9 July 2020

National Transport Commission
submitted to enquiries@ntc.gov.au

Dear Sir / Madam,

RE: *Government access to vehicle-generated data* Discussion Paper

Communications Alliance welcomes the opportunity to make a submission to the National Transport Commission (Commission) *Government access to vehicle-generated data* Discussion Paper (Paper).

The Paper raises 19 specific questions. In the following, we will focus on Questions 2, 7 and 18. This is not to say that individual members may not have a view with regard to other issues discussed in the Paper. For the purposes of our submission, however, we will concentrate on matters that we believe go to the creation of an effective and sustainable framework for Government access to vehicle-generated data (VGD).

Broadly speaking, the Paper seeks to drive the discussion as to how to create (where currently non-existent) and improve Government access to VGD. The primary purpose (at this stage) of such access to VGD is to improve road safety.

In various sections of the Paper (e.g. 4.3.5), the Paper contemplates the transmission of real-time data from vehicles to Government agencies (or a data aggregator). In the absence of any other networks capable of transmitting the data at a larger geographic scale and volume, we assume that it is envisaged that commercial mobile networks would be used for this purpose.

It is not quite clear to us whether the data to be transmitted would exclusively be transmitted 'over the top' (OTT), i.e. within an application that sends and receives the VGD (e.g. similar to WhatsApp), or whether – at least to some extent – it is being contemplated that data (e.g. location data) be transmitted (as metadata) from a SIM embedded in the vehicle. If VGD is being transmitted OTT, then such content is neither visible to mobile network operators (MNOs), nor would those operators have the ability to decrypt the data. Access to OTT content could occur through existing processes, e.g. on the basis of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), or through some form of new agreement between agencies and the application provider.

To the extent that the VGD is not transmitted OTT and could constitute some form of metadata (e.g. location data of a vehicle SIM that is being transmitted outside an application and sought to be accessed by agencies), further considerations around disclosure restrictions and privacy obligations may be warranted. We will discuss those under sections 2 and 3 below.

Against this background, we note the following:

1. Mobile network capacity and associated costs

It is likely that the data volumes to be transmitted will be substantial. These additional volumes need to be factored into the dimensioning of mobile networks and could require substantial amounts of additional CAPEX to be spent to facilitate the transmission of this data. Given the moving nature of vehicles, these expenditures would also not be limited to specific geographic locations (cells) but would need to be fairly ubiquitous (at least along major transport pathways and in urban areas) to allow for the transmission of large volumes of data in real-time, e.g. where an accident has occurred and congestion arises as a result. In addition, mobile networks may incur increased operational costs.

Any access arrangements that seek to make use of commercial networks ought to adequately account for the costs incurred by mobile networks and allow for appropriate compensation of and/or cost recovery by those networks, including through (but not limited to) usage charges.

Proponents of the proposed Option 2 (or Option 1 and 3 for that matter) may seek to argue that the public good, i.e. potentially improved road safety, merits a 'commercial sacrifice' by the involved parties, including by MNOs. However, it is important to note that the transmission and use of data will soon underlie every aspect of our lives, many of which will (hopefully) have some public good component. It would be unrealistic, and in our view unreasonable, to expect MNOs to subsidise our data economy without being able to realise an adequate economic return.

2. Storage of VGD

For the purposes of sections 2 and 3, we use the term VGD as meaning data that is not being transmitted OTT.

Where VGD is being transmitted by mobile networks and irrespective of the subsequent flow of data, MNO's technical and operational needs would likely require the storage of the data that they receive from vehicles. As with transmission capacity, storage capacity requirements are likely to be substantial and need to be accounted for in any cost-benefit analysis.

It is also not clear on what legislative and/or contractual basis MNOs would store VGD. In our view, the TIA Act (and more specifically the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*) does not provide sufficient legal clarity on whether communications between machines, sensors and connected 'things' without the direct involvement of a person form part of the data categories that must be retained by carriage service providers (CSPs) under the TIA Act. We have previously argued – and continue to do so – that this does not appear meaningful but would, if pursued for implementation, cause exorbitant costs to CSPs and imply an explosion in the amount of data that would be required to be retained.

Consequently, we argue that the legislation ought to put beyond doubt that such communications are excluded from the data retention regime, and that storage of VGD by MNOs, if indeed technically/operationally required and pursued, ought to be facilitated through contractual arrangements.

3. Disclosure of and access to VGD

The proposed Option 2 (and potentially also Option 1), which does not envisage legislative change, appears to assume that MNOs would be able and permitted to disclose VGD to Government agencies.

Part 13 of the *Telecommunications Act 1997* (Act) prohibits the disclosure by CSPs of "any information […] that relates to the affairs or personal particulars […] of another person".[1] The 2017 legal proceedings in *Privacy Commissioner v Telstra Corporation Limited* (Ben Grubb Case) and the discussions around 'information about a person' vs 'information relating to a person' highlight that the delineation between personal information and other information is subject to debate. Importantly, the Office of the Australian Information Commissioner states that "By using the broad phrase 'relates to', the CDR [Consumer Data Right] regime captures meta-data"[2], thereby taking a clear stance in a CDR context. It is not inconceivable that a similar view could be taken with respect to VGD, or at least subsets of VGD, particularly with respect to location data.

On this basis, and unless stated otherwise in the legislation, we would assume that VGD must not be disclosed by CSPs, unless subject to the disclosure exemptions created in section 280 of the Act. In the majority those exemptions relate to disclosures to Law Enforcement Agencies (LEAs) who request access pursuant to the TIA Act. (In this context, we note that access to data by LEAs retained under the data retention regime does not require a warrant.) Note that the TIA Act deliberately limits disclosure to 22 Law Enforcement Agencies and specific crimes and does not permit disclosure to other Government agencies.

This means that, in our view, in order for MNOs to be permitted to disclose VGD to transport agencies etc., legislative change would be required to either put beyond doubt that VGD does not fall into the categories of information that is protected by section 276 of the Act, or to create an exemption for the disclosure of VGD, similar to the exemptions established for the purpose of assisting the Australian Communications and Media Authority, the eSafety Commissioner or the Telecommunications Industry Ombudsman (section 284).

It is also worth pointing out that MNOs would not be in a position to aggregate or anonymise data and, thereby, potentially the data would fall outside the definition of information that is protected from disclosure by section 276 of the Act.

While the proposed Option 2 - a Government and industry data exchange partnership - appears to be the most attractive approach to improve Government access to VGD and establish a governance framework, we are concerned that a partnership without legislative change may not be able to achieve the desired outcome if some of the VGD was not being transmitted OTT.

Our industry is keen to remain engaged with this process and to work cooperatively with all stakeholders to establish an effective and efficient framework for the use of VGD in Australia. The principle of non-commercial sharing or exchange of such data between data providers and data recipients (i.e. the end-points of the data exchange) appears to be a useful starting point for a partnership. However, we note that this principle ought not to be taken to mean that all intermediaries and parties within the 'supply chain' of the data will be able to provide services on a non-commercial basis.

[1] Section 276 (1), Telecommunications Act 1997
[2] Chapter B: Key concepts, B.48, https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-b-key-concepts/

We look forward to further engaging with the Commission and all relevant stakeholders on this important project.

Please contact Christiane Gillespie-Jones (c.gillespiejones@commsalliance.com.au) if you have any questions.

Yours sincerely,

John Stanton
Chief Executive Officer
Communications Alliance