Australian Government for adoption under our ADR's. TIC supports harmonisation of ADR's with the UN Regulations, where it has been demonstrated the introduction of a vehicle regulatory standard is required and noting that Australia's unique multi-combination heavy vehicles may require specific regulatory standards.

Development of vehicle regulatory standards for automated vehicle systems, automated vehicle data capture (for use in crash investigation) and connected vehicle data transmission, is underway at the international level via the United Nations Working Party 29 (WP.29). Revisions to the UN Regulation on Steering Systems (UN R79) have been undertaken to capture advanced AV systems, these requirements have now been captured in ADR 90/00 by our regulators. 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 influences the way the vehicle is driven.

The Australian Government, through the Department of Infrastructure, Regional Development and Cities (DIRDC), is an active participant in WP.29 and the relevant working groups. While the global vehicle OEM's, through the global manufacturer's association, OICA, participate in WP.29 and are very active in the development of the necessary vehicle technical regulatory standards, UN Regulations and certification procedures for automated driving systems, data collection and storage and vehicle connectivity.

Recently, WP.29 created a dedicated working group for Automated/Autonomous and Connected Vehicles (GRVA), to lead on the development of UN Regulations for the automation aspects of AV's (for example UN R79 for automated steering functions). The first meeting of the new working group was held during September 2018. DIDRC has indicated that Australia will be an active participant in the GRVA.

The Australian government will adopt relevant AV, data and connectivity UN Regulations, as they are developed, as ADR's under its obligations as a signatory to the "1958 Agreement." ADR90/00 is the first such adoption of an UN AV regulation.

Timing Considerations:

The technology for automated driving systems to deliver SAE Levels 3, 4 and 5 (conditional automated driving, high degree 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 occur before 2030. TIC cautions Australian government not to "jump the gun" and develop unique Australian regulations for AV's. To do this would likely slow the uptake of such technology and vehicles in Australia, with OEM's required to develop unique AV hardware and software solutions for Australian deployment of AV's. Such development would be unlikely due to the cost recovery of such development in a small volume market such as Australia.

NTC Discussion Paper Scope:

TIC notes that the NTC Discussion Paper scope is limited to examining whether additional privacy protections (over and above existing protection mechanisms) for government collection and use of information (data) generated by connected and automated vehicles is needed.

The Discussion Paper is clear in defining areas that are out of scope, these include:

- Access to automated vehicle data by motor accident injury insurers.

- Obligations for Automated Driving System Entity (ADSE) 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 also presents three options for addressing the new privacy challenges of connected (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).*

In both cases the NTC considers that Option 2 best addresses the identified challenges while ensuring that governments can appropriately use information from future vehicle technology to benefit the community.

TIC Comment:
TIC supports the NTC's preferred approach, that is Option 2 for both automated vehicle data and connected vehicle data. TIC believes that this Option best addresses the identified challenges while ensuring that governments can appropriately use information from future vehicle technology to benefit the community.

The NTC have also proposed eight broad principles for addressing privacy challenges facing government for access to AV and C-ITS data (Table 1 of the Discussion Paper):

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.*

TIC Comment:

TIC supports the eight draft principles proposed by the NTC for addressing privacy challenges facing government for access to AV and C-ITS data.

TIC Responses to the Questions Posed in the Discussion Paper:

This section provides responses to each of the consultation questions raised in the Discussion Paper and is based on the 3 types of data identified in the Discussion Paper:
Type a): Traffic information
Type b): Owner/driver operation information
Type c): Vehicle Systems Operation

The Discussion Paper is based on an assumption that government would collect data generated by C-ITS and AV technology to inform and enhance decision making in:

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

However, the Discussion Paper does not define what data would be collected, nor how and when data would be collected (for example continuous "real time" data collection, download at the time of a potential infringement, or post event data collection and review) and TIC believes that these details should have been considered in the Discussion Paper. TIC is particularly concerned that government collection, access and use of data needs to provide a net public benefit. For example, while it is widely accepted that C-ITS vehicle information will provide significant benefits to traffic management and road safety strategies, the same information could be used for law enforcement (such as identifying speeding drivers). Such use as a law enforcement tool could discourage the take-up of these advanced system technologies, resulting in the

slower introduction of such features, delaying the road safety and traffic management benefits of AV and C-ITS technology.

3.1: The Discussion Paper details the following 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?***

TIC considers assumptions 1 and 2 are reasonable. TIC notes that the UN is currently developing a vehicle regulation for the capture and storage of AV data for use in crash investigation/s. TIC believes that Australia should NOT develop unique laws or regulations regarding the capture of AV and C-ITS data under an Australian unique safety assurance system. As such, TIC does not agree with, nor support, Assumption 3.

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 AV 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.***

TIC considers that the NTC has reasonably accurately captured current vehicle technology and anticipated future C-ITS and AV technology, however the Discussion Paper falls short of detailing all potential levels of C-ITS communication, detailing only V2V and V2I communication. This is a very narrow scope when compared to the more generally accepted view of V2X communications. An important example of V2X comms is vehicle to pedestrian mobile phone communication, allowing an array of vulnerable road user safety strategies to be investigated and deployed.

