WA position on NTC discussion paper: Regulating Government Access to C-ITS and Automated Vehicle Data

Overview of WA position

Western Australia (WA) supports Option One: that the existing privacy protections and government data use management are adequate to manage the risk posed by government use of data collected by automated vehicles.

This has been agreed to by the Connected and Automated Vehicles Advisory Committee and represents a whole-of-government position.

The NTC paper highlights two important risks regarding government access to data generated by C-ITS and automated vehicles. Firstly, there is a possibility that the use of this data by the government poses a material risk to individual privacy. Secondly, the Discussion Paper highlights the risk that privacy concerns will be a barrier to uptake of this technology.

WA proposes that the material risks posed by government use of this type of data be signalled as a potential issue to an overarching privacy regulator, and included in the national, authorising privacy legislation. The WA Government, and the Department of Transport, is already tasked with protecting the use of highly sensitive licensing data, and the protections in place are effective. In addition, WA is currently developing privacy principles, which will further clarify the need for data use by Government. These are expected to be finalised in the next year.

The Discussion Paper identifies that there "risk that broad collection and use by government of this information will be a barrier to the take-up of C-ITS and automated vehicle technology in Australia" (pg 2). WA is unaware of evidence suggesting that this is the case. If *perception* of privacy does prove a barrier, we would suggest this be better addressed through non-regulatory levers, such as behavioural insights and messaging.

Western Australia would accept the generation of high-level principles, if this is the overwhelming consensus among the State governments. However, we would highlight that the benefit of having high level principles is unlikely to be greater than the costs which would include:

- The costs of developing and agreeing to the principles;
- The opportunity cost of focussing on more urgent work to support the safe deployment of automated vehicles; and
- the cost of increased complexity and duplication between this and other regularity arrangements already safeguarding government use of data.

To reduce the above costs, we would recommend clear, concise and simple principles (example provided in Attachment A)

Please find responses to the consultation questions, which have been prepared in consultation with state government agencies.

Consultation Questions:

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

WA supports the assumption that it is difficult to irreversibly de-identify personal information given the significant breadth and depth of data collected as well as the fact that information collected will contain many identifiers.

WA supports the assumption that there is no consistent international approach to follow. The two international approaches identified vary significantly and following one over the other would be conjecture.

WA supports the need for legislative powers to enable access to AV information and notes that the safety assurance system will include data recording and sharing criterion.

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.***

Yes, current vehicle technology has been identified adequately in the paper. It is difficult to know exactly what level of C-ITS and automated vehicle technology will be built into AVs in the future however the paper has sufficiently anticipated what data may be collected. For this reason, it is difficult to establish and agree to specific principles without knowing what the reality may be.

The use of any video recording for driver recognition and to monitor driver alertness is no different to how they are used in taxis and other vehicles today – that is it is primarily a safety application. However, if cameras are to be extended for monitoring the whole of cabin of a private vehicle, it would be a challenge for privacy. If the vehicle is a shared or public, then this shouldn't be regarded as a new challenge for privacy, as current public vehicles such as buses and trains have such cameras installed on them.

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?***

As noted earlier, it is difficult to anticipate the technology that will be actualised in AVs and therefore the privacy challenges identified may or may not be realised.

With regard to the video recording internal to the vehicles, the privacy challenges identified anticipated for C-ITS and AV technology are specific to lower levels of autonomy. Therefore, these privacy challenges may only be short term challenges – dependent on how long technology takes to move from semi-automated to

fully automated vehicle technology. In the highest levels of vehicle autonomy, there will never be a need to monitor driver recognition, alertness and behaviour given that there will be no driver.

Similarly, the use of biometric, biological or health sensors to monitor alertness and behaviour of human drivers would be an issue in vehicles with lower levels of autonomy but not at higher levels. To some extent this information is currently collected by a number or wearable fitness trackers and users have embraced this technology without any care for 'privacy challenges'. WA suggests that more data is needed to determine the extent of this challenge.

WA agrees that in-cabin and external microphones are unlikely to present new challenges. The use of microphones to *listen in* to conversations are currently used by devices such as the Google Home Mini and Amazon Alexia and the public continues to embrace this without many concerns. WA believe surveillance device laws are quite restrictive and governments may not be able to collect any C-ITS or AV data without amending the existing SD laws.

The privacy challenge created by an AV's ability to recognise drivers and occupants could be negated by the occupant's ability to opt in or out of the customised experience. This raises the questions of how to protect vulnerable occupants who may not understand the implications of sharing personal data- for example young users, some disabled users where consent, or an 'opt out' is required?

