Transport Certification Australia

TCA SUBMISSION TO NATIONAL TRANSPORT COMMISSION DISCUSSION PAPER

TCA SUBMISSION: REGULATING GOVERNMENT ACCESS TO C-ITS AND AUTOMATED VEHICLE DATA

29 NOVEMBER 2018

CONTACT

Transport Certification Australia
Level 6, 333 Queen Street
Melbourne VIC 3000

Phone: + 61 3 8601 4600
Email: tca@tca.gov.au
Website: www.tca.gov.au

TCA SUBMISSION: REGULATING GOVERNMENT ACCESS TO C-ITS AND AUTOMATED VEHICLE DATA

29 NOVEMBER 2018

Transport Certification Australia Ltd
T: +61 3 8601 4600
E: tca@tca.gov.au
W: www.tca.gov.au

ABN 83 113 379 936

DOCUMENT DETAILS

Title:	TCA submission: Regulating government access to C-ITS and automated vehicle data
Document Number:	TCA-029
Version	03
Version Date	29 November 2018
Custodian	John Gordon

TCA page numbering convention: for ease of digital readability and referencing the cover is page 1.

ABOUT US

Transport Certification Australia (TCA) is the national government body responsible for providing assurance in the use of telematics and related intelligent technologies.

The term 'telematics' refers to systems which exchange data between vehicles and other locations, including:

- Vehicle to infrastructure (V2I) applications
- Vehicle to vehicle (V2V) applications
- Vehicle to elsewhere (V2X) applications.

OUR MISSION

To support government agencies and regulators by providing outcome-focused, technology neutral, disruption-resilient programs that address:

- Security
- Privacy
- Encourage innovation
- Facilitate an appropriate private sector contribution to the costs of regulation.

WHAT WE DO

Advice founded on a demonstrated capability to design and deploy frameworks and platforms as enablers for reform

Accreditation in the type-approval and certification of telematics and intelligent technologies and services, that give confidence to all stakeholders for their consideration and use

Administration of applications founded on the National Telematics Framework.

THE NATIONAL TELEMATICS FRAMEWORK

TCA is responsible for the management of the National Telematics Framework.

The Framework is a contemporary digital business platform which delivers:

- Public outcomes through an open technology market, which sustainably delivers upon the needs of government, industry and end-users
- Different assurance levels, based on objectives and risks of each telematics application
- Consistency and certainty to technology providers, so that government positions can be relied upon to make investment decisions
- Competition and choice, with technology providers delivering the latest technological developments at lower costs.

The National Telematics Framework has been adopted as an international standard by the International Standards Organization (ISO).

LINKING PRODUCERS AND CONSUMERS

Similar to other operational frameworks in other portfolios and industry sectors, the National Telematics Framework provides the enabling infrastructure, rules and administrative arrangements which bring together 'producers' and 'consumers'.

The structured interaction of producers and consumers deliver:

- Public outcomes sought by governments, industry sectors and the community (including productivity and safety reforms enabled through the use of telematics)

  together with

- Private interests of individuals and organisations (in pursuing business outcomes through the use of telematics).

EXECUTIVE SUMMARY

'Smart transport', including both automated vehicle (AV) systems, connected automated vehicle (CAV) systems, and cooperative intelligent transport systems (C-ITS), is rapidly evolving and deployments of both types of technology are occurring constantly.

TCA has had a long history of working in this field with regulatory telematics applications such as the Intelligent Access Program, and the National Telematics Framework, including legislative and policy provisions relating to privacy and security of data. TCA has also been central to the international development of telematics interoperability standards (such as ISO 15638) and has contributed to the international harmonisation of the Security Credential Management System (SCMS) architecture, which has been adopted by the United Stated and many parts of Europe.

TCA shares the learnings from these experiences, in the context of the questions and policy options considered in the NTC's discussion paper, *Regulating government access to C-ITS and automated vehicle data; September 2018*.

TCA supports the core recommendations of the NTC, with some caveats:

- Agreement that a legislative framework, based on outcome or principles-based legislative provisions, is needed to provide governance for the security and privacy of data from C-ITS and AV systems
- Agreement that government access to information (but not necessarily 'raw data') for the purposes of planning, system oversight and management, investment, research and other public good purposes is essential
- Agreement that most of the principles proposed in the discussion paper are appropriate – either as design principles for the new legislative framework or as principles to be incorporated as guidance for regulated parties.
- Agreement that the current privacy principles regime is inadequate to manage the complex and changing data environment into the future.

It is the considered option of TCA, however, that:

- The legislative framework needs to apply to all parties that generate, hold, collect, aggregate, transform/analyse and share data
- Traditional, prescriptive legislation will struggle to deal with rapidly evolving technology, systems and community expectations of information and privacy protection
- A privacy-by-design logic should underpin the entire framework wherever possible (with the internationally adopted SCMS approach being an example of privacy-by-design for key elements of the framework)
- Wherever possible, data should not simply be de-identified or pseudonymised, but also aggregated to a statistically valid degree
- Government access should not be the primary design feature for the data framework – but rather the integrity of the system to generate trust in consumers
- Clear access arrangements, with relevant 'tests' and thresholds for government access to 'raw' data should be incorporated into the legislation to provide assurance that data cannot be used for 'fishing' or compliance purposes without reasonable suspicion of unlawful behaviour
- The National Telematics Framework (NTF) is an example of a 'platform' approach to technology that is holistic, flexible, and includes privacy-by-design within its architecture – which extends beyond technology to include legislation, policy, operational and commercial dimensions.

The development of robust, interoperable and secure data management systems are essential for the rapid adoption of connected transport and automated vehicle systems. There are significant risks to safety, as well as economic, environmental and other outcomes from slower adoption of this technology.

It will be necessary to develop an end-to-end framework for the protection and governance of data from these systems, with robust legislation supported by principles, some prescription around specific elements, and supporting standards and guidance, the most effective way of achieving this, in light of a rapidly evolving technological and market environment.

TCA offers its support and expertise in developing and implementing operational policy in the future discussion and development of this legislative framework.

CONTENTS

1 INTRODUCTION AND CONTEXT

TCA is pleased to be given the opportunity to make a submission to the National Transport Commission's (NTC's) discussion paper *Regulating government access to C-ITS and automated vehicle data; September 2018*.

