Maurice Blackburn Pty Limited
ABN 21 105 657 949
Level 21
380 Latrobe Street
Melbourne VIC 3000

DX 466 Melbourne
T (03) 9605 2700
F (03) 9258 9600

3 July 2020

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

By email: automatedvehicles@ntc.gov.au

Dear Sir/Madam,

We welcome the opportunity to provide feedback in relation to the NTC Discussion Paper on Government access to vehicle-generated data.

Maurice Blackburn Pty Ltd is a plaintiff law firm with 33 permanent offices and 31 visiting offices throughout all mainland States and Territories. The firm specialises in personal injuries, medical negligence, employment and industrial law, dust diseases, superannuation (particularly total and permanent disability claims), negligent financial and other advice, and consumer and commercial class actions. The firm also has a substantial social justice practice.

In this submission, we do not seek to respond to every discussion question. Rather, we have identified those where we believe Maurice Blackburn's experience and expertise can add value to the discussion, and have responded to those below.

In particular, we address the following:

- We agree that the use of vehicle generated data to improve road safety is an appropriate starting point.
- It is vitally important that the consumer voice, and the voice of road users more broadly, continue to be heard in discussions between industry and government about data sharing.
- We see the ownership of data as central to this consultation. In any consideration of access to data, consumer privacy and trust in the process should be at the forefront.
- Public interest should drive any decisions as to what data is collected and shared.

Our responses to selected discussion questions appears below.

Question 1. Do our problem and opportunity statements accurately define the key problems to be addressed, and do they capture the breadth of problems that would need to be addressed?

Maurice Blackburn believes that the problem and opportunity statements in the Discussion Paper accurately capture a number of the key problems to be addressed, and the opportunities that exist to rectify those problems.

We offer the following observations in the hope that it might inform possible extensions to those problem and opportunity statements.

We agree with the statement on page 19 that: "*Oversharing and undersharing of data can create problems*".

We believe that the core issue here is the lack of trust that consumers have with government and industry to not misuse data. This is well captured on page 19 of the Discussion Paper where it says:

> *The vehicle industry is also reluctant to share data with governments due to concerns over the breadth of purposes it could be used for, particularly because many agencies hold roles both as regulators and transport system operators. Industry reluctance is founded on valid concerns of government use of data detrimentally impacting on them or their customers. This could include enforcement or compliance action, inadvertent release of commercial intellectual property and customer privacy.*

We are reminded of parallels between this discussion and that surrounding the release of the COVID Safe App. The uptake for that program never achieved the targets set by the government. Privacy is reported as a major reason for people refusing to download the app[1]. Obviously, some sort of social licence needs to exist between the data collector and the consumer in order for them to engage in these data sharing projects. The disappointing uptake seems to indicate that a lack of trust will trump the worthiness of the cause.

In response to the poor uptake, the Federal Government needed to provide legislated assurances[2] that:

- The data was depersonalised/anonymised
- The data would not be used to 'track' individuals
- Breaches of user consent would lead to harsh penalties
- There would be strict, legislated restrictions as to who could access the data
- The data could not be on-sold for other purposes
- There were legislated privacy protections[3] in place.

Maurice Blackburn urges the NTC to bear in mind the issues associated with de-identified data. There have been a number of high profile cases[4] where de-identified data has been published, only to be re-identified thereby resulting in a major privacy breach.

---

[1] https://theconversation.com/70-of-people-surveyed-said-theyd-download-a-coronavirus-app-only-44-did-why-the-gap-138427

[2] See for example https://www.theguardian.com/australia-news/2020/may/04/government-releases-draft-legislation-for-covidsafe-tracing-app-to-allay-privacy-concerns

[3] https://www.legislation.gov.au/Details/C2020A00044

[4] See for example: https://ovic.vic.gov.au/mediarelease/information-commissioner-investigates-breach-of-myki-users-privacy/; https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/mbspbs-data-publication/; https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records

This risk has real-world consequences for consumers. Consider an example of a domestic abuse survivor whose abusive partner is able to track their partner's movements through vehicle data. The risks of not getting this right can be enormous.

It is said that data is the new currency[5]. If this is the case, the data generated by automated vehicles would have significant monetary value[6].

