information and privacy commission
new south wales

Enquiries: Sarah Wyatt
Telephone: 1800 472 679
Our reference: IPC18/A000561

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

Submitted by email only to: htsirlina@ntc.gov.au

Dear Sir/Madam,

Regulating Government Access to C-ITS and Automated Vehicle Data

The purpose of this correspondence is to provide a submission to the National Transport Commission on its Discussion Paper on Regulating Government Access to C-ITS and Automated Vehicle Data. The following comments are provided for consideration.

Privacy legislation and personal information

Our comments consider the impact of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act) on issues discussed in the paper, and broader issues of a privacy context. Our comments are confined to the PPIP Act and HRIP Act and do not specifically consider the obligations and impact of the Commonwealth *Privacy Act 1998* on Commonwealth government agencies and private sector organisations. However, we note that regulation from a privacy perspective of private sector entities is a critical consideration in respect of addressing privacy challenges arising from automated vehicles and C-ITS technology.

The discussion paper speaks of personal information as defined in the Commonwealth *Privacy Act 1998*. However, we note the comment in the discussion paper that definitions of personal information are similar across all Australian jurisdictions. As such, although we have mostly considered the discussion paper in the context of the NSW legislation, we acknowledge that the principles are analogous to those across all Australian jurisdictions, and that the concerns are comparable.

Application of the PPIP Act

The PPIP Act outlines how NSW public sector agencies manage personal information. Agencies that are bound by the PPIP Act are NSW public sector agencies, statutory authorities, universities, NSW local councils, and other bodies whose accounts are subject to the Auditor General. The HRIP Act applies to organisations (NSW public sector agencies or a private sector persons) that are health service providers or that collect, hold or use health information. The broader application of the privacy implications of C-ITS and automated vehicle technology will therefore likely fall to the Commonwealth, particularly for non-government bodies.

The impact of the PPIP Act on C-ITS and automated vehicle data

Under the PPIP Act, NSW government agencies are required to comply with information protection principles (IPPs) unless they are exempted from compliance under legislation or under privacy codes or directions. The IPPs cover the collection, use and disclosure of personal information.

The PPIP Act contains exemptions to the IPPs. In relation to information collected by C-ITS and automated vehicles, the following exemptions may be applicable:

- An exemption for law enforcement and investigative agencies: sections 23 and 24 of the PPIP Act
- An exemption where compliance is lawfully authorised or required, or otherwise permitted under an Act or any other law: section 25 of the PPIP Act
- An exemption relating to information exchanges between public sector agencies to enable inquiries to be referred between agencies: section 27A of the PPIP Act.

Potential new privacy challenges

The discussion paper summarises three categories of the potential new privacy challenges. These are addressed below.

New information captured by automated vehicle technology

The discussion paper notes that one of the privacy challenges of C-ITS and automated vehicle technology is that of new information captured by automated vehicle technology. The paper notes that interior cameras in automated vehicles are likely to have the effect of continuous and widespread video recording, and that biometric data may also be collected. This could include health information or health-related information, for instance facial temperature, heart rate, breathing rate and glucose and biometric sensors could be used to recognise drivers and occupants to customise the driving experience. The Health Privacy Principles under the HRIP Act may operate in respect of the collection, use, disclosure and retention of such information.

While state government agencies may not necessarily have direct access to this information and data, it is conceivable that law enforcement, transport or regulatory agencies may seek access. In such instances, the agencies would need to ensure that they comply with the IPPs.

C-ITS technology may allow for more widespread direct collection of location information by government

The discussion paper notes that data generated by C-ITS technology (such as vehicle speed, location and direction) may be collected by the government on a widespread basis. This could include information collected by government agencies from roadside collection devices stations.

Section 4 of the PPIP Act defines personal information as 'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.' This definition, like the Commonwealth *Privacy Act 1998*, ensures that electronic databases are covered by the legislative scheme.

Information and data collected by C-ITS technology could include personal information if, for example, the individual's identity is apparent and the data shows the individual's travel patterns. As such, any agency collecting, using or disclosing such information would need to comply with the PPIP Act. In *WL v Randwick City Council* [2007] NSWADTAP 58 the Appeal Panel said that information may be personal information even though extrinsic knowledge is necessary to identify an individual, where the recipient of the information can link the information to an individual. The issue of information being linked to an individual is also at the core of the Tribunal's consideration of the privacy implications of the NSW public transport Opal card in *Waters v Transport for NSW* [2018] NSWCATAD 40 and *Transport for NSW v Waters* [2018] NSWCATAP 200.

C-ITS and automated vehicle technology will generate a greater breadth and depth of information

The discussion paper notes that C-ITS and automated vehicle technology introduce new privacy challenges because more information is generated and stored, and there is an increased opportunity for data linking by government. The NTC has observed that data produced by C-ITS and automated vehicle technology will likely be personal information and sensitive information. This has implications for agencies in relation to storage, retention and security of information.

As noted above, any NSW agency that collects, uses or discloses the information would need to ensure that it complies with the PPIP Act.