As the national government body responsible for administration of the government endorsed digital business platform for telematics and related technologies, and in time C-ITS applications, TCA is uniquely placed to provide input into the NTC's discussion paper.

The NTC's work in this space comes at a crucial time and could significantly influence the future data and privacy architecture for transport in Australia – as well as providing the opportunity to ensure that road managers have access to the analytics needed to effectively plan for and operate the transport system.

This submission will seek draw these two factors more closely together, as it is the view of TCA that it will not be possible to achieve both goals without a coherent, end-to-end privacy and data management regime that provides certainty to the market and consumers.

In this context, this submission first outlines the current data and privacy architecture that exists – TCA's current role and manager of heavy vehicle telematics and the National Telematics Framework. This submission then seeks to reframe the issue in broader terms than simply ensuring government access to data when necessary.

A proposed practical solution is outlined as a combination of the current NTC options, with additional detail on the potential strategic and operational benefits of such an approach.

1.1 ROLE AND FUNCTION OF TCA

TCA supports government agencies and regulators by providing outcome-focused, technology neutral, disruption-resilient programs that address security and privacy concerns, encourage innovation and facilitate an appropriate private sector contribution to the costs of regulation.

TCA exists because Australian Governments use and increasingly depend on telematics and related intelligent technologies – and its associated providers – to deliver public purpose outcomes across surface transport modes.

TCA was established with the purpose of managing a new set of stakeholders within the transport portfolio – technology providers – on behalf of Australia's road and transport agencies (and other portfolios).

TCA's role – like those of other, modern cross-cutting government organisations in other portfolios – involves the interaction of three distinct stakeholder groups to deliver improved public outcomes:

- Government agencies (which set policies and/or manage programs using telematics applications)
- Regulated stakeholders/end-users (which use telematics applications in response to government policies and/or programs)
- Private sector service providers (the technology and Intelligent Transport System sector, which deliver telematics products and services to regulated stakeholders/end-users).

TCA administers a contemporary, light-touch approach to manage transport technology applications, ensuring public outcomes are realised – and avoiding:

- Potential market failures, such as proprietary-based systems inhibiting inter-operability, or technology applications which impact the safety of road users and
- Potential regulatory failures, such as unintended technology prescription, or poorly constructed policy positions which could lead to duplication and inconsistencies.

TCA manages the intersection of policy, technical commercial and operational elements necessary to realise public outcomes – in partnership with government and technology providers.

Although TCA's origins were in heavy vehicle reforms which were dependent upon the use of telematics to advance productivity and safety outcomes for Australian Governments, TCA's Constitution and Memorandum of Understanding (MoU) anticipated – and was drafted from the outset of TCA's establishment to enable – the need for a broader role in providing services across numerous policy and program areas.

Established as a corporation, fully owned by Australia's road transport agencies, TCA is not a statutory body, however it has some functions and requirements that have been enacted in the Heavy Vehicle National Law. While these provisions relate primarily to the operation of Intelligent Access Program in a broad sense, they also outline a privacy framework that covers the end-to-end lifespan of the data collected, including all parties with access to or responsibility for data collection and management.

TCA's current functions and services (Advice, Accreditation and Administration services) apply across the following public policy domains:

- Management of an open technology market (through the National Telematics Framework)
- Heavy vehicles
- Public transport (buses)
- Taxis, hire cars and ride sharing
- Safety-based technologies for road safety (light vehicles)
- Connected and automated vehicles (light and heavy vehicles)
- Road transport network management.

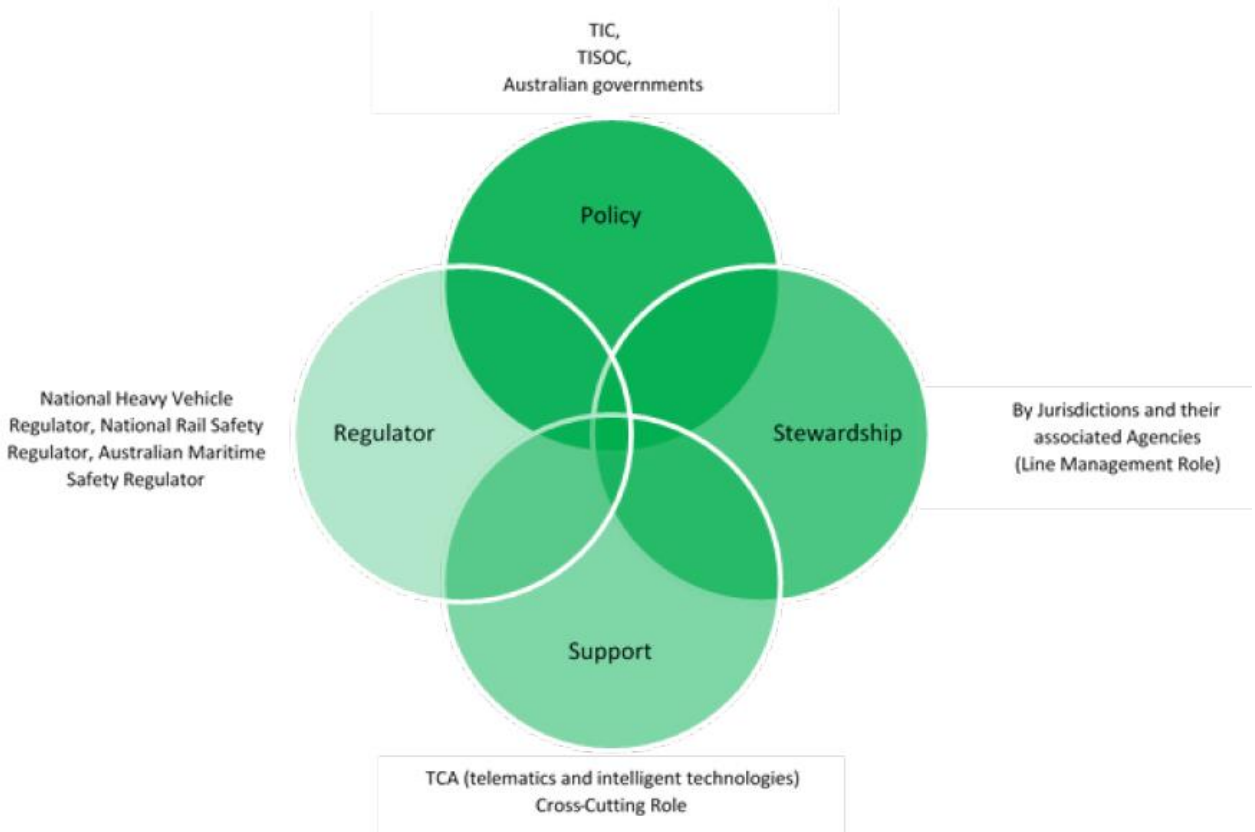
TCA derives its powers from different instruments linked to policy sectors, including:

- Ministerial policy decisions
- Legislation and regulations
- Guidelines
- Approval powers granted by TCA's Members and/or other organisations.

