Austroads Ltd
Level 9, 287 Elizabeth Street
Sydney NSW 2000 Australia
Tel: +61 2 8265 3300
Fax: +61 2 8265 3399
austroads@austroads.com.au
www.austroads.com.au
ACN: 136 812 390
ABN: 16 245 787 323

Our reference:
Our contact: Nick Koukoulas

29 November 2018

Ms Helen Tsirlina
National Transport Commission
Level 3, 600 Bourke Street
Melbourne, 3000 Victoria

Dear Ms Tsirlina,

REGULATING GOVERNMENT ACCESS TO C-ITS AND AUTOMATED VEHICLE DATA

Austroads commends the National Transport Commission on its discussion paper titled *Regulating Government Access to C-ITS and Automated Vehicle Data.*

While much work is being progressed on identifying the potential safety and mobility benefits of emerging vehicle technologies, and on establishing the regulatory and operational arrangements required to support their introduction and use, it is well recognised that further work will be necessary to identify and address the wide range of issues that these vehicles could potentially have on our communities.

Austroads, as the association of road transport agencies across Australia and New Zealand, has a critical role to play in planning for and supporting the introduction and use of future vehicle technologies on our road networks. Austroads and its member agencies have a lead role in the design, maintenance and operational practices for approximately 900,000 kilometres of roads, and also with the vehicle registration, driver training and driver licencing practices that are necessary to manage access to and use of our road networks. Austroads' manages a number of research programs, including a Connected and Automated Vehicles (CAVs) program that has produced multiple research reports of relevance to and cited in your report.

Our response does not propose to address the specific questions raised in the discussion paper, but rather asks that the following points be considered in ongoing discussion and evaluation of this policy development.

(a) The strong focus of the discussion paper on the privacy risk addresses only a part of this reports' mandate as described in recommendation 8 of *Regulatory reforms for automated road vehicles* as:

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

Austroads requests that NTC extend the focus of the discussion paper to *realisation of benefits with privacy safeguarded.* As part of this, Austroads recommends updating the test used in recommending policy options to *encourage and assist the realisation of beneficial future uses of [CAV] information to achieve road safety and network efficiency outcomes* from the current "ensures that beneficial future uses of [CAV] information are not restricted".

(b) To assist this broader focus on *realisation of benefits with privacy safeguarded*, Austroads requests the NTC consider a categorisation of CAV data that more closely aligns with how access to data would occur and what controls can be applied to safeguard privacy:

i. Data broadcast from a vehicle over open one-to-any channels

The nature of this method makes this data accessible to any party with the necessary tools to receive and interpret the data. Due to this characteristic, there are fewer options available to restrict how this type of data is used once it is transmitted. For example, security measures for C-ITS have the primary aim of providing confidence in the validity of the source, not to limit use of received data. This type of data transmission includes the standards-based C-ITS methods that occur over 802.11p or Cellular-V2X. For completeness, this method should include any wireless transmission that does require an establishment of trust or authentication between the sending vehicle and all recipients.

ii. **Data provided by a vehicle over private wireless methods**
In this category, the transmission of the data can be limited to trusted or authorised parties. Transmission of this data may occur either proactively (vehicle initiates transfer) or by request to the vehicle. Given the involvement of only trusted parties, there is some potential for the use of data to be limited by licencing or other agreements between parties. This type of data transmission includes cellular data (via base stations) and Wifi methods in cases where establishment of trust/authorisation is a part of the communication. Trusted parties for the receipt of data may include both private and government parties.

iii. **Data that can be accessed only by physical connection into the vehicle**
This type of data transmission requires physical access to the vehicle. This may include data stored on vehicles as part of Event Data Recorders or the Data Storage System for Automated Driving (DSSAD) contemplated by UNECE Working Party 29.

As regulatory approaches are only one part of the toolkit available to mitigate risks to privacy, this categorisation approach is based on differences in what controls may be available at the point of CAV-originated data leaving the source vehicle.

(c) Austroads agrees that much CAV-originated data may be 'personal information', at least at the point of transmission from the vehicle. Austroads' 2017 *Privacy Impact Assessment (PIA) for C-ITS data messages* (report AP-C100-17) "concluded data that is collected, used and disclosed in the standard messages in C-ITS is personal information". Austroads does not however agree that 'sensitive data' will be as prevalent. The same 2017 PIA (Austroads report AP-C100-17) found that "no sensitive data (using the definition in the Act) has been included in any of the potential C-ITS scenarios considered to date."

As C-ITS is based around a standards-based interoperable environment, any changes that introduced 'sensitive information' such as data from biometric functions would need to progress through a publicly visible multi-stage standards development process. It may therefore be appropriate to not treat standards-based C-ITS as including 'sensitive information' particularly if some protections were adopted to preclude or restrict future inclusion of 'sensitive information'.

