THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

National Transport Commission Australia Regulating Government Access to C-ITS and Automated Vehicle Data Discussion Paper

November 2018

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

Contact: **Jennifer Windsor**
President, NSW Young Lawyers

Eva Lu
Publications Officer, NSW Young Lawyers Communications, Entertainment and Technology Law Committee

Editor: Eva Lu, Publications Officer
Contributors: Ravi Nayyar, Suzana Livaja

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000, DX 362 Sydney
ACN 000 000 699 ABN 98 696 304 966
T +61 2 9926 0182
F +61 2 9926 0282
E ylgeneral@lawsociety.com.au
W www.younglawyers.com.au

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

The NSW Young Lawyers Communications, Entertainment and Technology Law Committee makes the following submission in response to the National Transport Commission's Regulating Government Access to C-ITS and Automated Vehicle Data Discussion Paper.

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 15 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers (solicitors and barristers) under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The Communications, Entertainment and Technology Law Committee (**Committee**) of NSW Young Lawyers aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to information and communication technology (including technology affecting legal practice), intellectual property, advertising and consumer protection, confidential information and privacy, entertainment, and the media. As innovation inevitably challenges custom, the Committee promotes forward thinking, particularly about the shape of the law and the legal profession.

1. Introduction

The Communications, Entertainment and Technology Law Committee (**Committee**) of NSW Young Lawyers welcomes the opportunity to comment on the National Transport Commission's (**NTC's**) Regulating Government Access to C-ITS and Automated Vehicle Data Discussion Paper (**Discussion Paper**).

The Committee commends the NTC for recognising the privacy challenges of government access to information generated by both cooperative intelligent transport system (**C-ITS**) and automated vehicle technology (**Vehicle Technology Data**) and the need for reform to address these challenges.

To address the privacy challenges, the Discussion Paper presents 3 options with respect to C-ITS technology and 4 options with respect to automated vehicle technology. The NTC has outlined that its preferred option is option 2, to implement "broad principles reform" for both C-ITS and automated vehicle technology.

The Committee recognises to a limited extent the need for appropriate information sharing, so governments can use Vehicle Technology Data to inform and enhance government decision-making. It also agrees that it is necessary to balance the potential improved decision making and public value of access with sufficient privacy protection to C-ITS and automated vehicle (**New Technology Vehicle**) users.

However, the Committee submits that in the case of Vehicle Technology Data, the protection of individual privacy should outweigh the need for government access to such data. The Committee considers that the NTC has underestimated the potential impact of the serious invasions of privacy that could result from government access to Vehicle Technology Data due to the depth and breadth of data available from New Technology Vehicles. The Committee encourages the NTC to reconsider its proposed option.

For reasons outlined in this Submission, the Committee's preferred options (with further limitations) are:

- for automated vehicle technology – option 4 – limit government collection, use and disclosure of all automated vehicle information to specific purposes; and
- for C-ITS technology – option 3 – limit government collection, use and disclosure of all C-ITS information to specific parties and purposes.

The Committee considers it critical that every attempt should be made to protect the privacy of all individuals, whether they are New Technology Vehicle users, a passenger of a New Technology Vehicle or a pedestrian as this is in line with community expectations and Australia's obligations under international law.

2. Analysis of NTC's Preferred Option

The Committee agrees that Australia's incumbent information access framework for government is unable to address the privacy challenges of Vehicle Technology Data, and supports reform to address these privacy challenges. The NTC correctly highlights that significant privacy challenges stem particularly from the overwhelming breadth and depth of Vehicle Technology Data. This includes the ability for government to access such data if the disclosing entity reasonably believes the disclosure is reasonably necessary for law enforcement related activities.[1]

The NTC presents a single preferred option 2 involving agreeing on broad principles with respect to limiting government collection, use and disclosure of Vehicle Technology Data (**Broad Principles Option**). The NTC considers the Broad Principles Option "best addresses the identified challenges while ensuring that governments can appropriately use information from future vehicle technology to benefit the community. This approach would help guide further development of the regulatory framework for C-ITS and automated vehicle technologies, whilst providing a sufficient degree of flexibility as the technology develops."[2]

The Committee recognises the need for a flexible approach in the regulation of Vehicle Technologies Data. However, the Committee submits that the proposed Broad Principles Option is unacceptable for Vehicle Technologies Data as a proposal to restrict government collection, use and disclosure of Vehicle Technologies Data. These "Broad Principles" do not afford the appropriate level of consideration and protection of privacy considering the potential breadth and depth of person information comprised in Vehicle Technologies Data.