TCA adopts a whole-of-government approach – to ensure harmonisation, consistency, interoperability across government portfolio areas and industry sectors – in the use of intelligent technologies.

The operational environment which TCA administers transcends any specific policy area. TCA articulates its role as a cross-cutting organisation through the following diagram.

Figure 1 –TCA's role as a cross-cutting, supporting entity



TCA is cross-cutting by nature: activities interface, but do not overlap, with a wide range of government and private sector entities, as illustrated in Figure 1.

There is no other entity – government or private – which performs TCA's role and function.

As a result, and by necessity, TCA interfaces with a wide range of government agencies, regulators and private sector entities – as per its Constitution and MoU.

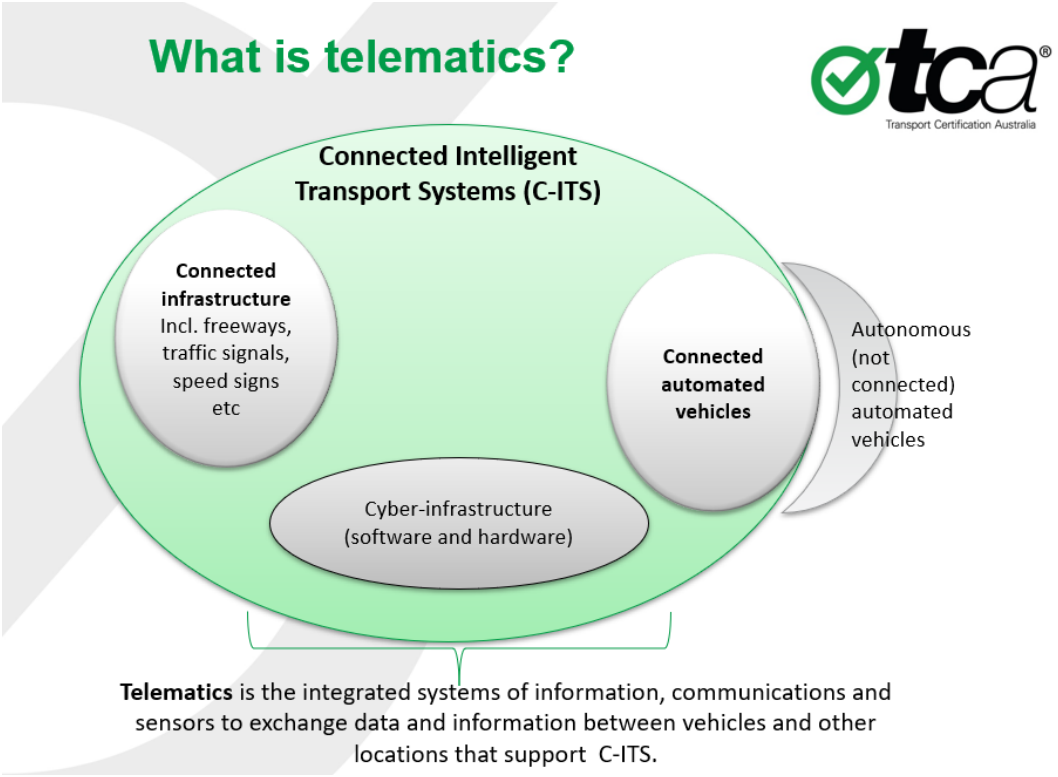
During 2016, TCA's Constitution and MoU was updated to:

- Reaffirm TCA's established role with respect to telematics and related intelligent technologies
- Expand TCA's role to support the emergence of connected and automated vehicles
- Recognise TCA's role in providing assurance through:
    - The type-approval of devices and systems
    - The certification and audit of technology providers.

1.2 AUSTRALIA'S NATIONAL TELEMATICS FRAMEWORK

The National Telematics Framework has been endorsed by Australia's transport Ministers, and provides a central point of reference for the deployment of telematics and related intelligent technologies in Australia across surface transport modes.

Figure 2 – What is telematics?



Telematics is often misunderstood as being only commercial business systems for tracking freight or logistics, but (as illustrated in Figure 2), the National Telematics framework takes a more holistic and modern approach, including all the integrated systems of information, communications and sensors (devices) to exchange data and information between vehicles and other locations.

The Framework provides a powerful and contemporary digital business platform and has been endorsed by both the Transport and Infrastructure Senior Officials Committee and Ministers. The Framework delivers:

- Public outcomes through an open technology market, which can sustainably deliver upon the needs of government, industry and end-users
- Consistency and certainty to technology providers, so that government positions can be relied upon to make investment decisions to support government through the National Telematics Framework

- Based on the certainty provided through the National Telematics Framework, technology providers are delivering competition and choice in the market, while delivering the latest technological developments at lower costs
- Stable, end-to-end privacy and data protection, based on a privacy-by-design model.

