Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D22/19059

30 August 2022

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

Dear National Transport Commission

Submission in response to the *On-road enforcement for automated vehicles* 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**) *On-road enforcement for automated vehicles* discussion paper (**the discussion paper**).

OVIC is the primary regulator for information privacy, information security and freedom of information in Victoria, administering the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). 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 this further opportunity to contribute to the NTC's automated vehicle reform program, specifically in respect of law enforcement interaction with automated vehicles on the road. This submission is organised around some of the topics and questions posed in Chapters 4 -7 of the discussion paper.

General comments

OVIC is pleased to see the NTC's design principles for government access to cooperative intelligent transport systems (**C-ITS**) and automated vehicle data[1] (**the design principles**) included in the discussion paper. The design principles highlight privacy as an important component to support the safe and commercial deployment and operation of automated vehicles in Australia. To that end, OVIC strongly recommends that any legislation, governance frameworks and regulations, relating to powers for law enforcement to access, use and share automated vehicle data, be informed by the design principles.

OVIC supports the NTC's proposal that a Privacy Impact Assessment (**PIA**)[2] be required before introducing new powers for law enforcement in relation to the access, use and disclosure of automated vehicle data to assist in addressing any privacy risks that would be raised by the new power. Additionally, to ensure that privacy risks are considered and managed over time, OVIC recommends that any PIAs be reviewed periodically and updated where necessary.

[1] See the Appendix on page 80 of the discussion paper.
[2] For further information on Privacy Impact Assessments, see OVIC's Privacy Impact Assessment guidance at: https://ovic.vic.gov.au/privacy/privacy-officer-toolkit/privacy-impact-assessments/.

Proposed scope of access to automated vehicle data

OVIC acknowledges the need for law enforcement to access automated vehicle data in order to respond to the road safety risks of automated vehicles. However, OVIC strongly recommends the scope of law enforcement powers to access automated vehicle data be appropriately limited to only what is necessary for them to fulfil their functions in relation to the on-road enforcement of automated vehicles.

OVIC is concerned by law enforcement's desire to obtain 'unconstrained access to automated vehicle data',[3] as it suggests that law enforcement would seek the power to collect, use and disclose all types of automated vehicle data.

In addition, when referring to the types of automated vehicle data that law enforcement may need or should have access to, the discussion paper uses quite broad terms in some instances. For example, the discussion paper states that law enforcement will need access to automated driving system (**ADS**) operational data, which includes 'relevant data following a crash'.[4] However, the discussion paper does not outline what kinds of information the phrase 'relevant data' would include. OVIC considers this to present a risk of scope creep, whereby law enforcement may collect automated vehicle data they deem relevant, but which may not be strictly necessary to fulfil their functions of addressing the road safety risks of automated vehicles.

OVIC notes that if the types of data law enforcement would have access to are not clearly defined, they may allow for broad, if not unconstrained, collection of automated vehicle data. This would inevitably result in the overcollection of data, including personal information, beyond that which is needed to fulfil their functions and constitute an unjustified invasion of privacy.

OVIC's recent experience is that, unless specifically limited, law enforcement bodies may seek data collected for one purpose for prosecution of crimes in unrelated domains. While there may be a public interest in the use of such data for prosecution of serious crimes, it is OVIC's view that such requests for data should be subject to independent oversight, because such oversight acts as a safeguard for individuals' privacy and is important for the preservation of public trust.

OVIC strongly considers that the types of automated vehicle data, to which existing or new law enforcement powers would allow access, must be clearly defined and appropriately limited to only what is necessary for them to fulfil their functions in relation to on-road enforcement of automated vehicles.

Storage of automated vehicle data

The discussion paper stated that the storage location for automated vehicle data would likely differ between fleet-managed and privately owned vehicles, with the former desiring cloud storage and the latter likely being onboard storage.[5]

OVIC understands that cloud storage may be more convenient for automated driving system entities (**ADSE**) with fleet-managed automated vehicles by storing data from all fleet-managed vehicles in the one store. However, OVIC notes that cloud storage of automated vehicle data poses a privacy risk, particularly where personal information is involved.

