Australian Automobile Association

Mailing Address:
GPO Box 1555
Canberra ACT 2601

Address:
103 Northbourne Ave
Canberra ACT 2601

P 02 6247 7311
F 02 6257 5320
W www.aaa.asn.au

MEMBER OF FIA

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

30 November 2018

Dear National Transport Commission

RE: Regulating Government access to C-ITS and automated vehicle data

The Australian Automobile Association (AAA) welcomes the opportunity to respond to the National Transport Commission (NTC) Discussion Paper *Regulating Government access to C-ITS and automated vehicle data.*

The AAA is the peak organisation for Australia's state-based motoring clubs and their eight million members. The AAA advances the interests of all road users across Australia to ensure land transport networks are safe and sustainable, and that the cost and access to transport is fair for all Australians.

It is expected that C-ITS and automated vehicle (AV) technology will generate vast amounts of data, which could be used by government to improve the safety and efficiency of the transport network. By enabling government access to this data, agencies can:

- Manage traffic in real-time and improve the efficiency of existing assets (with flow on environmental and fuel saving benefits)
- Monitor transport infrastructure performance
- Target investments based on consistent and reliable data
- Target law enforcement activities.

The AAA believes the benefits of government access to C-ITS and AV data should be balanced with the need to protect privacy. The Discussion Paper's analysis of Australia's privacy and surveillance laws does highlight the potential privacy challenges arising from C-ITS and AV data, especially through data linking.

The AAA broadly supports the direction of Option 2 in the Discussion Paper, which ips to agree on broad principles to limit government collection, use and disclosure of C-ITS and AV data.

The AAA believes the principles should focus on building community trust in how C-ITS and AV data will be collected and used. A lack of community trust could limit uptake of AVs, which are expected to be safer, more efficient and more environmentally friendly. The recent Productivity Commission (PC) inquiry in Data Availability and Use found that people are more willing for their data to be used if they understand how it is being used, can see benefits and have control over where it is shared.[1]

In addition, the principles should be flexible to account for:

- Rapidly changing technology. While most technologies identified in the Discussion Paper are already available in new vehicles, it is not yet understood how these technologies will operate in the future, or how the data will be collected. Technologies and data use will evolve over coming years.

[1] Productivity Commission, *Data Availability and Use*, Productivity Commission Inquiry Report, No, 82, 31 March 2017, Finding 3.1 and 4.2

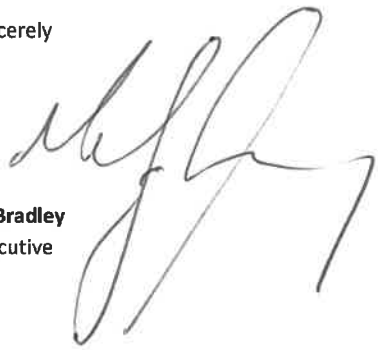
- Changing data handling practices. The Government has committed to implementing a new data sharing and release framework to oversee the integrity of data sharing and release activities of government agencies, following the PC data inquiry. Implementing new laws regulating government access to one sector without considering how it interacts with other laws and expectations will only create additional administrative confusion.

- International developments. While the Discussion Paper identifies that there is currently no coordinated international response to C-ITS and AV data use, Australia's response must consider how it interacts with international norms. Australia is a technology taker, importing 100% of new vehicles. Implementing regulation that is inconsistent with international norms would create additional administrative burden and potentially restrict vehicle choice in the future.

The AAA has responded to each of the questions outlined in the Discussion Paper in the enclosed document.

The AAA looks forward to progressing these matters with the NTC.

Yours sincerely



Michael Bradley
Chief Executive

Australian Automobile Association

Mailing Address:
GPO Box 1555
Canberra ACT 2601

Address:
103 Northbourne Ave
Canberra ACT 2601

P 02 6247 7311
F 02 6257 5320
W www.aaa.asn.au

MEMBER OF

AAA response to questions in the National Transport Commission Discussion Paper *Regulating Government access to C-ITS and automated vehicle data.*

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

The AAA believes the assumptions in the Discussion Paper are reasonable. The AAA agrees that C-ITS and AV data should be handled with care because it may not be possible to irreversibly de-identify the data generated by these technologies, given they are likely to contain many identifiers that could be linked with other government data sets.