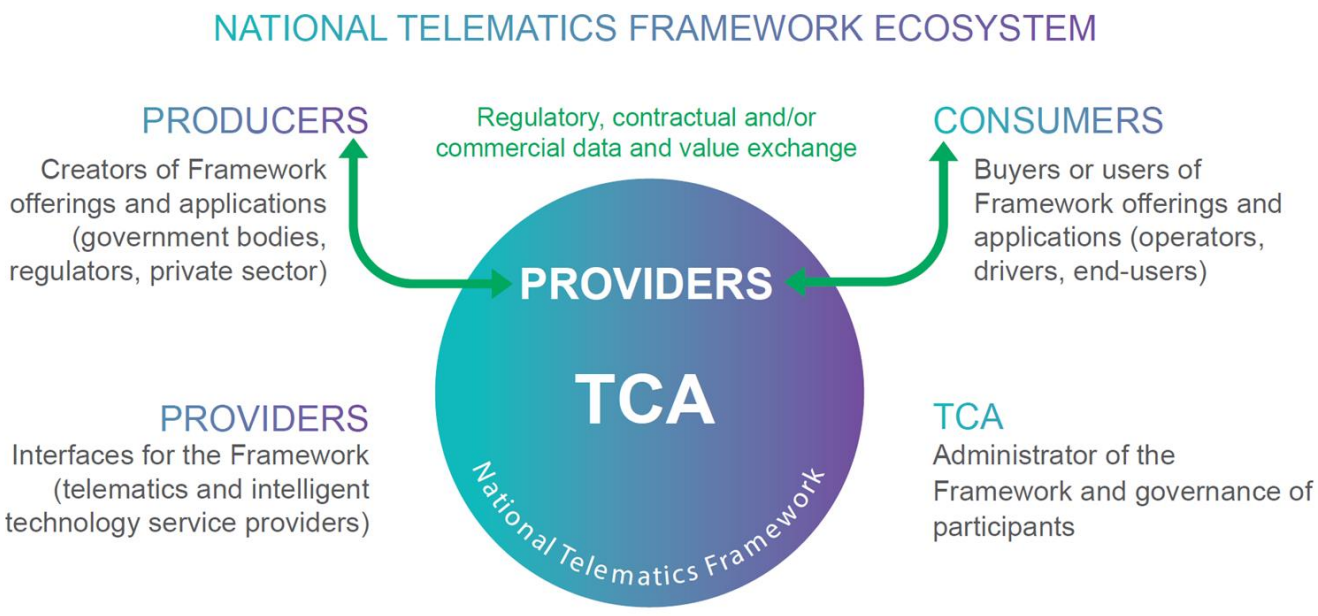
The National Telematics Framework provides a digital business platform with infrastructure and rules for an open marketplace that brings together 'producers' and 'consumers'. Understanding the relationships both within and outside the platform is central to the platform strategy.

Many platforms have an 'ecosystem' of similar structures. The owners of the platform control its intellectual property and governance. Providers serve as the platform's interface with users. Producers create their offerings, services or programs, and finally consumers purchase and/or use these offerings.

The figure below highlights the relationships, in simple terms the four entities are as follows (Figure 3):

- Producers – are the creators of the platform's offerings (including public policy owner or commercial entity)
- Consumers – the buyers or users of the offerings
- Providers – provide the interface for the platform that interfaces to deliver services (TCA Certified Service Providers)
- Owner – National Telematics Framework owner is the controller of the platform intellectual property and the governance of who may participate and in what ways within the platform (Transport Certification Australia).

Figure 3 – National Telematics Framework Ecosystem



In a platform environment, it is the network of producers and consumers that are the chief assets, as opposed to one organisation controlling resources and market structures to minimise movements consumers.

As the time of writing, nearly half of the articulated heavy vehicle fleet in Australia has a TCA type-approved Telematics In-Vehicle Unit (IVU) because of this platform approach, where end-users (i.e. consumers), have purchased the equipment for their own purposes, while government benefits by being able to easily implement new telematics applications and utilise analytics based on data from participating vehicles in this fleet.

The National Telematics Framework has also established a platform for future digital reform. The best evidence for this is the comparatively low marginal cost of 'turning on' new regulatory telematics applications.

In a world of traditional separate 'pipeline' models, individual businesses not only create barriers to competition, but also barriers to their customers leaving. With platforms, the focus shifts to the elimination of barriers to producers and consumers to maximise value creation (using rules and architecture).

This is the key outcome of TCA's administration of the National Telematics Framework – to ensure that at any one time, the rules and architecture are both contemporary and ensure competition, open markets and resilience through the provision of platform IP. This strategic business and economic thinking have been applied and endorsed by governments in the form of the National Telematics Framework.

The realisation of public outcomes through the National Telematics Framework is enabled through managed interactions – together with a separation of roles and responsibilities – in an operational environment.

In short, TCA's role is to 'regulate' providers of regulatory telematics applications, while the role of government agencies and regulators is to regulate end-users – by relying on the assurance provided by regulatory telematics applications.

This separation of roles and responsibilities is central to TCA's role and function, and the operation of the National Telematics Framework.

It is quite feasible that this model could be expanded or adapted to encompass and support the private and secure management of data from C-ITS and automated vehicle systems.

1.2.1 BENEFITS OF THE NATIONAL TELEMATICS FRAMEWORK

TCA's submission to the NTC Review of Regulatory Telematics in February 2018 contains a lengthy list of benefits of the NTF, but outlined below are a number which directly relate to the subject of this submission:

- Privacy framework protected by law (for heavy vehicle Intelligent Access data), and supported by standards/specifications, with both financial penalties, and the risk of commercial sanctions (such as having certification withdrawn)
- Delivers a robust cyber-infrastructure, with protections and safeguards for government and industry. This provides assurances to governments and industry that type-approved suppliers and certified service providers:
    - Have appropriate governance and management structures in place, including the necessary privacy and data protection capabilities
    - Have strategic business interests and plans which align with the interests and needs of government, industry sectors and end-users
    - Have the operational structures in place to manage the needs, and meet the expectations, of government and end-users
    - Understand the obligations of obtaining type-approval and certification.
- Individual government agencies/regulators retain autonomy over policy and program decisions to deliver public purpose outcomes, without needing a bespoke framework
- Transparent allocation of risks between the public and private sectors.

The Heavy Vehicle National Law (HVNL) already provides a best practice approach to managing privacy and data management. The NTF, which derives its powers from the HVNL, is based on this operating model and broader principles for telematics. This could be an example of a legislative framework if extended to other types of data and other entities, as outlined in 2.2.1 below).

1.3 WHY ACTION IS NEEDED

The importance of having a secure, private data architecture, with appropriate access arrangements and controls cannot be overstated.

