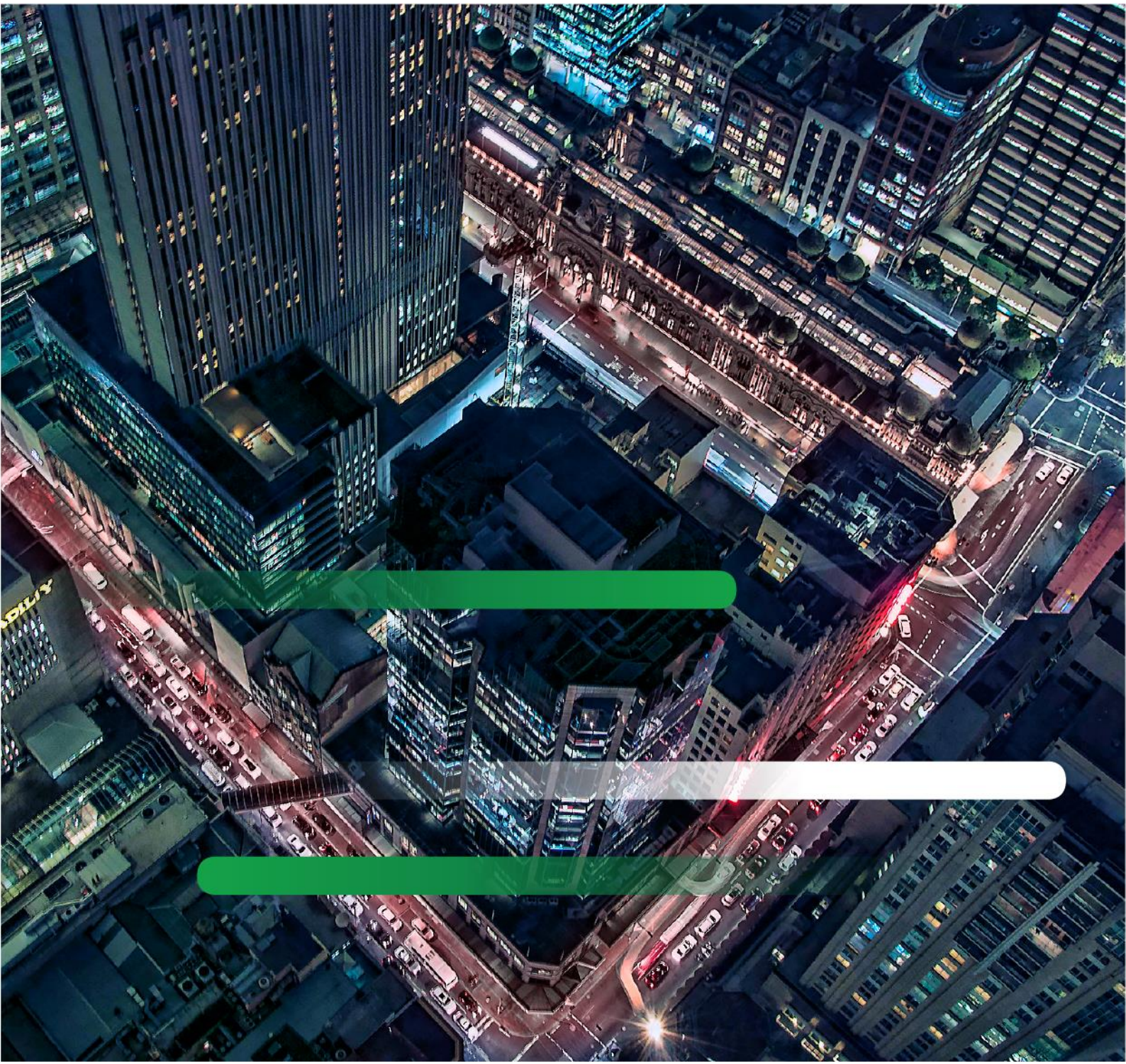
Transurban

Response to the NTC's regulating government access to C-ITS and automated vehicle data discussion paper



Reponse to the discussion paper

Transurban is pleased to respond to NTC's consultation process for Regulating Government Access to C-ITS and Automated Vehicle Data which was released in September 2018. This is another critical component of establishing a trusted environment in Australia for the introduction of automated vehicles and encouraging a future transport operating regime that delivers the safety and efficiency benefits promised by current directions of technology and process.

Our response is in the form of two over-arching discussion points, followed by responses to the individual consultation questions.

1. Discussion points

1.1 The position of a privately owned road operator, such as Transurban, is not addressed in the paper and remains unclear.