However, the AAA believes the NTC should fully evaluate the practical application of data linking and re-identification of C-ITS and AV data. While it may be technically possible to identify a person by linking multiple data sets, it may not be in practical terms, given the immense volume of data that would need to be collected from multiple sources.

The AAA agrees that international frameworks around privacy are inconsistent, which makes it problematic to follow a particular international approach. However, international developments should be carefully monitored, and Australia's response should not be inconsistent with international norms.

The AAA believes that the NTC should distinguish between data and information – to ensure clarity of what is being discussed. The AAA supports the definitions outlined by the PC data inquiry, which is:

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

2. **Have we accurately captured current vehicle technology and anticipated C-ITS and automated vehicle technology (and the information produced by it)? Please provide reasons for your view, including whether there are any other devices that are likely to collect information internal and external to the vehicle.**

The AAA believes the Discussion Paper captures current and new technologies.

Whilst the potential technology listed is plausible, the AAA believes the usage may be somewhat overstated. For instance, it is not clear why it is important for a level 5 AV to be constantly video monitoring and recording occupants in a private vehicle scenario. Likewise, even in lower level AV scenarios where a driver monitoring system may be incorporated, such systems are likely to be closed loop, and responsive to recognising a pre-programmed set of behavioural characteristics the vehicle systems can understand. The intent of this technology is to interpret the human face, not who the human is, although it is recognised that it could be.

The AAA believes that smart phone connectivity should be included in the discussion. A technical study undertaken by the Federation Internationale de l'Automobile (FIA) Region 1 found that some vehicles synced to a smart device can also capture personal contact information from that phone, such as phone calls, email address and even personal images.[2] This is not captured in the Discussion Paper.

[2] http://www.mycarmydata.eu/#

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?**

The AAA agrees the privacy challenges arising from C-ITS and AV technologies mostly result from the volume of data they will generate. Most of the AV technology analysed in the Discussion Paper is already available in connected vehicles, or used in other sectors, but the data generated and captured at this time is limited. It is reasonable to assume that the potential to identify a person increases with the amount of data being captured.

The AAA notes that the challenges outlined in the Discussion Paper are technically feasible if it is assumed all systems are connected. It is not altogether apparent why a driver monitoring system would necessarily be designed with open connectivity unless it incorporates some sort of emergency mode say to identify a seizure or heart attack. A stated above, such systems are more likely to be closed loop, and responsive to recognising a pre-programmed set of behavioural characteristics. These technologies will need to be monitored over time to ensure responses reflect an actual problem.

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?**

The AAA does not have a legal opinion on what C-ITS and AV data will be personal or sensitive information.

As outlined by the PC data inquiry, the definition of what constitutes personal and sensitive information is always changing. For instance, in 2015 the exact meaning was considered by the Full Court of the Federal Court in Privacy Commissioner v Telstra Corporation Limited. This case found that not all data generated by a person's use of a phone automatically constitutes information about the person. The PC data inquiry states that the outcome of this trial is that:

> not all data generated by a person's use of a product or service will constitute personal information, even if the person may be reasonably identifiable by cross-matching the data with other information. As such, individuals will not automatically be entitled to access all of the information generated through their use of a product or service. The individual must be 'the subject matter' of the data.[3]

The above example highlights the challenge of developing a response to managing C-ITS and AV data based on the meaning of personal information.

The AAA believes a key aspect of managing C-ITS and AV data will be in ensuring community trust in how it is collected and how it is used, in addition to identifying what is personal information and what is not.

5. **Have we broadly identified the key reasons why governments may collect information generated by vehicle technology? Please outline any additional reasons governments may collect this information.**

The Discussion Paper provides a brief overview of the key reasons why governments may collect C-ITS and AV data.