The discussion paper released by the NTC frames the problem in terms of the potential for consumers not to uptake the new technologies of connected and automated vehicles (and other forms of C-ITS). While this is true from a certain perspective, the true risks are more complex, and exist whether users opt-in or out of more connected travel.

A more detailed exploration of risks might include the following:

- Reduced trust in the privacy and data protection of the emerging ecosystem could lead to
    - Slow or reduced adoption by segments of society, resulting in reduced (or more slowly realised) safety benefits than would otherwise be the. In a tangible form, connected and automated technologies could have a paradigm-shifting impact on road crashes – with the potential to save hundreds of lives per year in Australia alone
    - Slow adoption of connected or automated vehicles (particularly amongst the freight sector) could slow both safety and productivity benefits. As an example, currently available vehicle platooning technology retrofitted to existing trucks, has been estimated to have potential fuel savings of between 5 and 15% - a significant improvement for an industry with narrow margins
    - Deliberate opting-out of connectivity has the potential to undermine the effectiveness of the tools and applications that build upon technology as a platform – for example collection of non-personal data to assist in managing the transport system. It is likely that some benefits from connectivity (such as pedestrian warnings of approaching vehicles at street crossings) would only be of significant value when most vehicles and most pedestrians are part of the connected transport ecosystem.
- Lack of an end-to-end secure data ecosystem could lead to increased risks of interoperability failures between devices, malicious hacking, deliberate tampering to disguise illegal behaviours, or other behaviours.
- The emerging 'smart' transport system will need to somehow be linked with financial remunerations to be effective and efficient. Ensuring that the system can accurately, verifiably identify that someone is who they say they are, and that they have appropriate authorisation to pay for a journey from a linked account is essential. It does not necessarily follow, however, that the data the system generates must allow the actual identity of that person to be ascertained. A secure, private and trustworthy architecture that protects their data from end-to-end will be essential for the travelling public to opt into using connected transport that is in any way linked to financial systems.
- Australia's international reputation is also at risk, if a lesser standard for data protection is accepted domestically than that required internationally. TCA can attest to the importance of not 're-inventing the wheel' with new technologies. This requires global and national harmonisation of standards, approaches and technical standards (though as outlined later in this submission – not to the degree of overly prescribing technical approaches and requirements)
- Connected and automated vehicles offer significant research, manufacturing and other economic opportunities for Australia. Many commentators have advised of the value of being 'on the leading edge, but not the bleeding edge' of technological development, there can be no doubting that there is a massive benefit in taking advantage of changing markets, in having a highly skilled local workforce focused in the knowledge-economy as well as the traditional manufacturing sectors. Early adoption of connected and automated technology has the potential to offer Australia significant economic opportunities, but this relies upon strong consumer acceptance of the technology for local testing and market development

It is the view of TCA that it is therefore essential to adopt as closely as possible the international standards for the protection of data through a secure architecture, rather than focusing only on government access to and protection of data.

As a nation, we cannot afford to develop legislative provisions and policy responses in isolation, but instead need a single, harmonized response that takes the focus on the technology user and provider, rather than a fragmented regulator perspective. A 'joined up' approach to data security, sharing, privacy, use/access and regulation is essential.

1.3.1 THE EVOLUTION OF INFORMATION AND PRIVACY

A compounding problem is the somewhat outdated concepts, governance arrangements and definitions of 'private information'.

The current approach to managing privacy through a principles-based legislative approach has worked well, generally, in the past because it has provided guidance and flexibility in managing data privacy, combined with clear avenues for regulatory access to data for specific (primarily enforcement) purposes.

This framework, however, was premised on the concept of 'private data' that was singular, point in time, and generally separate from other indicators, meta-data, or content. Contact lists, medical records, transaction histories and other examples abound.

Connected transport data – whether generated and 'owned' by governments or private bodies, or citizens themselves, is of both a different nature and scale. The sheer amount of transport data will be both daunting, and invaluable. The volume of data will pose a challenge to effectively applying the privacy principles as they stand. More importantly, though, this emerging form of data is different in nature, not simply in quantity – often being continuous streams of data and meta-data where every single element of the data may be able to be turned into private data through transforming or adding other data sets, should it not be adequately protected from source to destruction.

This data is also entirely fluid – flowing from device to device, system to system as needed to ensure the safe and efficient management of the network. Cars will need to be able to transmit to trucks, roadside devices, smartphones used by pedestrians, drones and enforcement vehicles/devices, and unless the architecture requires it, each application or device could develop their own privacy and security system under the existing principles.

This cannot be managed through the simple application of the existing privacy principles. While current principle-based privacy arrangements have served well in the past, and for certain types of data, the existing privacy regime is not fit-for-purpose and not sufficient to protect data security in a connected transport system ecosystem. The meaning of private information has changed with the advent of connected 'big data' and is fundamentally different in an automated transport future – especially one where biometrics are commonly used.

Fortunately, there are solutions which have been and are currently still being developed.

2 FEEDBACK ON THE NTC'S DISCUSSION PAPER

2.1 FOCUS AND SCOPE OF THE REVIEW

TCA encourages this review to take an expanded perspective beyond simply government 'owned' data. Data from C-ITS and automated vehicle systems will often exist as 'information streams' that will interact with numerous devices, information systems and other data-streams and sources. The privacy and security framework for data needs to support a holistic data architecture – from data generation though use, transfer and sharing, to final storage and potentially destruction.

A robust end-to-end secure data architecture for automated vehicles, connected automated vehicles, and other C-ITS systems is essential in the expectation of the use of these systems for charging and economic regulation (including access concessions) which necessitates a single coherent policy and legislative approach.

TCA supports the NTC taking a broader approach and joining up with other bodies working in this and related policy areas to develop a workable legislative and policy framework. The National Measurement Institute, for example, are currently reviewing the existing legislation for devices that are used for trade or charging. This is an ideal opportunity to integrate a transport system data legislative framework that would support charging in the future.

The Australian government is also reviewing data access for private information through the National Data Commissioner. This review should liaise with and integrate with this approach, to the degree it is appropriate.

The discussion paper currently divides consideration of AV from C-ITS data, but combines data protection issues and government access to data together according to the source of the data (AV or C-ITS). If the more holistic view of data protection and access TCA proposes is adopted, it is potentially more appropriate to shape the questions of the discussion paper around the data protection architecture for all relevant transport data (regardless of whether from C-ITS or AV sources), and separately consider the question of government access and use of data regardless of source.