For example, cloud storage providers may store and process information in an overseas location, subject to privacy legislation that does not require the same level of privacy protection as the PDP Act or the privacy legislation of other Australian jurisdictions. In such circumstances, there is likely an increased risk of data

[3] See page 46 of the discussion paper at 4.2
[4] See page 45 of the discussion paper at 4.1.
[5] See pages 47 – 48 of the discussion paper.

breaches occurring, as the cloud service provider may not provide sufficient information security measures to protect the automated vehicle data it is storing.

While there are cybersecurity risks to storing vehicle data in the cloud there are also security risks related to onboard storage within the physical body of the vehicle. There are very few instances in which an automated vehicle may be considered to be "offline" and therefore vehicle-specific attacks may also be anticipated.

OVIC notes that there is evidence of incentives for bad actors to exploit either cloud or local data and effective oversight of either cloud or local data handling is therefore important. Modern vehicles, even non-automated ones, contain a great deal of data that can be used to infer the behaviour and activities of drivers and their passengers, and this data is often held by local service centres or third parties with access to the vehicle application programming interface (**API**). Individuals handling data in those contexts are unlikely to have been extensively trained in how to handle and protect personal information. There is also evidence that the software development governance of vehicle manufacturers – even experienced ones – is not always sufficiently secure.[6]

Those risks aside, OVIC recommends that automated vehicle data be stored onboard for all automated vehicles because it would:

- reduce the privacy risks associated with cloud storage of information, in the sense that exposure of the data relating to one vehicle is likely to be less damaging than the exposure of the data related to the movement and operation of millions of vehicles and their passengers[7];
- provide a consistent approach to the storage of automated vehicle data regardless of the type of owner; and
- ensure law enforcement can efficiently determine how to access the vehicle generated data needed at the roadside.

That said, OVIC notes the types and level of automated vehicle data that law enforcement could access from onboard storage should be restricted. Without restrictions, providing roadside access to such data through a standardised port would effectively allow law enforcement to access all automated vehicle data in the onboard storage.

Due to the sheer volume and variety of data that automated vehicles generate and store, along with that data likely amounting to personal and sensitive information,[8] providing unrestricted access to all onboard data storage would increase the risk of law enforcement collecting data beyond its remit and breaching individuals' privacy.

OVIC recommends introducing a requirement that security protocols be put in place to ensure that, when law enforcement access onboard data of automated vehicles, they can only access the types of data they require and are authorised to access.

In-vehicle cameras

OVIC understands the NTC proposes a power to provide law enforcement with access to in-vehicle camera data 'for the purpose of enforcing fallback-ready user obligations including, but not limited to, determining

[6] https://www.zdnet.com/article/mercedes-benz-onboard-logic-unit-olu-source-code-leaks-online/.

[7] The damage to an individual may nevertheless be substantial and operators or manufacturers of automated vehicles should bear some responsibility for the impact to any individual's privacy rights.

[8] As noted in OVIC's *Submission in response to Regulating government access to C-ITS and automated vehicle data discussion paper*, 22 November 2018, the NTC recognised that C-ITS and automated vehicle data would likely amount to personal information due to the ability to match such data with other datasets to identify an individual. OVIC's submission 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.

whether a person is a driver or fallback ready user and whether the fallback-ready user took back control within a reasonable time.'[9] The NTC also proposes that such access should be restricted to these purposes unless the data can be accessed through other specific processes such as a warrant or court order.[10]

However, the discussion paper has also stated that there are no requirements for automated vehicles to have in-vehicle cameras and the abovementioned purposes could be achieved through alternative means such as accessing information generated from relevant sensors.

