



THE LAW SOCIETY
OF NEW SOUTH WALES

Our Ref: PDL:DHin1617180

29 November 2018

Dr Geoff Allan
A/Chief Executive Officer
National Transport Commission
Level 3/600 Bourke Street
Melbourne VIC 3000

By email: enquiries@ntc.gov.au

Dear Dr Allan,

Regulating government access to C-ITS and automated vehicle data

Thank you for the opportunity to provide comments in relation to the National Transport Commission's ("NTC") discussion paper *Regulating government access to C-ITS and automated vehicle data*. The Law Society's Privacy and Data Law Committee has contributed to this letter.

The Law Society acknowledges that digital technologies that constitute Intelligent Transport Systems ("ITS") are rapidly developing and have been promoted for the potential benefits they offer in relation to economic efficiency, relieving transport congestion, reducing pollution and increasing public safety.¹ However, these potential benefits must be balanced against the risks that ITS present to individuals' privacy, particularly when information produced by ITS is collected and used by government.

The Law Society commends the NTC² and University of NSW ("UNSW") researchers³ for their methodological rigour and comprehensive analysis of the potential new privacy challenges of government access to information generated by ITS, specifically two types of ITS: automated vehicle technology and Cooperative Intelligent Transport Systems ("C-ITS"). We agree with your remarks that 'government access to the type, breadth and depth of personal or sensitive

¹ ITS Australia, *Smart Transport for Australia Report*, p8 <<https://www.its-australia.com.au/wp-content/uploads/Smart-Transport-for-Australia.pdf>> (accessed 18 November 2018).

² National Transport Commission, *Regulating Government Access to C-ITS and Automated Vehicle Data – Discussion Paper*, September 2018 <[https://www.ntc.gov.au/Media/Reports/\(614D48BA-F48B-38C8-FA90-A103E49A38CF\).pdf](https://www.ntc.gov.au/Media/Reports/(614D48BA-F48B-38C8-FA90-A103E49A38CF).pdf)> (accessed 18 November 2018).

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* (UNSW, Sydney, 2 July 2018) <[https://www.ntc.gov.au/Media/Reports/\(A4689742-E776-D8B3-1837-C4F6F3969B2E\).pdf](https://www.ntc.gov.au/Media/Reports/(A4689742-E776-D8B3-1837-C4F6F3969B2E).pdf)> (accessed 18 November 2018).

information generated by C-ITS and automated vehicle technology presents a privacy challenge.⁴ Our view is that the current privacy legislative framework is not advanced enough to deal with the challenges to privacy presented by developments in automated vehicle technology and C-ITS. In particular, Australia's current information access framework applying to government collection and use of information may not be robust enough to protect privacy amidst (a) the rapid developments in transport technology/ITS that challenge privacy and (b) the desire to maintain an openness to future technological developments. In the context of the present consultation, the Law Society considers that the fundamental overarching policy concern is striking an appropriate balance between government power to collect, store and access data and providing sufficient privacy protections for users of automated vehicles and C-ITS.

Taking as its frame of reference the Options proposed by the NTC's Discussion Paper, the Law Society agrees that reform is preferable to no change, but disagrees with the NTC's preliminary preferred 'broad principles' of Option 2. The Law Society considers that, with respect to addressing the new privacy challenges of automated vehicle technology, Option 4 is the preferable option. With respect to addressing the new privacy challenges of C-ITS technology, Option 3 is the preferred option. Both Options favour limiting government collection, use and disclosure of information to specific purposes and, in the case of C-ITS, also to specific parties. These Options are preferred because they are the more privacy-protective of the proposed Options, while allowing the flexibility to consider specific government activities that require collection of information as legitimate needs arise.

Privacy challenges

The Australian framework of privacy laws is comprehensively set out by the UNSW report. We briefly note some of its key features here for context. The concept of privacy plays an important role in the relationship between persons and governments and has the status of a fundamental human right.⁵ In an era where the collection, storage and application of information about individuals is integral to the work of government and is facilitated by technological developments, the human rights dimension of privacy is paramount to considerations of legislative reforms that could impinge on individuals' privacy.

Australia's international legal obligations to protect individuals' privacy are set out in Article 17 of the *International Covenant on Civil and Political Rights* ("ICCPR").⁶ The United Nations Human Rights Committee has interpreted the right to apply to 'gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies'.⁷ By way of further guidance, the Committee emphasises that:

In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may

⁴ Dr Geoff Allan, NTC Acting Chief Executive, cited in NTC Media Release "Tackling privacy challenges of government access to data from automated vehicles" dated 27 September 2018 < <https://www.ntc.gov.au/about-ntc/news/media-releases/tackling-privacy-challenges-of-government-access-to-data-from-automated-vehicles/> > (accessed 18 November 2018).

⁵ Article 12, *Universal Declaration of Human Rights* 1948.

⁶ Article 17, *International Covenant on Civil and Political Rights* 1966:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

⁷ United Nations Human Rights Committee, *General Comment No. 16 – Article 17*, 8 April 1988, at para. 10.

control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.⁸

The Law Society considers that the comments of the Human Rights Committee continue to be relevant to the discussion on regulating government access to automated vehicle data and C-ITS.