2.2 EXAMPLES OF END-TO-END DATA PROTECTION FRAMEWORKS

2.2.1 HEAVY VEHICLE NATIONAL LAW - INTELLIGENT ACCESS PROGRAM

The HVNL currently contains an end-to-end data protection framework, with explicit obligations, requirements and penalties for breaching these obligations on all parties in the data 'chain'. In addition to clear allocation of responsibilities between parties and substantial penalties for releasing information contrary to the legislative requirements, the legislation outlines the circumstances in which data may be used for research and public good purposes.

Similar to what we envisage for AV's and some C-ITS systems, Chapter 7 of the Heavy Vehicle National Law (HVNL) – Intelligent Access Program – already provides a framework for privacy and data protection.

(It is important to note that Chapter 7 of the HVNL contains provisions which relate to both the 'IAP application', and the 'IAP operating model' – which was subsequently renamed the National Telematics Framework, which houses multiple telematics applications. The change of naming convention was essential to avoid confusion between the 'IAP application' and the 'IAP operating model'. However, that this was only a half-way house until such time as further structural changes to the HVNL could be implemented to distinguish this separation, and to de-couple the provisions which relate to the IAP application from the National Telematics Framework (IAP operating model), so that the common privacy and data management provisions which apply to all telematics applications, could be progressed by the NTC).

Chapter 7 provides the highest level of privacy protections, in recognition that telematics applications have – by their very nature –the ability to compromise privacy principles without appropriate regulatory, technical, intuitional and operational safeguards.

The concept behind Chapter 7 by the NTC, in the original form of the (Model Legislation — Intelligent Access Program) Regulations 2006, was based on the same principles that also apply to the transport marketplace in which AV's and C-ITS systems will operate.

For instance, Chapter 7 includes specific provisions which relate to privacy protection and data management, including the role and function of TCA as the national administrator of the National Telematics Framework (IAP Operating Model). In this context, the role of TCA is a critical privacy protection safeguard for telematics applications administered through the National Telematics Framework.

This framework protects the privacy of individuals and operators by collecting data for individual telematics applications in accordance with disclosed intended purposes.

There are penalties in Chapter 7 which apply to TCA, service providers and governments for the mis-use of data collected through telematics application.

These provisions provide the trust framework that gives assurance to program entrants that their privacy rights are be protected, despite the increased sharing of their data necessary for program operation. Over time, demonstration of this has resulted in heightened trust and higher uptake.

This legislation therefore goes far further than the privacy principles, and enshrines specific legislative obligations (and penalties) on those who participate in the framework – primarily in relation to protection of data privacy, but also in reporting of tampering and other acts or omissions.

TCA regards Chapter 7 of the HVNL as a starting point for a legislative framework for protection of transmissible data, and the basis for the NTF.

This type of approach, supported by the principles and guidance material suggested in 2.4.3 below could form a core element of the new C-ITS and AV data privacy framework to provide the regulatory certainty needed by the market to encourage voluntary uptake of AVs and connected vehicle technologies.

2.2.2 GLOBAL C-ITS SECURITY DATA FRAMEWORK

The operation of connected vehicles requires a secure operational environment for transferring information. The Security Credential Management System (SCMS) approach has been adopted by the European Union and United States of American transport agencies, amongst other global decision-makers, as the basis for secure, private data exchange.

While the discussion paper touched on the Section on an SCMS, the system and its potential impacts were not explored.

TCA has provided additional information on SCMS for information, but the key point that this forms the central plank of a vehicle/device/infrastructure data exchange system is not explicit.

SCMS ensures that vehicles, infrastructure, pedestrians and other actors within the C-ITS ecosystem can trust information received from vehicles, infrastructure, pedestrians and other actors. This is an important cornerstone (that information received is secure, trustworthy and unaltered) but doesn't control beyond that initial exchange how that information may be stored, joined with other data, or used for other purposes downstream.

A SCMS provides security for the 'internet of cars' and is being deployed in the United States and across Europe. Australia has worked in close collaboration with international policy and technical experts to define an internationally-harmonised architecture for the SCMS, and an interrelated, harmonised security policy framework (and other key resources) that stands to benefit all regions.

Australia is undertaking discussions relating to the implementation of its own SCMS, with TCA liaising with the United States and European agencies to achieve international harmonisation of key standards for connected vehicles and C-ITS.

An SCMS operates on a privacy-by-design model, with vehicles (and the privacy of users) protected through rotating identifiers (referred to as pseudonym certificates) that still allow the vehicle to exchange trusted information securely through the certificate validation system.

Within an SCMS ecosystem, various components (policy, governance, infrastructure, policies and clear accountabilities for all actors) must be in place, supported by one or more organisational structures responsible for the effective management of such a system.

If implemented in Australia, the security domain created by an SCMS could form a key component of a more secure privacy and data regime, supporting legislative, policy and other elements.

2.3 BEYOND SCMS AND 'VEHICLE DATA'

Without pre-empting the need for detailed development of options, and discussion of details at this stage, it is possible to provide comment on the options proposed by the NTC, within a broader data management and privacy-by-design framework.

The next section summarises TCA's comments on key areas of the NTC's questions, and proposed options.

These proposals focus on a legislative and supporting framework needed to create an end-to-end data protection and access framework. An SCMS data exchange and security standard is the core of this privacy-by-design model, but needs to be supported by:

- Legislation establishing the requirements and obligations (both at an outcome level, and as appropriate, more prescriptive provisions) on parties in relation to data management, including:
    - Enshrining the data standard in legislation and/or the safety management system approach used for AV's
    - Providing requirements for data protection and access and penalties for breaches of the requirements (including potentially creating categories of sensitivity of data)
    - Providing principles for the management of data (within organisational data management policies and practices), including ensuring that data is of a sufficient quality for its intended purpose (i.e. non-evidentiary data sets should not be used as the basis of prosecutions, and evidentiary data should be required for purposes intended to lead to enforcement
    - Establishing or providing regulatory standing for operational guidance (such as minimum requirements for the de-identification or aggregation of data prior to use and release, preventing the use of private data for compliance 'fishing', enshrining access to private data for the purposes of prosecuting breaches of transport legislation, and requiring the use of warrants or other mechanisms to access data).
- Appropriate standards, either set as mandatory within the legislation, or guidance information to assist organisations to meet the performance outcomes set in the legislation
- Operational systems developed by organisations or groups of organisations, to meet the requirements of the legislation, mandatory standards and commercial requirements.

