Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D20/8580

10 July 2020

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

By email only:
automatedvehicles@ntc.gov.au

Dear National Transport Commission

Submission in response to the *Government access to vehicle-generated data* discussion paper

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission in response to the National Transport Commission's (**NTC**) *Government access to vehicle-generated data* discussion paper (**the paper**).

OVIC is the primary regulator for information privacy, information security, and freedom of information in Victoria, administering the *Freedom of Information Act 1982* (Vic) and the *Privacy and Data Protection Act 2014* (**PDP Act**). My office has a strong interest in new and emerging technologies – such as automated vehicles – and their impact on individuals' privacy, and as Information Commissioner one of my functions under the PDP Act is to make public statements on such matters.

OVIC appreciates the opportunity to contribute once again to the NTC's automated vehicle reform program, specifically in respect of government access and use of vehicle-generated data. This submission is organised around some of the questions posed in the paper, and draws on themes that OVIC has previously raised in relation to automated vehicles, namely in an earlier submission to the NTC on its *Regulating government access to C-ITS and automated vehicle data* discussion paper (**previous submission**).[1]

Key points

OVIC welcomes the NTC's approach to highlighting privacy as an important component to support the safe commercial deployment and operation of automated vehicles in Australia, both in this paper and its automated vehicle reform program more broadly. As we noted in our previous submission, strong privacy protections can enhance and achieve business objectives, help encourage user uptake of automated vehicle technologies, and build public trust in governments' access and use of vehicle-generated data.

While government access and use of this data can reap many benefits, such as improved road safety and better informed transport policies and planning, a lack of appropriate privacy protections may impact on users' and industry's willingness to capture or provide vehicle-generated data to government agencies, a key challenge identified in the paper. OVIC therefore strongly supports robust governance frameworks and regulations informed by the privacy principles developed by the NTC, placing appropriate limitations on governments' collection and use of vehicle-generated data.

[1] OVIC's *Submission in response to Regulating government access to C-ITS and automated vehicle data discussion paper*, 22 November 2018, is available at https://ovic.vic.gov.au/wp-content/uploads/2018/11/Submission-to-National-Transport-Commission-Regulating-Government-Access-to-C-ITS-and-AV-Data.pdf.

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 discussed?

OVIC agrees with the opportunity statement outlined in the paper, that there is scope for stakeholder consultation on exchange and sharing of vehicle data to understand which vehicle-generated data can be used to support road safety in Australia, and what an appropriate framework might look like to support such an exchange.

Stakeholder consultation (that includes the broader public, along with industry and government) will play an important role in determining community expectations around what government access to vehicle-generated data should look like. A data access framework that aligns with community expectations will help to build public trust in government collection and use of this data, and may encourage users to opt-in or provide consent for government to access their vehicle-generated data, should consent be relied upon as the authority to permit the collection of vehicle-generated data from users (OVIC's views on consent are detailed below under Question 9).

OVIC also agrees with the three problem statements identified in the paper, in particular the lack of an appropriate framework to establish government access and use of vehicle-generated data. OVIC agrees that, as noted on page 63 of the paper, existing access frameworks are unlikely to be adequate to address the privacy challenges posed by automated vehicles and government access to vehicle-generated data.

These challenges include the breadth of purposes for which government could potentially use such data which, without appropriate limitations in place, could lead to increased risk of scope creep. Another challenge is the growing potential for entities to undertake data linkage activities from which personal information could potentially be inferred, even from de-identified or aggregated data, facilitated by greater availability of and access to datasets, and increased technical ability, such as through the use of artificial intelligence (**AI**).

The absence of appropriate privacy protections around government access and use of vehicle-generated data may also be a contributing factor to industry and user unwillingness to provide such data to government, as covered under the first problem statement.

Question 6: Is there value in establishing a national data aggregator or trust broker? Could good data definitions, practices and cooperation between entities achieve the same outcome?

Establishing a national data aggregator may help address some of the challenges to government access to vehicle-generated data identified in the paper. For example, the paper notes that transport agencies have limited capability to ingest and derive meaningful insights from data. In this instance, a national data aggregator with the appropriate capabilities may be of value to transport agencies, reducing the need for such agencies to improve their own analytics capabilities, and saving them from the costs associated with doing so.

In the Victorian context, for example, the Victorian Centre for Data Insights (**VCDI**) is a centre of expertise that works with departments and agencies across the Victorian public sector (**VPS**) to bring together data for sharing, analysis, and insights. In addition to its analytics and insights services, the VCDI also offers strategic services and advice to support the development of organisations' data strategies, as well as training to help organisations build capability within their workforce. The VCDI operates under the *Victorian Data Sharing Act 2017*, following strict rules around data sharing, privacy and security to help build community trust. A national data aggregator in the context of government access to vehicle-generated data could play a similar role, facilitating the sharing of vehicle-generated data between entities, and providing analytics and insights services to agencies that may not have the capability to conduct analytics themselves.

Another key challenge noted in the paper is maintaining user privacy and data protection in many of the use cases identified. The paper further notes that there are greater privacy concerns when government collects raw data compared to government accessing processed information or aggregated reports. This is likely due to the potential to infer personal information from raw data and subsequently use that personal information for purposes far beyond the purpose of collection.

Establishing a national data aggregator may address this challenge by ensuring that data is only used for the purposes for which it was collected, through implementing and regulating effective access controls aimed at limiting the use of data to that which is reasonable and necessary.

Question 9: Have we accurately described the key barriers to accessing vehicle-generated data? Are there additional barriers?

Security

Closely related to the privacy challenges of government access to vehicle-generated data is the security aspect. Security is becoming significantly more pertinent as the risk of cyberattacks increases with the growing use of automated vehicles, as noted in the paper. In considering access to vehicle-generated data, the security of that data held by government must also be ensured.