The Law Society agrees with the NTC's approach that, in order to appreciate the complexity of ITS, it may be useful when assessing privacy challenges and policy considerations to draw a distinction between two forms of ITS - automated vehicle technology and C-ITS – while also recognising there is an overlap between the two. The distinction allows for analysis of the different types of information generated by each system; consideration of the purpose for which information collection is proposed to serve and its implications for the privacy rights of individuals.

The NTC identifies three categories of privacy challenges presented by automated vehicle technology and C-ITS.⁹

These categorisations are useful in so far as they identify that privacy challenges will relate to type of information; method of information gathering; and breadth and depth of information collected. The Law Society finds this analysis to be of assistance but seeks to offer some additional comments on the privacy challenges that ITS, such as automated vehicle technology and C-ITS present.

The overarching challenge for the privacy law framework is one of keeping up with the demands and challenges of rapid advancements in technology and the expanded collection of personal information that it enables. While the development of privacy principles has been useful for attempts at establishing a coherent framework for the protection of privacy, each of these principles is to be tested as new privacy dilemmas arise.

Specifically, with respect to the privacy challenges presented by automated vehicle technology and C-ITS, the Law Society has concerns about:

- 1) Who is the subject of privacy protection and to what extent will they have privacy protection claims in the context of automated vehicle technology and C-ITS, considering that the information gathered will potentially encroach on the privacy of owners, passengers and members of the public external to the vehicle? Each of these potentially affected persons will have different levels of control over the collection of information that relates to them.
- 2) Whether information taken for a particular purpose could be used for other purposes for which an individual's consent has not been obtained and, as such, may undermine the notion of informed consent by individuals in relation to their personal information.
- 3) How data types generated from automated vehicle technology and C-ITS will be treated and therefore what legal implications will flow. The UNSW report sets out the issue in terms of the distinction between 'personal information' and 'sensitive information'. The former hinges on the 'degree to which an individual is 'readily identifiable'¹⁰ from the information, bearing in mind that identifiability will depend on factors such as context, who is doing the identification and from what sources the

⁸ Ibid.

⁹ NTC Discussion Paper p.3.

¹⁰ Note 3 above, p.12.

identification is made. The meaning of 'sensitive information' differs across jurisdictions but, in the Commonwealth *Privacy Act 1988* for example, it includes information or an opinion about an individual's race, ethnicity, political opinions, membership of political associations, religious beliefs or affiliation, sexual orientation, sexual practices, health information, genetic information and biometric information. The distinction is important because different types of information will attract different privacy obligations, risks and protections. Of importance also are attributes of a person that may be regarded as sensitive information but which are not specified in existing legislation as such. An example may be the emotional, cognitive and behavioural attributes that an automated vehicle can capture from its built-in health sensors.¹¹

- 4) Whether appropriate processes and safeguards will exist to collect and protect sensitive personal information and biometric data that is collected.
- 5) Uncertainty as to the precise purposes for which the collected data is authorised to be used, by whom and the extent to which the scope of the authorisation can be extended without the appropriate consent of the persons concerned or even parliamentary oversight.
- 6) Implications for the future considering that standards and consequences change over time. For example, what might be acceptable practices now may have implications for more wide-ranging surveillance in the future that trespasses on individual rights and liberties in unnecessary and disproportionate ways, constituting an arbitrary interference with the right to privacy under Article 17 of the *ICCPR*.

In consideration of these concerns, and those detailed in the UNSW research and the NTC Discussion Paper, the Law Society recommends that the starting point for reform and regulation of the information access framework be one that is the most privacy-protective. In its Guidelines, the Office of the Australian Information Commissioner ("OAIC") states that, as principles-based law, Australian Privacy Principle ("APP") entities are provided:

with the flexibility to tailor their personal information handling practices to their diverse needs and business models, and to the diverse needs of individuals. The APPs are also technology neutral, applying equally to paper-based and digital environments. This is intended to preserve their relevance and applicability, in a context of continually changing and emerging technologies.¹²

In other words, the APPs incorporate the concept of 'privacy by design'. This is the idea that the security of data and protection of privacy ought to be embedded within an agency's practices of data handling. The Law Society recommends that this approach guide selection of the preferred Options to address the privacy challenges presented by ITS.

Proposed Options to address privacy challenges

The NTC has proposed four Options to address privacy challenges of automated vehicle technology and three Options to address privacy challenges of C-ITS.

The NTC considers that, of the proposed Options, Option 2 is preferable in both cases, requiring the development of broad principles on limiting government collection, use and disclosure of information. The NTC's view is that because Option 2 subscribes to broad principles it 'best addresses the identified challenges while ensuring that governments can

¹¹ NTC Discussion paper p.28.

¹² Office of the Information Privacy Commissioner, *Australian Privacy Principles Guidelines*, 2015 <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines> (accessed 20 November 2018).