This brings forward questions of data ownership. Section 1.7.3 of the Discussion Paper assumes that data generated by automated vehicles may be owned by the vehicle manufacturer or providers of a telematics service, and '…*governed by common law and the agreements made when buying a new vehicle or engaging a vehicle data service'*. Maurice Blackburn urges the NTC to consider whether the road user or vehicle owner – those whom the data is about – *should* have some degree of ownership and therefore control of the data via 'opt-out' data access mechanisms.

Consumers need assurances that government and industry will resist the temptation to monetise the collected data.

Maurice Blackburn believes that unless similar protections are afforded for data collected from automated vehicles as were legislated for the COVID Safe App, the willingness to share that data may be difficult to obtain.

To that end, Maurice Blackburn offers the following as possible extensions to the Opportunity Statement on page 20 of the Discussion Paper:

i. As mentioned above, we see this process as an ideal opportunity to firm up questions around data ownership, further articulating the importance of consumer rights to ownership of data and how that data is used (see also our response to Question 4 in relation to data storage);
ii. We believe that one of the prime opportunities to arise from this process would be for the development of clear principles that articulate the circumstances where data sharing is appropriate, as opposed to there being access to an ongoing stream of data which can then be put to particular uses; and
iii. That there should be a clear focus on minimisation of data collection, such that only data that is to be used for an identified public good (such as road safety) should be collected and then used.

Question 2: In our table, have we accurately captured all the regulatory and legislative mechanisms government could currently use to access vehicle-generated data?

Maurice Blackburn is unable to identify any specific legislative process which directly gives government access to vehicle generated data, outside those already contained in Table 1 on page 32 of the Discussion Paper.

We bring to NTC's attention that government agencies, such as compulsory third party insurers for road accidents, may also access vehicle-generated data as a result of the carrying out of administration of statutory injury schemes, usually with the consent of the claimant. This may occur in a similar way to their current access to dash cam footage

[5] See for example https://www.forbes.com/sites/michelleevans1/2018/03/12/why-data-is-the-most-important-currency-used-in-commerce-today/#6603545354eb
[6] We note the estimates provided by McKinsey and Company in section3.2.3 of the Discussion Paper.

provided by a claimant seeking to provide insight as to the circumstances of a transport accident.

Question 4: Do you agree with our assumptions on the currently low uptake and limited availability of technology that supports the generation of vehicle data and that there are few and limited current government access arrangements for vehicle-generated data?

Maurice Blackburn agrees with the NTC's assessment that there are few and limited current government access arrangements for vehicle generated data.

We believe, however, that this level of access may be appropriate.

Maurice Blackburn believes that any increases in government access arrangements must be clearly done with an agreed and identifiable cause – such as road safety – in mind. The cause must come before any increase in access.

NTC is correct in noting a series of unique risks associated with vehicle generated data in section 3.5, on page 34 of the Discussion Paper:

Cybersecurity risks:

The risk of data being obtained through cybercrime is an ongoing issue, as is the potential for damage to be caused through the hacking of automated systems.

Modern vehicles contain highly sophisticated hardware and software as a matter of course. This kind of technology provides functionality, but it also increases the surface attack area for hackers with nefarious intent. Digital security of modern vehicles is therefore a critically important factor when considering data collection and sharing arrangements.

For many reasons, open source software has significant advantages over closed or proprietary programs, as it allows coders and developers to collaborate for the purposes of identifying vulnerabilities in code before the product is shipped. It also allows consumers to understand what this technology is being used for, thereby generating trust.

The NTC must have digital security front of mind when designing data sharing arrangements. Maurice Blackburn suggests the NTC consider the use of open source software, or open standards among manufacturers at the very least, in respect of programs for data collection for road safety objectives[7].

Data storage systems:

We note that this section (along with section 3.4 of the Discussion Paper) refers to the use of data to assist in settling legal liability issues that may arise as a result of road safety or enforcement processes.

In the past, we have argued that a streamlined and cost-efficient mechanism to access event/accident data could rationalise the process of insurance claims and reduce litigation. This would be favourable to all parties and reduce the burden on the public purse of

[7] This has broader implications than cyber security issues. It is worth noting that Volkswagen was only able to defraud its emissions data because they were using hidden, proprietary code. See for example https://www.nytimes.com/2015/09/23/nyregion/volkswagens-diesel-fraud-makes-critic-of-secret-code-a-prophet.html

protracted and complicated litigation, particularly if it can be made available soon after the accident in order to settle questions of fault.