As noted in OVIC's previous submission, given that government regularly enters into agreements and partnerships with private operators, a consistent security standard should apply to both public and private entities holding vehicle-generated data. In Victoria, for example, the Victorian Protective Data Security Framework (**VPDSF**) and associated Standards apply to private sector providers or operators acting under a State contract to the Victorian government.[2] A framework for government access to vehicle-generated data could include a similar security standard that applies to entities collecting, using, and sharing such data.

Privacy

It is possible to have a completely secure system that nevertheless does not respect privacy, so security is only one aspect of the challenges to the more widespread use of vehicle-generated data. OVIC agrees that ensuring user privacy is one of the greatest challenges to government accessing vehicle-generated data, however OVIC is of the view that privacy should not be seen as a barrier to access. OVIC considers that maintaining user privacy should instead be seen as an enabler to facilitating government access to vehicle-generated data – as noted above, strong privacy protections may encourage users and industry to capture vehicle-generated data, as well as provide access to such data to government. Governments may not garner necessary support in the community for the introduction of important new systems If people feel that their privacy may be infringed.

De-identified or aggregated data

The paper indicates that there may be industry willingness to capture certain types of identifying vehicle-generated data, provided users are de-identified or the data is aggregated (on page 97). The paper also gives examples of entities providing aggregated or de-identified data to transport agencies – for example, removing personally identifiable information such as a vehicle identification number from a dataset, before providing the data to a transport agency.

[2] Further information on the VPDSF is available on the OVIC website at https://ovic.vic.gov.au/data-protection/framework-vpdsf/.

While OVIC supports the use of de-identified or aggregated data over data containing identifiable information about individuals, it is crucial that entities sharing de-identified vehicle-generated data – and similarly, governments collecting such data – are mindful of the limitations of de-identification and the risk of re-identification.[3]

This risk of re-identification is particularly heightened where unit-record level information is involved. Entities sharing, collecting, and using de-identified unit-record level vehicle-generated data should accordingly ensure that appropriate governance processes and adequate privacy and security measures are in place to manage the risks arising from the use (particularly downstream use) of de-identified or aggregated vehicle-generated data.

Consent

OVIC welcomes the 'guest-centric' approach, noted on page 66 of the paper, of industry participants requesting consent from vehicle users for the collection of their data for transport agency purposes. The paper further notes that consent to collect data may be based on the use of a connected vehicle service, or the specific purposes for which the data is collected.

While consent offers users control over their information and who it is shared with, this approach can also be problematic, as OVIC raised in our previous submission. For example, in order to be meaningful, consent needs to be voluntary – which would likely not be the case if use of a connected vehicle service was contingent on users having no choice but to provide access to the data generated by the vehicle.

Another relevant element of consent is that it must be informed. This includes the user knowing all the different purposes to which the vehicle-generated data may be put. As acknowledged in the paper, the nascent nature of the automated vehicle industry makes it difficult, if not impossible, to foresee the full of extent of government access to vehicle-generated data, beyond that already identified in the paper. The possible use of big data and emerging technologies (such as artificial intelligence) to process vehicle-generated data, coupled with the growing generation and availability of other data sets with which vehicle-generated data may be combined, further add to this challenge. As such, informing users of what their data may be used for in order to obtain informed consent will likely not be feasible, or challenging at the very least.

In light of the challenges of obtaining meaningful consent from users, either to collect their vehicle-generated data or to share such data with government, OVIC suggests that governments ensure they have the legislative authority to collect vehicle-generated data, rather than relying on users' consent. However, notice should still be provided – users still need to be informed of matters such as why their data is being collected and under what authority, the purposes for which it will be used and with whom it will be shared, and who is able to access that data. Being transparent about the collection and use of users' vehicle-generated data is essential, regardless of whether or not consent is sought, will help to build public trust in government access to vehicle-generated data.

Q18: Does the NTC's preferred approach (option 2) best address the problems we have identified? If not, what approach would better address these problems?

OVIC supports the NTC's preferred approach of Option 2, which proposes creating a data exchange partnership between industry and government to identify and develop use cases for the exchange of vehicle-generated data. Given the deployment and adoption of automated vehicles in Australia is still in the early stages, identifying use cases and benefits from vehicle-generated data is an important first step to

[3] Further information about the limitations of de-identification can be found in OVIC's report *Protecting unit-record level personal information*, May 2018, available at https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf.

establishing a framework – including future legislative reform – for the safe and appropriate sharing of vehicle-generated data.

However, such a data exchange partnership must ensure that there are adequate privacy protections for users. For example, the paper notes that Option 2 could include the development of a shared vision and principles.[4] These could include the privacy principles previously developed by the NTC in an earlier discussion paper, *Regulating government access to C-ITS and automated vehicle data*.

OVIC also welcomes principles that could include, as noted in the paper, principles for achieving national consistency (which should also encompass security standards), and in particular, minimising the amount of data needed to achieve an outcome. This latter principle is similar to the collection minimisation principle, a key tenet of many privacy laws including the PDP Act.

In line with the collection minimisation principle, government access to vehicle-generated data should be limited to what is necessary to fulfil a particular activity or purpose, rather than collecting as much data as possible simply because it is available, or because it may be useful in the future.

Thank you for the opportunity to comment on the discussion paper. OVIC will continue to follow the progress of the NTC's automated vehicle reform program with interest.

I have no objection to this submission being published by the NTC without further reference to me. I also propose to publish a copy of this submission on the OVIC website, but would be happy to adjust the timing of this to allow the NTC to collate and publish submissions proactively.

If you would like to discuss this submission, please do not hesitate to contact me directly or my colleague Tricia Asibal, Senior Policy Officer at tricia.asibal@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner

[4] On page 85.