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.¹³ To this extent, Option 2 seeks to offer a framework that would potentially enable balancing investigations into the government's power to access data and consideration of privacy protection for users of automated vehicles.

The Law Society agrees that detail around the overall legislative framework for automated vehicle technology and C-ITS is required. Additionally, we agree that the potential applications and benefits arising from government access to data generated by automated vehicle technology and C-ITS is necessary.¹⁴ However, we do not consider that Option 2 goes far enough in either case in achieving these objectives. This is because it does not begin from a privacy-protective presumption, nor is the protection of individuals' data and privacy necessarily embedded within the broad principles approach.

If there is to be adoption of the new technology and consumer trust in it, the public needs to know what information government is collecting; how that information is being collected; for what purpose it is being collected and stored; where it is being stored and with what security over it; which agencies or entities have access to the information and what are the future implications. A broad principles approach entails a degree of uncertainty that may not instil enough public confidence in the information security and aspects of the technology at this point in time. A stronger statement acknowledging individuals' privacy protection and clarity around limitations on collection and use of information will more likely reassure the public and promote consumer take-up of the technologies and associated products.

In the case of automated vehicle technology, Option 3 goes further than Option 2 to achieve these ends in that it specifies the sources from which government collection of data will be limited (i.e. in-cabin cameras and biometric, biological or health sensors to specific purposes). However, the question remains, what is the status of sources of information collection that are not listed in this reform option? These would include dashboard cameras, external camera input units and V2V/V2I communication devices. A more widely encompassing statement of limitation as conveyed by Option 4's limitation of government collection, use and disclosure of *all* automated vehicle information to specific purposes (emphasis added) would address this concern.

By casting a wider net over the scope of information that is to be scrutinised, Option 4 permits a more rigorous framework than Options 2 and 3 for addressing the new privacy challenges of automated vehicle technology. Acknowledging, as the UNSW report does, that data can become sensitive depending on context,¹⁵ Option 4 is preferable because it can account for contextual variances. As such, it is more consistent than the other Options with taking a privacy-protective point of departure and an approach to reform that embeds privacy from the outset and throughout the lifecycle of the information collected rather than simply supplementing privacy considerations after the collection has occurred.

Our preference for Option 3 in the context of C-ITS relies on similar arguments. A notable difference, however, is that C-ITS Option 3, unlike automated vehicle technology Option 4, proposes the limitation of government collection of C-ITS information, use and disclosure to *specific parties* in addition to the limitation of government collection of C-ITS information, use and disclosure to specific purposes. This is an important consideration, yet it is not apparent why the same limitation does not apply in the case of automated vehicle technology. For the avoidance of doubt, we recommend that Option 4, in the context of automated vehicle

¹³ NTC Discussion Paper, p.4.

¹⁴ Ibid, p.64.

¹⁵ Note 3 above, p.1.

technology, be revised to limit government collection, use and disclosure of all C-ITS information to *specific parties* and purposes (emphasis added).

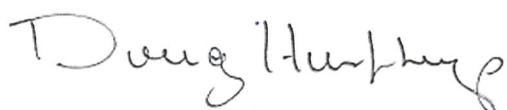
From a government access perspective, an expansive notion of limitations on government collection, use and disclosure of information may place additional accountability, transparency and scrutiny on the information gathering activities of government. However, accountability, transparency and scrutiny are features of a democratic system that upholds these principles and adherence to its international human rights obligations to protect privacy. Further, they are principles consistent with the current APPs. Reform Option 4 (automated vehicle technology) and Option 3 (C-ITS) are not inherently obstructive to governments' goals of increasing efficiency, managing the environmental effects of transport and increasing the safety of the travelling public. They have the potential to cultivate consistency in the Australian regulatory context by emphasising key Australian privacy principles and with the European General Data Protection Regulation ("GDPR") principles of 'privacy by design', 'privacy by default', 'data minimisation', 'data avoidance' and 'right to be forgotten / right to erasure'.¹⁶

Recommendations

The Law Society generally agrees with the NTC's draft principles for addressing the privacy challenges of government access to C-ITS and automated vehicle data.¹⁷ We consider the principles to be more conducive to support for Option 4 (automatic vehicle technology) and Option 3 (C-ITS) than reform Option 2. Further, we suggest that Principle 5 could be strengthened by including a proposal that the agencies or entities that have access to information be specified. Also developing guiding principles as to who has access to the information generated by the automated vehicle technology and C-ITS would be sensible and desirable. Additionally, the 'consent' referred to in Principle 7 ought to specify that it be 'informed consent' that is obtained from users and the 'opt out' option for users ought to be available at any point in time where practicable. We recommend that Principle 8 include oversight by the OAIC.

Thank you for considering this submission. Should you have any queries with regard to this submission, please contact Ida Nursoo, Policy Lawyer on 9926 0275 or email ida.nursoo@lawsociety.com.au

Yours sincerely,



Doug Humphreys OAM
President

¹⁶ NTC Discussion Paper, p.16.

¹⁷ Ibid, p.5.