The importance of having a coherent approach that sets industry and community expectations, while also harmonising with common international and industry practice cannot be overstated. The risks outlined in the discussion paper, and section 1.3 above highlight the need for consumer trust in data systems.

Evidence and past experience have shown that this trust will need to be built on system integrity, interoperability and data privacy-by-design, rather than fragmented approach (one rule for government with other rules for industry or citizens) for access and privacy protection.

2.4 COMMENT ON THE RECOMMENDED OPTION AND QUESTIONS

2.4.1 TCA RESPONSE TO THE DISCUSSION PAPER OPTIONS

As outlined above, TCA supports a blended approach, with a mix of legislation, with principles to guide the development of commercial data management systems, operational standards:

- legislation focusing on outcomes
- more prescriptive legislated protections (e.g. mandating SCMS or equivalency)
- legislative principles for organisations to use when designing data protections and access policies (see section 2.4.3 below for further comment on the proposed principles)
- a mix of mandatory standards, and guidance information
- operational requirements (such as data aggregation standards for release of information)
- differing levels of privacy/security required for more highly sensitive information (such as biometric data or personal opinions).

One of the reasons why legislation should be largely outcome-based and principle-based in nature is to respond to the rapidly evolving, and highly variable nature of the data environment. For example, the legislation should support a framework distinguishing between data that could reasonably be found from

other sources, versus biometric data, opinions captured in recordings etc). A risk-based approach should be built into the framework (potentially though guidance material, coupled with examples of appropriate privacy protection 'levels' for different levels of data risk).

This approach also allows for the rapid evolution of data and avoids the problem of 'hard coding' types of data and specific protection requirements into the legislation. Conversely, some prescriptive arrangements will likely be required to ensure that offences can be reasonably linked to breaches of the legislation (which is often difficult with principles-based legislation).

2.4.2 TCA RESPONSE TO KEY NTC CONSULTATION QUESTIONS

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

1. The first assumption relating to the difficulty of irreversibly de-identifying personal data is strongly supported. TCA experience in managing transport telematics data confirms that transport data of this nature is inherently difficult (if not impossible) to permanently and irreversibly de-identify.

   Aggregation, combined with privacy-by-design features to ensure that data is (as far as possible) not initially associated with private information such as personal identifiers, as well as ensuring that data is aggregated to a statistically appropriate level to prevent reidentification of personal information is essential. Even so, without legislative obligations on data holders to ensure that information is appropriately protected, this is still insufficient.

2. The second assumption that data access and protection frameworks will remain inconsistent is potentially not valid. As outlined above, the SCMS approach is an internationally agreed approach to managing the secure, interoperable and trusted exchange of C-ITS data. While there remains much discussion about the nature of the security framework, the NTC should proceed on the basis that Australia will indeed need to comply with one of the emerging international standards for data management, security and access. To do otherwise, is to effectively plan to have a unique approach that differs from global practice, with all the many risks that entails. Complementary elements are needed, however, to manage storage, linking and use of that data following that initial data exchange, as this occurs outside the SCMS system.

6: Is the current information access framework for government collection sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology? and

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?

The response to both questions 6 and 7, taken collectively, is no, with caveats. The current legislative framework governing the IAP is robust, and was appropriate when drafted, though potentially overly restrictive considering the evolution of regulatory telematics (as one field of C-ITS). Allowing all other C-ITS data to be governed by generic privacy principles and standards (and where they exist, legislation) is insufficient for the future, where governments seek to incentivise and encourage uptake of C-ITS and automated vehicle systems.

8: Are separate options for addressing the privacy challenges of C-ITS technology and automated vehicle technology reasonable for achieving any future reform?

As outlined previously, a single legislative framework for the protection and security of connected vehicle data and intelligent transport systems needs to be establishing that governs all relevant parties (not just government). While there may be provisions that apply separately to C-ITS data and system managers, as against automated vehicle system providers and data, the same legislative framework, principles, security systems and other elements should generally apply.

This privacy and security legislative framework should be designed around outcomes such as robustness, interoperability, efficiency and effectiveness in protection and securing data. Government access to data

should not be a design consideration, but rather should be achieve separately through legislative provisions, with appropriate 'tests' for different levels and types of data access.

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

By themselves, it is it TCA's opinion that these principles (or a subset of them) would not address the privacy challenges. Legislation providing both outcomes for certain objectives, and prescriptive requirements and penalties where appropriate, combined with a data-management framework such as the SCMS and other management standards will be essential to manage the privacy challenges of the future.

While guidelines offer weaker protection, they are more flexible, and may be more appropriate for certain issues. For example, data aggregation techniques to achieve statistically valid anonymity would probably not be appropriate or needed in law, but would be valuable guidance as a standard or guidance document.

2.4.3 TCA RESPONSE TO THE PROPOSED DRAFT PRINCIPLES FOR PRIVACY MANAGEMENT

The NTC discussion paper sets out eight draft principles which could be used to govern a future AV and C-ITS data environment. It is noted in discussion with the NTC, that some of these are 'design principles' that would govern the development of the legislative framework, while others are 'legislative principles' that would be enshrined in law as written, and would apply to regulated parties.

The following table seeks to distinguish between these two categories and provides comments on the principles themselves.

Table 1: TCA categorisation of and comments on the draft principles for managing privacy challenges

Draft principles	TCA categorisation and comment
Principle 1: C-ITS information and automated vehicle information must be clearly defined to ensure any additional privacy protections only capture relevant information.	Agree in principle. All potentially private data collected by connected transport should be protected through a privacy-by-design architecture and have appropriate privacy protections according to the potential risk resulting from release of the data. Rigid or prescriptive definitions will not be able to rapidly adapt, however. Outcome or principles-based law, with inclusive definitions are needed to avoid hard-coding exclusive definitions into law. This is a design principle to guide drafters and would not add any value as a principle for regulated parties.
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).	Agree, however, this should be broadened to all regulated parties. This is an appropriate legislative principle to guide regulated parties.
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	Agree. This is critical and should distinguish and support flexible responses to different types of 'personal data' as outlined above. This legislative framework should apply to all entities generating, collecting, sharing, holding, aggregating or otherwise involved in the data 'chain' – not just governments.