The Committee agrees with Vaile, Zalnieriute and Moses in that a large amount of Vehicle Technology Data can be personal information, and certain categories of it can be sensitive information (such as biometric information collected by an automated vehicle to identify occupants) under the *Privacy Act 1988* (Cth) (**Privacy Act**).[3] The amount and quality of the Vehicle Technology Data collected is also likely to dramatically increase with the advancement in the technology of automated vehicles and C-ITS. This is likely to include the development of additional and more accurate sensor input units and cameras. As a result, such information

[1] *Privacy Act 1988* (Cth) APP 6.2(e).
[2] National Transport Commission, 'Regulating Government Access to C-ITS and Automated Vehicle Data: Discussion Paper' (Report, National Transport Commission, September 2018) 4.
[3] David Vaile, Monika Zalnieriute and Lyria Bennett Moses, 'The Privacy and Data Protection Regulatory Framework for C-ITS and AV Systems: Report for the National Transport Commission' (Report, Allens Hub for Technology, Law & Innovation, 2 July 2018) 19-26.

needs to be afforded a higher level of protection than "broad principles" as any unauthorised use or disclosure of such information can have severe personal ramifications for the subject of that information.

The Broad Principles Option also ignores the reality of modern data analytics capabilities, particularly with respect to the aggregation of various sets of data in a way that links previously un-identifiable sets of data to an individual. The quality and accuracy of the insights gleaned from analysis of Vehicle Technology Data can be multiplied through aggregation of multiple datasets collected by New Technology Vehicles and the application of increasingly sophisticated (machine learning) algorithms to those datasets. As Vaile, Zalnieriute and Moses argue, "the more useful related information you have, and the more effective tools, the more identifiable a given data set becomes".[4] As such, there is a risk that data which may initially have been un-identifiable with reference to an individual would be outside the scope of the protections of the Privacy Act, and consent or notification to its use and disclosure would not have been obtained from that individual, exacerbating the risks to privacy of ordinary citizens using New Technology Vehicles.

Further, the Committee is of the view that a single set of principles is unable to address the privacy challenges that arise in this context. While it is recognised that data generated by each of C-ITS and automated vehicles technologies will present similar privacy challenges and that the data captured by each will likely be personal information and sensitive information, the risks and personal ramifications for the individuals who are the subject of such data and the types of information that can be derived from such technologies vary greatly. The Discussion Paper identifies that C-ITS technology is likely to produce data such as vehicle speed, location or direction through the use of various components of the transport network (vehicles, roads and infrastructure). On the other hand, automated vehicles use a number of cameras, sensors, radars, real-time maps and large quantities of data through specialised software. The type of data that could be produced by automated vehicles and the way that it could be linked to an individual are not yet known and as such their collection requires consideration through a more restrictive lens.

As such, while the same reform option for the collection of data from C-ITS and automated vehicle technologies is recommended by the NTC, the Committee supports the separation of the two. This will allow the development of distinct mechanisms for considering whether data sets collected from each should be used, shared or released.

Additionally, the Committee steadfastly values an individual's desire to protect their privacy, particularly in the digital age. Despite the lack of a recognised general right to privacy in Australia, the Committee stresses the recognition of the right to privacy as a fundamental human right in the Universal Declaration of Human Rights,

[4] Ibid 16.

the International Covenant on Civil and Political Rights and other international instruments and treaties to which Australia is a signatory. The Committee strongly submits that this right must not be unduly or otherwise illegally interfered with by any person, whether a state or non-state actor. Indeed, the Committee is especially concerned about the respect of this right in an age where immense amounts of personal information (let alone that which is Vehicle Technology Data)[5] being collected and used without individuals' consent and for purposes unknown to them on several occasions.

The Committee submits that the privacy concerns which arise in the context of Vehicle Technology Data outweigh the need for government access to such data until it can be reasonably ascertained how the use and disclosure of Vehicle Technology Data will impact on individuals and their privacy, given how revealing the insights yielded by analysis of Vehicle Technology Data can be, particularly sensitive information collected by biometric sensors and in-cabin cameras.

3. The Committee's Preferred Options

The Committee submits in favour of the more privacy protective reform options presented in the Discussion Paper, being:

- option 4 for automated vehicles – limit government collection, use and disclosure of all automated vehicle information to specific purposes; and
- option 3 for C-ITS – limit government collection, use and disclosure of all C-ITS information to specific parties and purposes.

The Committee notes that these options expressly presume Vehicle Technology Data to be personal information (and provide scope for certain categories of this data to be classified as sensitive information), thus automatically affording all Vehicle Technology Data the relevant protections under the Privacy Act without having to first prove that the relevant Vehicle Technology Data falls within the definition of personal information.