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 ability for C-ITS and automated vehicle technology to generate information or form an opinion about an identified individual as described by the *Privacy Act (1988)* is considered personal information. For example; biometric sensors that can record fingerprints and therefore identify an individual as well as make judgements regarding the individual's ability to control take a vehicle – whether this is true or not.

C-ITS and AV technology is likely to generate sensitive information regarding the health or biometric information on an individual. Sensitive information described in the *Privacy Act (1988)* may not necessarily be generated in real time but could be used to identify an individual once linked with other data.

Currently health data is considered 'personal information' but other data such as consumer choice, location, movement are not necessarily considered personal or sensitive. Yet it is possible that this data can also be used to control or manipulate, if in sufficient quantity and detail. Nonetheless, C-ITS data should be controlled as per any other information considered by the Privacy Act.

The WA position is that personal information is personal information no matter the method of which it is collected by and therefore the privacy principles which are currently in development will adequately cover the privacy of the information that will be produced by C-ITS and AV technology.

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.

Yes, the key reasons for government collection of information have been broadly identified in the discussion paper. The following are a list of other potential uses of data that government would or could be interested in, including (but not limited to):

- Improving the delivery of government services and infrastructure (including, but not limited to, transport services);
- Providing private sector access to government data to facilitate third party services (e.g. contribute to the "transport" internet of things, or providing the data required to ensure affordable third-party mobility services are available in a region); and
- For revenue collection or demand management purposes at some future point in time (e.g. road user charging / congestion charges for empty vehicle travel).
- In addition to road safety, data may also be used by the government for other security purposes, such as terrorism threats, criminal investigations etc.
- Would the government use health data to trigger emergency response or warnings for example if body temperature and glucose levels were recorded.
- Feed into open data arrangements already in place (https://imovecrc.com/news-articles/intelligent-transport-systems/australian-transport-open-data/), e.g. third-party access for commercialisation/research/etc

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.

The current information access framework for government collection is sufficient to cover privacy challenges. However, given the sheer depth and breadth of information that will be collected for the first time by C-ITS and automated vehicle technology, it would be beneficial to revisit the information access framework considering this new data.

WA supports the regulation being outcomes based, so that as data privacy legislation changes to keep up with technology, so too will legislative controls.

Once again, WA notes that the state is currently developing privacy principles, which will further clarify the need for data use by Government. WA also has strict surveillance laws, which would further limit data use.

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.

Yes, as above. There is sufficiency in the current framework however there is also benefit to be gained from reassessing the framework. Given the nature of the collection and use of data is unknown the framework must be robust enough to cater for a range of uses and collection methods. As a principle,

emerging/developing technology such as AV and C-ITS should trigger a review of existing arrangements to ensure they are appropriate. The collection of personal information for law enforcement purposes (which is for overall good of the community) is likely to be acceptable to most of the public.

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.

Separate options for addressing the future reform is reasonable given that there is more difference than overlap of the nature of the data gathered by the two technologies. The data generated from AV technology is more likely to be of a sensitive nature and therefore will require more stringent guidelines around it.

The application of an outcomes-based approach is appropriate as the level and type of technology employed may vary between and within different levels of autonomy. WA supports a formal scoping exercise as a preliminary step to gain a greater understanding of whether separate options are beneficial.

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

While the criteria are helpful, it is good practice to include an assessment as to whether the proposed options address the problem identified. The Discussion Paper poses the problem as the risk that *public privacy concerns may be a barrier to uptake*. It would be helpful to include an assessment criterion which assesses which option best reduces the barrier to uptake of AVs.

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?

From a WA perspective, Option One is viable. However, for national consistency there could be benefit in having broad principles around the collection and use of this information.

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

See question 9.

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?

WA supports Option One. As with the reform around AV technology, WA does not support the limitation of data collection for government. WA recognises that there is benefit in having broad principles that enable flexibility for the development of the C-ITS framework

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

Yes the draft principles adequately address the concerns around privacy created by the collection of data by C-ITS and AV technology. With regard to Principle 7, for the purposes of government data collection, allowing users to opt in and out is unnecessary. This is more appropriate for non-government data collection and usage.

Illustrative privacy principles

1. Nationally agreed definition of personal information.
2. Personal information should be collected legally and de-identified before use by government.
3. Personal information should be collected for a specific purpose and used for that purpose.
4. Management, use, storage and disposal of information should be secure and ethical.
5. The government should be able to collect de-identified personal data for purposes of law enforcement, or to meet other legal responsibilities of the state.
6. Privacy protection measures should be regularly reviewed to ensure they keep pace with technological changes.