We note the paper's primary focus is on government agencies gathering C-ITS and automated vehicle data. There is also an evaluation of private capture of data centres for vehicle manufacturers or suppliers gathering safety-related data. We believe there is an opportunity to also consider private operators of transport infrastructure, including toll-road operators such as Transurban and its peers, which are likely to be gathering travel data.

A toll-road-concession holder, such as us, will not have the same range of alternative data sources to compare the vehicle-related information, an issue that is important in the discussion of the nature of personal information. Therefore, we see the position of toll-road operators as uncertain in the analysis and suggest that further policy development should include recognition of this boundary issue.

We would prefer to see a clear statement that any new regime would apply to government agencies not private operators. Private operators such as Transurban, would need to assess new information sources and treat such information as required by the Privacy Principles.

1.2 It is not clear that a new regulatory framework, supported by legislation, is required to deliver the necessary level of privacy protection.

The discussion paper recognises that there is an existing framework of privacy protection reflecting Commonwealth privacy principles covering all states and territories, with the exception of Western Australia. It then suggests that a new framework is required, largely on the basis of an increasing breadth and depth of information and that there may be new types of information that were not contemplated when the current privacy principles were developed.

The paper states that these new types of information will challenge the existing principles. While we defer to the NTC's extensive examination of this issue, like many organisations, we generally prefer the application or amendment of existing legislation over the creation of new laws or regulations. In this vein, we wondered if the broad nature of the existing principles, spanning the collection, use, protection, disclosure and destruction of personal information, could provide adequate privacy protection for the community as well as the flexibility required to ensure their ongoing relevancy in the face of this rapidly changing transport technology.

However, we note, that applying the existing principles to the transport task would require a focus on their consistent application across jurisdictions - a sizeable task as in practice (and as the NTC notes in their paper) there is inconsistent application of the existing principles now across the different states. Ensuring consistency across state jurisdictions would be an ongoing issue in governing the application of any national principles – whether the existing ones are utilised or a new set of principles are created.

2. Comments on individual consultation questions

Our comments on specific questions posed in the discussion paper are included over the next few pages. We hope these comments provide constructive feedback on a complex set of issues and help find a path to an appropriate regime for both government and industry.

Question	Comment
1. Are the assumptions the NTC has identified for this discussion paper reasonable?	There are three assumptions and these are separately addressed: a. That it is difficult to irreversibly de-identify personal information – reasonable evidence is provided for this. b. That differences in other jurisdictions, especially the EU and across the US, mean that NTC should not follow any international model – whilst it is acknowledged that there are differences internationally, this need not necessarily mean that international models are not appropriate or could at least provide learnings that could add value to the Australian context. c. That NTC may propose specific legislation for the safety assurance scheme data access – this is a sound assumption as it is under NTC control.
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 core embedded devices in C-ITS and AVs appear to be well covered. However, we query whether consideration should be given to the role of customer-owned 4G and future 5G devices within the vehicle in the dissemination of vehicle-related data. At least one of these is usually connected to contemporary vehicles and this provides a parallel channel to the direct C-ITS route. The obvious application that is increasingly being used in this way is navigation and we are reaching the point at which it will be more common to present a phone app on the dashboard than use embedded software, although not necessarily for AV operation. Though we note, this may have been left out of the discussion paper as it is not in the direct path of Dedicated Short-Range Communication transmission and the privacy issues will be more relevant to companies such as Google and Apple. Nevertheless, for completeness, it may be useful to recognise the potential for future crossover.
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?	There are two types of privacy challenge presented. The first recognises that basic information such as vehicle speed, position and route from the CAV may not necessarily be different from today's data, but that the volume and breadth of the potential data gathered will give rise to new challenges. This is overlaid with the potential of government to link such data to other sources. As noted in the previous section, we question whether the creation of more data would necessarily

	preclude the application of the existing provisions. The discussion paper does not fully explain how the volume and complexity of expected data loads will threaten the existing privacy principles and we wonder if there was additional discussion available in relation to this point. The second type of data challenge noted in the paper relates to new types of information that may be collected by biometric, biological or health sensors in automated vehicles. These may be installed to allow real-time assessment of the ability of an occupant to take back control if required. The point is well made that this type of information differs from that collected by current vehicles and may be particularly sensitive, because it captures an individual's emotional, cognitive and behavioural attributes and state, as well as health information. We recommend, at least for private organisations such as Transurban, the more stringent obligations in relation to sensitive information under the current Privacy Principles continue to apply.
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?	There will be a great deal of information generated by C-ITS operations. This will include basic parameters such as speed and position of a vehicle, which will support many of the safety applications. The key question here is whether this should be considered personal information. As the discussion paper notes, on face value, it may not normally be captured by the standard privacy definitions of personal information. This is because the C-ITS software protocols have been set up to give each vehicle a set of pseudonyms which it will rotate through during a journey. This is to prevent the very risk that a receiver of the information could otherwise reconstruct a journey and associate it with an owner of a vehicle, for example, using registration information. Instead the pseudonyms will randomise the data. The discussion paper then draws on analysis in its supporting papers by UNSW and Van Dijk to show that under certain circumstances it may be possible to reverse engineer the process and associate C-ITS data with a particular vehicle and then, via correlation with the registration database, with its owner. We support a prudent approach being taken by government agencies, though we would encourage analysis of new sources of information and the context in which they will be collected, used and disclosed so as to determine whether it is or isn't personal information. However, this does not necessarily mean that a new regime for protection of such information is required.