The Committee also submits that its preferred options identified above should be subject to additional limitations to ensure a privacy-centric approach with respect to Vehicle Technology Data, given the amount thereof collected on individuals and how revealing the insights gleaned from the data can be about those persons. The additional limitations are as follows:

[5] See, eg, Kathy Winter, *For Self-Driving Cars, There's Big Meaning behind One Big Number: 4 Terabytes* (14 April 2017) Intel Newsroom <https://newsroom.intel.com/editorials/self-driving-cars-big-meaning-behind-one-number-4-terabytes/>.

- Automated vehicle data can only be collected, used and disclosed for automated vehicle compliance and law enforcement purposes, which must be narrowly defined, reasonable and risk-based in terms of the necessity, and only as per a warrant or court order.
- C-ITS data can be collected, used and disclosed for C-ITS-specific compliance and law enforcement purposes which must be narrowly defined, reasonable and risk-based in terms of the necessity, and only as per a warrant or court order. C-ITS data can also be collected, used and disclosed by road agencies for network operations and strategic planning on an aggregated basis.

The Committee acknowledges that the need for a clear, reasonable and risk-based access regime in relation to Vehicle Technology Data is belied by the criminal usage of emergent technologies to plan, coordinate and execute criminal activity (including terrorist attacks). The Committee further acknowledges that the technological ingenuity of criminals is well-known[6] and automated vehicles, in particular, will increasingly be used by criminal actors.

In that vein, the Committee calls for the establishment of a lawful access regime in relation to Vehicle Technology Data for compliance and law enforcement purposes, under which only certain law enforcement agencies (**LEAs**) can get access to the data with a warrant or court order. Such a regime would override disclosures reasonably necessary for law enforcement related activities permitted under APP 6.2(e). This is consistent with the principle at international law that the right to privacy is not absolute but can be interfered with in a non-arbitrary and lawful fashion.[7]

The Committee submits the lawful access regime must be narrowly defined in terms of:

- the LEAs that can obtain access to the data; and
- the offences in relation to which those LEAs can seek access.

This is to ensure that the regime only applies to prosecute serious criminal and terrorist activity. The NTC may consider looking to the *Telecommunications (Interception and Access) Act 1979* (Cth) (**Interception and Access Act**) as an example. The LEAs that can obtain access to Vehicle Technology Data should be restricted

[6] Europol, 'European Union Serious and Organised Crime Threat Assessment: Crime in the Age of Technology' (Report, European Police Office, 2017) 24.
[7] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17(1); Department of Home Affairs, *Statement of Principles on Access to Evidence and Encryption* (September 2018) <https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption>.

to some of the 'criminal law enforcement agencies' defined in section 110A of the Interception and Access Act, but similarly, only if they have a court order or warrant. The offences in relation to which those LEAs can seek a warrant to access specific data could be limited to some of those defined as 'serious offences' in section 5D of the Interception and Access Act. However, the Committee does not consider that all 'criminal law enforcement agencies' and 'serious offences' as defined in the Interception and Access Act would be appropriate for Vehicle Technology Data and strongly recommends the NTC conduct further consultation on suitable definitions of LEAs and offences for compliance and law enforcement purposes specific to Vehicle Technology Data.

4. Additional Considerations

The Committee also recommends that the development and consideration of government access to Vehicle Technology Data should not occur in isolation to other data sharing and access regimes. For example, consideration should be given to the national facial biometric matching regime being considered in a number of jurisdictions across Australia, and the proposal by the Department of Prime Minister and Cabinet to introduce Australian Government Data Sharing and Release legislation. The Committee considers that any Vehicle Technology Data should be expressly excluded from such legislation until there is greater clarity with respect to the types of data that will encompass Vehicle Technology Data. Following this, careful consideration can be given as to the objectives, risks and benefits of the inclusion of Vehicle Technology Data within the ambit of such legislations.

5. Concluding Comments

NSW Young Lawyers and the Committee thank you for the opportunity to make this submission. The Committee strongly encourages the NTC to reconsider its preferred option for reasons outlined in this Submission and would appreciate further consultation on the NTC's recommendations to the Transport and Infrastructure Council.

Please note that the views and opinions expressed in this submission are on behalf of the Committee and its contributors and do not reflect the views or opinions of any employer or company related to the contributors.

If you have any queries or require further submissions, please contact the undersigned at your convenience.

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Contact:

Jennifer Windsor
President
NSW Young Lawyers

Email: president@younglawyers.com.au

Alternate Contact:

Eva Lu
Publications Officer, NSW Young Lawyers
Communications, Entertainment and Technology Law Committee

Email: cet.chair@younglawyers.com.au