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?***

TIC believes that the Discussion Paper captures the major privacy challenges, however TIC remains concerned that AV and C-ITS data should not be gathered and used for “real time”, nor retrospective, law enforcement activities such as speeding. To allow data to be used for such proposes would likely discourage the take-up of C-ITS and AV technology, leading to a slower introduction and delayed road safety and traffic management benefits. TIC does not have any objection to such data being used for crash investigation purposes.

3.3: Is the information that is generated by vehicle technology personal information?
The NTC Discussion Paper 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?***

TIC believes that data generated by the use of the vehicle could potentially identify the driver and/or other occupants of the vehicle and/or its cargo/freight. TIC is of the opinion that this is personal/sensitive data

and should not be available to any person (other than the driver), or party, including government. TIC acknowledges that a private/personal agreement (for example an employment contract) could over-ride the access, or even ownership, of this type of 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 AV technology to inform and enhance decision making in law enforcement, traffic management and road safety, as well as 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.***

TIC supports the use of de-identified C-ITS and/or AV data for the purpose of traffic management, safety strategy planning and crash mitigation analysis. TIC does not support the use of personal C-ITS and/or AV "real time" data, or retrospective data analysis for law enforcement activities such as speeding. TIC also believes that the NTC must better define the term "government" when discussing data access availability and recommendations as to who can access C-ITS and AV data. Should, for example, a privately operated "toll" road operator have the same access rights to C-ITS and/or AV data for the use of traffic management planning in a similar manner as a State government road agency may, when using data for a similar purpose on a State owned public road?

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.***

As was detailed in TIC's opening comments, many heavy vehicles in Australia have been generating sensitive data for a number of years now, with much of this data being captured, stored and used by third party organisations, the examples of IAP and private company telematics were sited earlier in this submission. The current information access framework for government collection of AV and C-ITS data appears to be sufficient to cover current privacy issues. This "balance" may be disrupted if government, either directly, or using third party organisations, was to increase its "reach" for C-ITS and automated vehicle technology data. The NTC has recognised in the Discussion Paper that much of the data generated will be owned by the driver and/or vehicle owner/operator and cannot be disclosed without their approval and this has been included this the NTC's Draft Principle 7b. TIC supports this approach.

3.5: Government use, disclosure, de-identification and destruction of information generated by vehicle technology.
The NTC details 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 AV 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.***

TIC believes that AV and C-ITS vehicle data should only be used for the specific purpose/project that it was collected for, after its intended use the data should be deleted and not stored or kept in any format for any subsequent (or secondary) use. Abuse of this principal could lead to a lack of consumer trust, leading to potential uncertainty of the use of data obtained from these vehicles/systems. In turn leading to a slower uptake of AV and/or C-ITS vehicles and their data systems, delaying the road safety and traffic management benefits that could be afforded by this technology.

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 Discussion Paper has 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.***

TIC believes that heavy vehicles may be fitted with different (not controlled by the one source, system or entity) C-ITS and/or of automated vehicle technologies. While in other cases the integration of C-ITS and AV technology will be "as-one" and "seamlessly" integrated into the vehicle, the latter being provide typically by the vehicle OEM. Irrespective of the integration, or separation, of both C-ITS and of automated vehicle technologies, TIC believes that a common position/methodology should be possible to address the privacy issues associated with these systems/technologies. Data needs to be categorised by ownership, for example personal, vehicle and government, beyond this, the source of the data that an AV system or C-ITS system generates is not significant.

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

TIC believes that the NTC Discussion Paper presents a balanced and wide ranging review of the criteria for assessing the automated vehicle reform options, as summarised in Table 3 of the Discussion Paper. The NTC also draws parallels to existing automated heavy vehicle data systems such as IAP and Electronic Work Diaries (EWD's), highlighting the associated laws that protect both the privacy and the general rights of the heavy vehicle driver/operator, working within these electronic data schemes.

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?***

TIC supports the NTC's preferred approach, that is, Option 2 - *broad principles limiting government collection, use and disclosure of automated vehicle information*. TIC believes that this Option offers the best balance of identifying challenges while ensuring that governments can appropriately use information from these emerging vehicle technologies to benefit the broader community.

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

TIC believes that the NTC Discussion Paper presents a balanced review of the criteria for assessing the C-ITS vehicle reform options, as summarised in Table 4 of the Discussion Paper. The NTC Discussion Paper also recognises that C-ITS vehicle data technology is still in its infancy, both in Australia and globally and the need for potential regulation has not been adequately established at this point in time, while highlighting that regulation flexibility is currently important so as not to stifle development, or impede this technology's uptake.

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?***

TIC again supports the NTC's preferred approach, that is, Option 2 - *broad principles limiting government collection, use and disclosure of C-ITS vehicle information*. TIC believes that this Option offers the best

balance of identifying challenges while ensuring that governments can appropriately use information from these emerging vehicle technologies to benefit the broader community.

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

TIC supports the eight draft principles developed by the NTC and detailed in the Discussion Paper, for use in addressing the privacy challenges of government access to C-ITS and automated vehicle data identified by the NTC.

I trust that you find TIC's submission acceptable and that the issues that have been raised in this document will be considered in the review and formulation principals to support the collection storage and access of data generated by connected and automated vehicles in Australia.
Please contact the undersigned, on 0408 225212 or m.hammond@truck-industry-council.org for any questions about this submission.

Yours faithfully,

Mark Hammond
Chief Technical Officer