While both in-vehicle cameras and relevant sensors effectively fulfil surveillance functions by monitoring the alertness and movements of individuals within the automated vehicle, in-vehicle cameras are more privacy invasive. In-vehicle cameras not only collect information about an individual's alertness and movement, but they also unnecessarily collect information about the individual's physical appearance, from which they can be identified (i.e., personal information).

OVIC strongly recommends that law enforcement is not provided with a power to access in-vehicle camera data on the basis that:

- this data will be personal information due to it involving video footage that can identify an individual; and
- the purposes for which law enforcement seek to access this data could be reasonably achieved in a more privacy enhancing method, being through sensors that do not involve video surveillance of the individual.

Retention of automated vehicle data

While the discussion paper does not include a question relating to data retention, OVIC understands there is currently no consensus on what the retention period should be for automated vehicle data. Some providers, such as Tesla, have access to real-time or near-real-time data. They are likely to make the argument that this is necessary for product improvement, however this does not mean that the owners or occupants of such vehicles should surrender their human right to privacy and some safeguards are necessary.

OVIC recommends that a retention period be required for any automated vehicle data, particularly personal information, collected and held by law enforcement, as there are privacy risks associated with retaining personal information when it is no longer needed for its primary purpose. For example, such retention increases the possibility of personal information being used for a purpose other than the purpose for which it was collected, along with the possibility of the information being subject to a data breach.

Introducing a retention period would assist in balancing the protection of individuals' privacy with the need for law enforcement to use automated vehicle data to fulfil their functions relating to the on-road enforcement of automated vehicles.

Data sharing

OVIC recognises the need for law enforcement to undertake data sharing activities in relation to fulfilling reporting obligations to the in-service regulator and investigating an incident where an ADSE has been nominated as 'at fault'.[11]

In principle, OVIC supports the NTC's proposal that the types of data and purposes for which law enforcement could share that data with the in-service regulator should be outlined in a new power for law enforcement to share data with the in-service regulator. However, there are concerns with the details of

[9] See page 64 of the discussion paper at 6.2.3.
[10] Ibid.
[11] See pages 70 to 73 of the discussion paper.

the types of data the NTC proposes law enforcement could share with the in-service regulator. For example, the NTC states the types of data could include ADS operational data which, as noted earlier in this submission, includes 'relevant data following a crash' and may therefore enable disclosure of any data following a crash that law enforcement deems relevant regardless of necessity.

OVIC is similarly concerned about the NTC's proposal to allow law enforcement to disclose 'relevant data and information'[12] to ADSEs, particularly given it provides no restrictions around the purposes for which automated vehicle data can be disclosed to ADSEs.

To ensure that data sharing with the in-service regulator and ADSEs is conducted in a privacy enhancing way, OVIC recommends that:

- data sharing be limited to where it is necessary for law enforcement to fulfill their functions strictly in relation to enforcement of automated vehicles;
- the specific purposes for which it is necessary for law enforcement to share automated vehicle data be expressly outlined, either in legislation or in an information sharing agreement with the in-service regulator and ADSEs;
- requests by law enforcement for access to automated vehicle data for other purposes should require a warrant, to ensure proper oversight of the handling and disposal of data;
- the in-service regulator and ADSEs be required to maintain the same information security standards required of law enforcement under the PDP Act, to ensure the security of the automated vehicle data;[13]
- a PIA be completed before law enforcement enter into any information sharing agreement or introduce new data sharing powers; and
- any information sharing agreements between law enforcement and the in-service regulator and ADSEs are regularly audited to ensure that personal information is being handled in accordance with the PDP Act and to address any privacy risks that develop over time.

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.

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

Yours sincerely

Sven Bluemmel
Information Commissioner

[12] See page 73 of the discussion paper at 7.2.3.
[13] For further information on the security standards required under the PDP Act, see the Victorian Protective Data Security Standards (**VPDSS**) and Victorian Protective Data Security Framework (**VPDSF**), both of which are available on OVIC's website at https://ovic.vic.gov.au/data-protection/information-security-resources/.