We note that currently, the only mechanism for an injured person to access event data is through a direct request to the owner of the data, which could be refused, or through discovery processes as part of actual or anticipated legislation.

We submit that this creates a significant disadvantage to the injured person and affords an inequitably powerful position to the manufacturers (if they are deemed to be the owners of the data) who, as the potential defendant, have an interest in protecting the data.

Therefore, we submit that decisions around data ownership should prioritise the enabling of road victims to enjoy early and transparent access to event data in order to ensure issues of fault are dealt with expediently and to avoid issues of power imbalance.

We further submit that this will be essential to community acceptance of automated vehicle technology. Without regulation of early access to data, or a shift in focus to consumer ownership of data, concern around unfair disadvantage in assignment of fault after an accident could result in a reduced uptake of the technology.

Question 5: What issues do you believe will be created if ExVe is adopted and that would need to be considered in Australia?

We note page 45 of the Discussion Paper where it says:

> *The European Vehicle industry has outlined its view that access to vehicle-generated data by third parties, including transport agencies…, will be delivered through the 'extended vehicle concept' (ExVe). ExVe is intended to reduce 'attack surfaces' to the vehicle by 'extending' the vehicle onto the vehicle manufacturer's server and controlling access only through this server.*
>
> *The ExVe aims to reduce interfaces to the vehicle to only those required by law…., or those that connect to the vehicle manufacturer's server or a neutral server.*

We agree that the key point, as detailed in the Discussion Paper is that:

> *A key aspect of the ExVe is its neutral server, which enables entities other than the vehicle manufacturer (including governments) to access data directly from vehicle manufacturers.*

Maurice Blackburn submits that the neutrality of the server which collects the data is vital. It also highlights the importance on ensuring that stated principles around data sharing (under what circumstances may the government seek to access that data) are clearly articulated.

Whilst we agree that appropriate incentives may be necessary to encourage data to be shared, as discussed in section 3.7.2 of the Discussion Paper, we also believe that *disincentives* must also be managed. As mentioned earlier, the key disincentives surround privacy, the unintended use or misuse of data, and failure to seek informed consent for data to be shared.

We strongly endorse the principles discussed in section 3.7.3:

> *….for research and planning purposes de-identified data and aggregated data should be used. Information derived from telematics data must only be accessed for*

the purposes for which it is collected, and any data collected should also be clearly outlined unless a warrant is obtained.

We note the paragraph in section 4.3.2 that says:

Through our consultation in developing this discussion paper, we did not observe a desire from transport agencies to use data from vehicles for targeted, individual enforcement or surveillance purposes.

Whilst we are pleased that this has been the case to date, Maurice Blackburn considers it possible that this desire may change once the data is actually in place. The potential for overreach by government and the agencies is palpable.

Maurice Blackburn notes the appropriate uses for data outlined in sections 4.3.3 to 4.3.8 of the Discussion Paper. We further note that none of those uses requires the sharing of personalised data.

Question 10: Do you agree that road safety data should be considered the priority purpose for which we seek to exchange data with industry?

Yes.

We would go further and suggest that road safety should be *the only purpose*, for now. Only once the exchange of data in relation to road safety is embedded should we look to other priorities. Again, we repeat that there should be a clear focus on minimisation of data collection, particularly at this early stage.

We note the outcomes of research demonstrated in Figure 6 (page 76) of the Discussion Paper. We agree that all seven priorities listed in the figure are worthy priorities, but that none is more important than road safety and that none need be implemented immediately save for road safety.

We agree with the statement on page 77, that:

….we consider road safety could be the logical starting point for initial access arrangements to be made for data from the light vehicle industry.

Maurice Blackburn agrees with the reasons provided on page 77 for choosing road safety. We further note that this section goes on to say:

Only de-identified, technical data is required from the vehicle, which does not require the consent of users to collect and would be difficult to combine with other data to infer personal information from.

As mentioned earlier, it is important to collect the minimum data necessary to address an identified use. Where this can be done with de-identified data, then that should be prioritised.