Options for addressing privacy challenges for data generated by automated vehicle technology

The discussion paper identifies four options for addressing privacy challenges in respect of data generated by automated vehicles technology. These are:

- Option 1 – Rely on the existing information access framework to address the new privacy challenges of automated vehicle technology (no change)
- Option 2 – Agree broad principles on limiting government collection, use and disclosure of automated vehicle information
- Option 3 – Limit government collection, use and disclosure of automated vehicle information from in-cabin cameras and biometric, biological or health sensors to specific purposes

- Option 4 – Limit government collection, use and disclosure of all automated vehicle information to specific purposes.

Option 2 is identified in the discussion paper as the preferred option. This is because "it best addresses the identified challenges while ensuring that governments can appropriately use information from future vehicle technology to benefit the community."[1]

I note that Option 1 would not allow for anticipated and as yet unanticipated privacy challenges that may arise from data generated by automated vehicle technology. Option 2 provides flexibility in respect to the challenges and allows for further legislative reform identified as Options 3 and 4. In respect of the proposed options, I would like to continue to be consulted.

Options for addressing privacy challenges for data generated by C-ITS technology

The discussion paper identifies three options for addressing privacy challenges for data generated by C-ITS technology. These are:

- Option 1 – Rely on the existing information access framework to address the new privacy challenges of C-ITS technology (no change)

- Option 2 – Agree broad principles on limiting government collection, use and disclosure of C-ITS information

- Option 3 – Limit government collection, use and disclosure of all C-ITS information to specific purposes.

Again, option 2 is identified as the preferred option. I make the same observation about the options as noted above.

Option 2 – Principles

A single set of principles has been developed in the discussion paper for automated vehicles technology and C-ITS technology. As to the draft principles, I make the following comments:

1) The definitions in Principle 1 may include definitions for 'new information' referred to in the paper.

2) The regulatory framework described in Principle 3 should capture holding, retention and storage of information.

3) The legislative basis that would enforce the principles and any non-compliance should be thoroughly considered.

As noted above, I would like to be consulted as to the further development of Options and Principles to address the foreshadowed privacy challenges.

[1] Discussion paper, page 4.

Consent regarding surveillance devices

The discussion paper notes that express or implied consent is sufficient for the use of surveillance devices. This could include the installation, use and maintenance of data surveillance equipment or tracking devices.

The discussion paper also notes that it may be possible to imply consent of individuals for use of C-ITS devices, and that road agencies could possibly as individuals for express consent to use these devices through registration and licensing processes.

The UNSW report[2] referred to in the discussion paper discusses consent, stating:

> Consent may also be sought for a wide range of collections, uses or disclosures which are not essential to the provision of a particular service. In some circumstances, the subject may have little practical choice but to consent. For instance, the operators of various systems in the C-ITS or AV environment may insist on consent for a wide range of data uses as a condition for access to a vehicle's software. There may come to be limited alternatives, particularly for users who are unable to use alternative travel services, for example as a result of poverty or disability.[3]

There are circumstances where consent is said to be given, but such consent may not have been freely given. It is suggested that express consent of individuals is preferable, and that implied consent is not informed consent. This is demonstrated by the language used in the PPIP Act.

The authors of a 2016 Clayton Utz report[4] state that they expect that manufacturers will seek to obtain broad consents from purchasers or vehicles.

Broad consent, whether it is requested by manufacturer, insurers or government agencies, may be considered to be 'bundled consent'. This is a request for an individual to give general consent to a wide range of collections, uses and disclosures of their personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not. This may not meet the criteria for valid and informed consent, and reliance on such consent terms can be open to challenge. Also for consideration is the impact on individuals in instances where there is no choice but to consent, and what options there are for those who do not consent.

Currently, the IPC encourages members of the public to carefully read any Privacy Policy that they are provided with, and to ask for clarification if they do not understand

---

[2] Vaile D, Zalnieriute M and Bennet Moses L (2018) *The privacy and data protection regulatory framework for C-ITS and AV systems*, Sydney, UNSW.

[3] Ibid, 41.

[4] Clayton Utz (2016) *Driving into the future: regulating driverless vehicles in Australia*, Melbourne, Clayton Utz.

something. I support a model of consent in which individuals can select the uses or disclosures which are agreeable as distinct from a holistic request for consent. This approach supports the provision of informed consent.
I do not support the practice of bundling together or consolidating multiple requests for an individual's consent to a range or uses and disclosures of their personal information. Individuals should be given the option of indicating separately which use or disclosure they agree to.

Any collection, use or disclosure of personal information from data generated by automated vehicles and C-ITS should be done with express consent and not bundled consent. This applies to consent sought by government agencies and commercial entities such as insurers and vehicle manufacturers.

Contact details

I hope these comments will be of assistance. If you have any questions regarding these comments, please contact Sarah Wyatt, Assistant Director, Legal Counsel and Regulatory Advice on 1800 472 679 or by email at sarah.wyatt@ipc.nsw.gov.au.

Yours sincerely

Samantha Gavel
NSW Privacy Commissioner