Draft principles	TCA categorisation and comment
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.	This is a design principle to guide drafters and would not add any value as a principle for regulated parties.
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.	Agree. Privacy protections (obligations and penalties for breaches) should be set in legislation and supported with mandatory guidelines for outcome areas needing higher levels of guidance, and guidance material for areas needing less rigorous support. While guidelines offer weaker protection, they are more flexible, and may be more appropriate for certain issues. For example, data aggregation techniques to achieve statistically valid anonymity would probably not be appropriate or needed in law, but would be valuable guidance as a standard or guidance document. This is a design principle to guide drafters and would not add any value as a principle for regulated parties.
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.	Agree. This principle should underpin and inform the design of the legislation, to have categories of 'personal information', which organisations should match to appropriate levels of protection. This is a design principle to guide drafters and would not add any value as a principle for regulated parties.
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	Agree, but noting earlier comments relating to the new 'types' of data generated by C-ITS and automated vehicle systems. Some of this data will effectively render 'permission' and other concepts such as 'right to be forgotten' near impossible to achieve in practice. This will be particularly true of data sets blended from different sources and aggregated and de-identified information extracted for higher-order purposes. It would be unworkable to require permission to be given for use of derivative data sets, for example, but altering collected

Draft principles	TCA categorisation and comment
no longer necessary for the purpose it was collected for.	data in some manner, should not be an easy 'out' from privacy requirements. This is an appropriate legislative principle to guide regulated parties.
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.	Agree, but noting earlier comments relating to the new 'types' of data generated by C-ITS and automated vehicle systems and caveat below. Some of this data will effectively render 'permission' and other concepts such as 'right to be forgotten' near impossible to achieve in practice. The design of the SCMS fundamentally separates identity from trust. When an entity receives information from another C-ITS participant, received information can be validated as secure, trustworthy and unaltered without having to know the identity of the sender. A government C-ITS participant (through smart infrastructure instrumented with roadside C-ITS stations) it is therefore incapable (by design) to determine whether the sender has opted in or out. This should apply to all regulated parties, but only to data that is actually private (i.e., not necessary data which is not identifiable, as suggested above). This is therefore both an appropriate legislative principle to guide regulated parties, and also a design principle. In terms of design for the new legislative framework, private information should only be access by Government where a truly 'opting-in' to voluntary access is viable, or where there is a valid enforcement process (for example, a warrant, reasonable suspicion, etc).
Principle 8: Privacy protections for C-ITS and automated vehicle data should be regularly reviewed to ensure privacy is adequately protected.	Agree, however, this should be broadened to all regulated parties. This is an appropriate legislative principle to guide regulated parties.
Other potential principles for consideration: • **Minimise harm principle** (a principle related to principle 2, but relating to the prevention of harm to the individual or company affected) • **Proportionality of protection** (relating to principle 5, and establishing that different types of data are likely to be regarded by consumers as having	These legislative principles would better guide regulated parties in the designing of data collection, protection, aggregation, management, and sharing. TCA is of the view that a low bar for government access to 'raw' data would compromise the integrity of C-ITS and automated vehicle data systems and slow adoption (see the risks identified earlier).

Draft principles	TCA categorisation and comment
more potential for harm if revealed / used inappropriately. Higher levels of protection should be inbuilt where possible) • **Proportionality of responsibility** (trusted entities that have access to raw data – such as the ABS or TCA currently, should have additional obligations to protect from misuse or reidentification of data) • **Aggregation and de-identification where possible** (de-identification is insufficient to protect privacy, and must be combined, wherever possible, with an appropriate level of data aggregation) • **Clarity of purpose in use and design of data management** (in many cases governments will need access to aggregated information about infrastructure and service usage, rather than tracking specific people and individuals. Law enforcement should not be used as the default for access arrangements to all data – as this can be achieved through routine court and enforcement processes)	In the current environment, 'trusted entities' like TCA and the ABS have access to personal, private data that is either mandatorily required, or voluntarily supplied, on the basis that it provides a public good after being aggregated for the use of public policy and other purposes. Like TCA and ABS, entities with access to this kind of data (especially government agencies with enforcement roles) should have a higher 'tier' of responsibility to protect data privacy – without hampering access to aggregated and de-identified data for public policy purposes. In addition to clear legislative responsibilities, trusted entities also have a clear purpose based on a structural separation between 'enforcement' and other similar uses of data, from the holder and aggregator of data which may be identified. Traditional expectations of 'reasonable suspicion' should be the basis of access to 'raw' personal data, however, it will be important that the legislation provide for 'system monitoring' to identify faults, and potential illegal behaviour. Clear clauses enabling research and use of aggregated and de-identified data is also critical. The current IAP legislative provisions could provide guidance, though without additional guidance and supporting information, this clause could be restrictive.

3 CONCLUSIONS

The development of robust, interoperable, secure data management systems are essential for the rapid adoption of connected transport and automated vehicle systems. There are significant risks to safety, as well as economic, environmental and other outcomes from slower adoption of this technology.

It will be necessary to develop an end-to-end framework for the protection and governance of data generated by these systems. Traditional prescriptive legislation will struggle to respond and adapt to the rapidly changing nature of technological systems, data utilisation, and community expectations of data and privacy protection. Robust legislation based on a blend of prescription for key elements, and utilising outcomes or principles-based provisions for more fluid requirements is strongly recommended. As with other legislative frameworks, this legislation should be supported by principles (either embedded in the law or in subordinate legislation), some prescription around specific elements, and supporting standards and guidance.

All parties with relevant roles in this emerging data infrastructure should be regulated appropriately, rather than only focusing on government. Existing and new systems such as the SCMS and related data management and exchange systems are an excellent basis to establish this new legislative regime upon.

TCA looks forward to working closely with the NTC and supporting further discussion about the approach and details of this new governance framework for AV and C-ITS data.