Enforcement should <u>not</u> be the priority purpose for the exchange of data with government, and it should certainly not be a use that is implemented in the introductory stages. If data were to be utilised for enforcement purposes initially, this would very likely lead to a reduced update of the technology.

Maurice Blackburn is of the view that at least in the initial stages of rolling out this technology, the existing frameworks for gathering enforcement related information are sufficient.

Question 14: Do you agree with the analysis presented in Table 7? What other opportunities are there for vehicle-generated data, and why?

Maurice Blackburn agrees that the vehicle-generated data categorisation process in Table 7 describes an appropriate methodology for considering such data.

In terms of future directions for the work, we note section 6.6 which says:

> *At the conclusion of our workshops, we surveyed stakeholder sentiment on building an ongoing forum between industry and government to continue discussing data access. There was strong support across both industry and government participants to continue engagement. Further consultation may be required to determine the appropriate forum.*

We believe, however, that the voices of consumers and road users are currently missing in this process. Consideration of the impact of the decisions made in this process on consumers and road users is vital.

Maurice Blackburn urges the NTC to prioritise the further consultation mentioned in 6.6, and that consumers and road users be given equal status to government and industry in that process.

Question 16: Should road safety be adopted as the priority for developing use cases for government use of vehicle-generated data? If not, what other approach should Australia take?

Yes. We agree with NTC's decision to adopt road safety as the priority in developing use cases for government use of vehicle-generated data.

Question 18: Does the NTC's preferred approach (option 2) best address the problems we have identified? If not, what approach would better address these problems?

We note the three options put forward to improve government access to vehicle-generated data and establish standards and governance frameworks, being:

- Option 1: No change to existing framework and legislation
- Option 2: Government and industry data exchange partnership
- Option 3: Legislative reform

We agree that Option 1 is not a viable option, as it is clear that current arrangements do not address the identified problems.

We further note NTC's decision to select Option 2 as their preferred option.

We note that, according to section 7.3.2 of the Discussion Paper:

This option proposes creating a data exchange partnership between industry and government that will identify and develop use cases for the exchange of data between industry and government.

Whilst supporting the idea of the data exchange partnership, we reiterate:

i. The importance of ensuring that consumers and road users are given equal billing with other stakeholders in this partnership (this is currently missing in Figure 7), and
ii. The need for the development of clear principles underpinning the exchange of data.

Maurice Blackburn favours legislative reform (Option 3). We believe it will be necessary in order to:

i. Clarify consumer rights in relation to data ownership and use
ii. Minimise data collection and exchange, limited to only matters of public good
iii. Spell out the principles underpinning any exchange of data between industry and government
iv. Limit the uses of data by government (as per the COVID Tracing app)
v. Make the necessary references to existing privacy provisions.

We refer to section 7.3.4 of the Discussion Paper noting that the NTC does not prefer Option 3 for reasons including:

Without a clear understanding of the potential uses and benefits of vehicle-generated data, government will not be able to accurately legislate to capture all potential benefits

We agree that there is a current lack of understanding of the potential uses of this data and therefore the associated risks to privacy and consequential ramifications to consumers and the public. For this reason we are of the view that it is all the more important that legislative reform (i.e. Option 3) is implemented for suggested new uses so that proper care is taken to consider the ramifications for all parties, including consumers.

Legislative reform would also assist in improving the transparency and trustworthiness of the process for consumers. We note that legislative reform regarding the COVID Safe App resulted in clear communication to the public of the control they retained over their data and how the data would be handled. We suggest that a similar process is appropriate for vehicle generated data, particularly in the initial stages.

Maurice Blackburn also believes that legislation could set the terms for a pilot of a data exchange model, which involves consumers, road users, manufacturers and government.

As always, we appreciate the thorough and consultative process adopted by NTC for this project.

Should you wish to discuss anything in this submission in more detail, we would be pleased to make ourselves available to you. Please do not hesitate to make contact.

Yours faithfully,

Katie Minogue
Senior Associate
Maurice Blackburn Lawyers
(03) 9784 6155
KMinogue@mauriceblackburn.com.au

Tamara Wright
Associate
Maurice Blackburn Lawyers
(03) 8102 2160
TWright@mauriceblackburn.com.au