(d) Some intended beneficial uses by government of CAV-originated data have a requirement for data that may be 'personal information' or which may be reconstructed to infer 'personal information'. A small number of intended beneficial uses by government of CAV-originated data make use of data that is or could be reconstructed to be 'sensitive information'. In many of these cases, the benefits to the affected individual and the broader community can be substantial. It is therefore in the community interest that this NTC work include explicit examples of how the *realisation of benefits with privacy safeguarded* can be achieved. Case examples could include both cases where 'personal information' and 'sensitive information' are involved and not involved. To have relevance to the future use of CAV-originated data, these case examples will need to be forward looking and extend beyond discussion of existing trials and pilots.

i. Alerts provided to a road authority about a sensed speed limit differing from the expected (map-based) speed limit, about a pothole or some other road attributes. Data of this nature was identified by road authorities as being of strong interest in Austroads' 2018 *CAV Open Data Recommendations* (report AP-R581-18). For this data to be actionable by road authorities, there needs to be some confidence in the sources of the alerts, but no dependence on either 'personal information' or 'sensitive information'.Beneficial data categories could include:

    i. Asset data from machine vision systems, or vehicle based such as exception reports on condition of key assets (missing traffic signs and potholes are examples here)

    ii. Data which may provide enhanced network operations such as travel speeds, incidents, road closures, or road works

iii. Data which may validate data sets that road authorities generate, and supply to CAVs (such as speed zone changes, or road incidents)

iv. Data which may be used to enhance crash reporting and research uses, such as incidents of emergency braking events

v. Data which could be used to enhance registration and licensing operation such as vehicle defects that have not been rectified.

ii. Crash avoidance through messages exchanged between vehicles (V2V) and with infrastructure (V2I) about vehicle position and trajectory. Austroads' 2017 PIA (report AP-C100-17) identified the standards-based Cooperative Awareness Message (CAM) used for this beneficial activity to include 'personal information' or data that could be reconstructed to become 'personal information'.

iii. Post-crash investigation by police and other road safety groups is important to assist the avoidance of future crashes. This activity would benefit from access to both 'personal information' and 'sensitive information'.

(e) The examples in (d) above highlight a misalignment between:

i. Only some beneficial uses by government of CAV-originated data have any requirement for 'personal information' and even fewer have a requirement for 'sensitive information'; and

ii. The NTC considering that CAV-generated data will "most likely be personal information and sensitive information, especially when held by road agencies and law enforcement agencies".

Achieving the intended road safety and network efficiency outcomes and efficient enforcement of traffic laws requires the practical resolution of this misalignment. The case examples suggested in (d) should therefore focus on how *realisation of benefits with privacy safeguarded* can be achieved. Failing to demonstrate this may lead international stakeholders to conclude that Australia has an unfavourable environment to realise the benefits from CAVs and encourage them to direct investment elsewhere.

(f) In working through case examples such as in (d), consideration should be included on the practicality of the approach and its impact on the potential for benefit realisation. Consideration of requirements for managing the provision of consent may be of particular relevance in this regard.

(g) Similarly, working through case examples such as in (d) may prove useful in demonstrating and working through any opportunities and risks associated with the interactions between government use of CAV-originated data and access and modification by the private-sector of CAV-originated data. As an extension of this, Austroads would support a broadening of privacy considerations

(h) The discussion paper includes some consideration of international approaches, however Austroads' view is that these need to be more directly factored into the recommendation of policy options. Australia is a small market in the automotive world and is committed to following international standards. Accordingly, a test around alignment to international approaches should be considered as part of recommending policy options and the principles should likewise address this need for international alignment.

(i) The draft principles currently focus on "addressing the privacy challenges". Although some mention is made of benefit realisation, Austroads' view is that this needs to be elevated so that the realisation of benefits sits alongside the safeguarding of privacy as the focus for the principles.

(j) Some of the principles outlined in *table 1* (page 5) may be problematic for the practical operation of some connected vehicle systems. For example, obtaining consent (principle 7b) from individual road users, by multiple road authorities (including, private, state and territory, and local) would be challenging and may prevent effective deployment of C-ITS systems. While Austroads understands that these may be guiding principles for further regulatory framework development, we would welcome opportunities to work with the NTC on these principles on a case-by-case basis before they are endorsed.

Further details about the Austroads CAV program, including CAV research reports and CAV trial projects that are being undertaken and/or supported by the individual road agency members, may be accessed via the following webpage:
http://www.austroads.com.au/drivers-vehicles/connected-and-automated-vehicles

The list above is not an exhaustive list of potential CAV data privacy issues that have been highlighted during our CAV work program, but hopefully it does provide some value to the NTC's review. Austroads would be happy to discuss these issues and others in further detail if requested. Austroads offers assistance to develop the case examples as per (d) and updating the principles as per (i) in the context of a collaborative approach to integrating the dual objectives of benefit realisation and safeguarding privacy.

Yours sincerely

Nick Koukoulas
Chief Executive