



30 November 2018

Attn: Regulating government access to C-ITS
and automated vehicle data

National Transport Commission
Level 3/600 Bourke Street
Melbourne VIC 3000

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

The Australian Trucking Association (ATA) welcomes the opportunity to provide this submission to the *Regulating Government Access to C-ITS and Automated Vehicle Data* discussion paper.

The ATA is the peak body representing trucking operators. Its members include state and sector associations, some of Australia's major logistics companies and businesses with leading expertise in truck technology. Through its members, the ATA represents thousands of trucking businesses, ranging from owner drivers to large fleets.

To build industry confidence in automated and intelligent technologies and encourage further uptake, a strong regulatory framework for data access and privacy is essential.

Data generated by co-operative intelligent transport systems (C-ITS) and automated vehicle (AV) technologies offers the potential to underpin continued innovation in transport safety and efficiency. However, operators using these systems in their fleets have highlighted the need for driver confidence regarding the protection of their privacy. It is only with robust privacy protections for users established through individual operators' policies that drivers have been willing to engage with the technologies.

Operators using these systems are reporting significant safety outcomes particularly in the mitigation of risk by monitoring driver alertness and behaviour. These systems create substantial amounts of sensitive data including video and audio recordings and health information.

Government collection, use and disclosure of this type of data must be limited. Appropriate privacy protections will help to lower user concerns and build broader trust ensuring the buy-in of drivers and uptake by trucking businesses.

Current industry best practice includes the development of company policies that

- clearly state that systems will only be operated with regard to the privacy and civil liberties of all employees
- ensure images or events collected are only viewed by authorised personnel

- require that digital footage is not stored by the user (the business). Digital footage is stored by the technology provider with robust security measures to prevent unauthorised access
- grant access to data in relation to an offence, possible offence or traffic incident only within 24 hours of an event
- require authorisation for access to data and decryption of information
- grant access to data for civil or criminal proceedings
- require requests for access to data be in writing and include a reason for the request.

Accordingly the ATA recommends that:

Recommendation 1

Governments should adopt

Option 2 – agree broad principles on limiting government collection, use and disclosure of C-ITS and AV information (reform option)

with particular emphasis on the establishment of

- Protections relating to data from biometric, biological or health monitoring technologies
- Incorporation of additional privacy limitations necessary to maintain individual privacy.

Recommendation 2

Access to C-ITS and AV data should be limited to uses that benefit the general public and improve safety outcomes by informing

- Safe vehicle and automated technologies i.e. through data provision for no blame safety investigations
- Efficient and safe transport systems
- Planning and policy development

Recommendation 3

C-ITS and AV data privacy protections developed by government must stipulate that data cannot be used for

- Commercialisation (such as insurers or those who seek to profit from access to data)
- Covert law enforcement or surveillance outside of current law enforcement standards/methods
- Data matching by government departments seeking to achieve outcomes unrelated to safety, policy or planning outcomes.

Recommendation 4

Government should treat C-ITS and AV data as ‘personal’ information as defined in the *Privacy Act 1988* (Cth) because this will

- Limit potential adverse effects on individuals
- Offer assurance to users that their information will be protected under privacy legislation in addition to any privacy protections in other laws such as road transport laws
- ensure consistency across organisations and jurisdictions.

Recommendation 5

Specific data types that are particularly sensitive should be defined as 'sensitive' as identified in the *Privacy Act 1988* (Cth) and be subject to additional limitations. Government should not collect, use or disclose sensitive data which would include

- in-cab audio or video recordings
- data from vehicle health or biometric sensors

It is noted that governments may access this data if

- required or authorised under Australian law, a court or tribunal
- to prevent threat to life or safety.

If you would like further information regarding this submission or would like to discuss these recommendations in more detail please contact Melissa Weller, Safety and Skills Adviser on (02) 6253 6900 or melissa.weller@truck.net.au.

Kind regards

A handwritten signature in black ink, appearing to read 'Ben Maguire', with a stylized, cursive script.

Ben Maguire
Chief Executive Officer