The AAA believes C-ITS and AV data provides significant opportunities to improve traffic management and network planning. These opportunities will be available for government agencies across all levels, not just state government. For instance, the Bureau of Infrastructure Transport and Regional Economics is developing a road-speed performance and reliability dashboard using traffic probe data from HERE Technologies, supplied by

---

[3] Productivity Commission, *Data Availability and Use*, Productivity Commission Inquiry Report, No, 82, 31 March 2017, p.59

Australian Automobile Association

Mailing Address:
GPO Box 1555
Canberra ACT 2601

Address:
103 Northbourne Ave
Canberra ACT 2601

P 02 6247 7311
F 02 6257 5320
W www.aaa.asn.au

MEMBER OF

consulting firm Houston Kemp. The data will be used to consistently measure road speed performance and reliability and conduct before and after assessments for road infrastructure projects.

The AAA is also using traffic data from HERE Technologies and Houston Kemp for its Road Congestion in Australia report, which assesses speed performance and reliability of the arterial road network across all Australian capital cities. The AAA report is an example of the new opportunities C-ITS and AV data provide in managing and tracking the performance of Australia's transport infrastructure.

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 the Discussion Paper highlights, government collection powers and surveillance laws are inconsistent across jurisdictions, and law enforcement exceptions are particularly broad. The current frameworks may not prevent new surveillance activities above those generally accepted by the community as a result of C-ITS and AV data.

The effect of over-surveillance could deter public uptake of new vehicles, which are generally safer, more fuel efficient and more environmentally friendly.

7. **Is the current information access framework for government use, disclosure and destruction/de-identification sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology? Please provide reasons for your view, including what parties may be affected if there is no change.**

The AAA believes the current framework may not be sufficient to cover new privacy challenges, due to the inconsistent practices across states and territories regarding the use, disclosure and destruction of personal information. The privacy challenges are not necessarily new; they already exist due to technological developments throughout the economy. However, the volume of C-ITS and AV data that is expected to be generated means that existing information access frameworks should be reviewed.

The AAA believes the NTC should consider evaluating what cyber security standards should be in place to manage C-ITS and AV data. As stated above, over-surveillance could deter the public from purchasing new vehicles; however, a data breach with malicious intent would have an equally or even a greater impact on community trust.

8. **Are separate options for addressing the privacy challenges of C-ITS technology and of automated vehicle technology reasonable for achieving any future reform? Please provide reasons for your view**

The AAA supports the NTC in considering separate options to address privacy challenges for C-ITS and AV data. While there is a large degree of overlap, C-ITS and AVs can operate independently of each other and both technologies are likely to be deployed at different times. However, the AAA believes the principles for managing C-ITS and AV data should be consistent.

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

The AAA supports the NTC criteria for assessing the automated vehicle reform options.

10. **Is there is a need for reform to address the identified problem and the privacy challenges of automated vehicle technology (that is, option 1 is not viable)? At this stage of automated vehicle development, which option best addresses these privacy challenges while recognising the need for appropriate information sharing and why?**

The AAA supports the NTC developing broad principles to manage collection and use of C-ITS and AV data. The AAA agrees that existing laws and frameworks may not be sufficient to manage the privacy challenges arising from the volume of data that is expected to be generated by C-ITS and AV technology. However, given the technology is not yet widespread and the actual collection and use of the data is not yet fully understood, the AAA believes the principles must be flexible to ensure they meet changing community standards and international norms.

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

The AAA supports the NTC criteria for assessing the automated vehicle reform options.

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?**

As per question 10.

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

The AAA broadly supports the draft principles in the Discussion Paper. However, the AAA believes the NTC should take the following into consideration:

- The principles should reflect the considerable opportunities C-ITS and AV data provide government in improving the safety and efficiency of the transport network. A heavy focus on limiting the collection, use and disclosure of data could result in lost opportunities.
- The principles referring to regulatory responses should have regard for international norms to managing C-ITS and AV data.
- An additional principle which requires agencies to implement best practice cyber security management standards is worthy of consideration.