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. Section 5 provides a good coverage of the likely reasons for collection by government.
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. *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? Please provide reasons for your view, including what parties may be affected if there is no change.*	Point 1.2 in our preamble is relevant to our response to Questions 6 and 7.We suggest that the careful application of the existing Privacy Principles should be able to support the life-cycle of collection, use, disclosure and destruction of C-ITS and AV information. However, like in the application of any national approach, effort will be required in ensuring consistency.
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 should not be required for the consistent application of Privacy Principles to each of the two domains. Separate consideration of the status of data types may well be required, for example, to determine whether particular sets of information within each domain should be considered personal information.
9. Are the criteria for assessing the automated vehicle reform options comprehensive and reasonable?	The three criteria are: a) *recognises the identified new privacy challenges of automated vehicle information and the likely inability of Australia's information access framework to sufficiently address these* b) *ensures that beneficial future uses of automated vehicle information are not restricted* c) *provides appropriate flexibility for developing the overall automated vehicle legislative framework (such as new powers for government to collect automated vehicle information). This includes ensuring that artificial barriers are not created at this stage of automated vehicle reform development.* Our comments on each are as addressed in the same sequence: a) This criterion assumes a new regime is required and that the existing framework is unworkable. As noted in our previous responses, we query whether the existing principles could be applied. We note the extensive work

	undertaken by the NTC and wonder if there is further discussion on this point that might be made public to provide further clarification on this evaluation. b) This is an appropriate criterion, which makes no inherent assumptions about the outcomes. c) We considered this criterion to be seemingly at odds with the arguments presented within the discussion paper. The paper largely builds the case that there are insufficient protections for government access under existing provisions and we note that the purpose of this criterion appears to be building in capability to add new powers. We accept that this is possibly to create flexibility and provide a level of "future-proofing". It is probably the case that the broader reform examination of law enforcement requirements will identify areas for legislative reform thus eliminating the need to capture them in the criteria for privacy evaluation.
10. Is there is a need for reform to address the identified problem and the privacy challenges?	We do believe there is a case for reform to deliver consistent application of existing Privacy Principles. We suggest that the most appropriate response would be a variation of Option 1 – rather than 'no change', a better response might be to work within the existing privacy framework to ensure clear and consistent application of Privacy Principles.
11. Are the criteria for assessing the C-ITS reform options comprehensive and reasonable?	The criteria are similar to those for AV information: *a) recognises the identified new privacy challenges of C-ITS information and the likely inability of Australia's information access framework to sufficiently address these* *b) ensures that beneficial future uses and applications of C-ITS information are not restricted* *c) recognises that the C-ITS framework in Australia is in the early stages of development and provides appropriate flexibility for its development.* Criteria a) and b) are essentially the same as those addressed under question 9 and our comments there apply here as well. Criterion c) is a more generic form of the earlier version, without reference to legislation. In our view, this is a more appropriate expression of the requirement
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	Our position is the same as that expressed in response to Question 10. We do believe there is a case for reform, at the very least to deliver consistent application of existing Privacy Principles. We suggest that the most appropriate response would be a variation of Option 1 – rather than 'no change', a better response would be to work within the existing privacy

the need for appropriate information sharing and why?	framework to ensure clear and consistent application of Privacy Principles.
13. Would the draft principles adequately address the privacy challenges of C-ITS and automated vehicle technology?	The proposed principles may address the privacy challenges, but, we suggest that an improved application of existing provisions could also be effective. This would not necessarily require a new layer of regulation or new legislation. Finally, as mentioned earlier, we hope to see a clear reference to the role of private operators of road infrastructure in any further analysis and would welcome discussion with the NTC on this point if it could prove useful to your program of work.

-ENDS-

CONTACT

Transurban

Senior Manager, Strategic Initiatives

Jeremy Nassau

Email jnassau@transurban.com