SQUIRE PATTON BOGGS

SQUIRE PATTON BOGGS

Submission to the National Transport Commission: *on Regulating Government Access to C-ITS and Automated Vehicle Data*

November 2018

CONTENTS

1. Executive Summary

Thank you for the opportunity to share this response to the *Submission to the National Transport Commission on Regulating Government Access to C-ITS and Automated Vehicle Data.* **As a global leader in the legal and social aspects of driverless vehicles, Squire Patton Boggs wants to commend you and your colleagues for undertaking this vitally important initiative.**

These submissions have been prepared by the Data Privacy and Cybersecurity Practice of Squire Patton Boggs (AU). Squire Patton Boggs is a full-service global law firm providing insight at the point where law, business and government meet. The Data Privacy and Cybersecurity Practice team has substantial experience advising a broad client base, including domestic and international publicly listed companies, large privately owned companies, not-for-profits and small business. The team acts on the forefront of advancing regulatory measures in data privacy and cybersecurity and these submissions are part of an ongoing commitment to advise on and contribute towards best practice regulatory standards and compliance across the privacy and cybersecurity space in Australia.

1.2 Australia's current regulatory landscape for automated and connected vehicles, with respect to privacy, is inadequate:

(a) Australia's privacy statues do not operate uniformly across each Australian state, causing a fractured approach to regulation on a state-by-state basis and across the government/private-sector divide;

(b) State and Federal governments are likely to systematically collect sensitive information without consent in breach of current privacy regulations due to the fluid nature of the information revealed by automated and connected vehicle data;

(c) legislative reform is necessary to ensure compliance with or exclusion of the application of state surveillance laws;

(d) current privacy exceptions for law enforcement activities are too broad and may promote general or mass surveillance of automated and connected vehicle users because of the amount and type of automated and connected vehicle data;

(e) requirements to destroy or de-identify automated and connected vehicles imposed on governments do not uniformly apply and, where they do, are inadequate; and

(f) cybersecurity and data management requirements imposed on government agencies do not adequately protect the collected automated and connected vehicle data held.

1.3 We submit that reforms based on the following principles will go some way to address the inadequacies outlined above:

(a) automated and connected vehicle information is personal information;

(b) a national regulatory framework supporting lawful access, use and disclosure of automated and connected vehicle information;

(c) the proposed national framework should be founded in the Australian Privacy Principles (**APP**) established by the *Privacy Act 1988* (Cth) (**Privacy Act**)

incorporating additional privacy limitations is necessary to maintain individual privacy;

(d) specific data types that are particularly sensitive should be defined as sensitive and subject to additional limitations. These include collection, use and disclosure (which would limit government entities to only using that information for automated vehicle compliance and enforcement, unless a warrant or court order was obtained to allow alternative uses, such as general law enforcement or surveillance);

(e) any proposed protections should be legislative;

(f) any proposed protections will need to specify the data covered, the purposed for which it can be used and which parties specific limitations apply;

(g) proposed privacy protections should cover additional elements, such as destruction and notification, to address other identified gaps; and

(h) heightened best practice standards of cyber security and data management should apply to government entities when dealing in automated and connected vehicle data.

Yours sincerely

Margie Tannock
Partner & Head of Public Policy, Australia
Squire Patton Boggs

+61 8 9429 7456
margie.tannock@squirepb.com

2 Threshold Issues

2.1 In reviewing the Discussion Paper and associated Report we identified a number of fringe or threshold issues that should be addressed outside the scope of the NTC's submission questions. These issues, and our submissions on those issues, are outlined below.

- ***Addressing government distrust in Australia***

2.2 A major recurring theme that is paramount across all market commentary is that automated and connected vehicle data will signal a paradigm shift in governmental collection of data from individuals. While consumers have accepted (or at least tolerated) the large-scale collection of personal data by global tech companies like Facebook, Google, Apple and Samsung, the commencement of large scale collection of automated and connected vehicle data by government will raise fresh concerns regarding data collection from Australia's populace.

2.3 These privacy concerns may be a potential barrier to the technology's take-up and use in Australia. This concern is not only held by the NTC, but also uniformly presents itself as the prime area of concern across contemporary commentary on the issue.[1] The significant theorised benefits associated with increased use of automated and connected vehicles include reduced traffic fatalities and road congestion, increased emission efficiency and boosts to individual autonomy, especially for individuals who may be unable to currently drive, including disabled individuals and the elderly.[2] Reduced uptake of automated and connected vehicles by Australian consumers will limit beneficial change.

2.4 Broad scale privacy concerns may also pose significant risks to the technology's broad-scale implementation in Australia. Generally, the Australian public has recently shown it is generally unwilling to surrender its privacy. National unease regarding the Australian Government's upcoming My Health Record project culminated in a crescendo on the final day to opt-out of the system. High-user traffic lead to the website crashing, forcing the Government to extend the deadline for an additional ten weeks to meet demand.[3] This response from the Australian public should come as no surprise given recent reports of government distrust from multiple sources. Figures coming out of Edelman's 2018 Trust Barometer global report indicates that trust in government bodies in Australia fell 2% to 35%, the lowest trust levels across the previous five years.[4] A report commissioned by the Unisys Corporations found that 49% of Australians did not trust the government to keep their data safe, expecting a data breach to occur within the next 12 months.[5] These figures should be troubling for Australian governments moving forward as levels of distrust among Australians appears significant and widespread.

2.5 Addressing consumer privacy concerns must be the primary focus of proposed legislation to regulate the collection and use of automated and connected vehicle data. Without implementing thorough checks on governmental collection, use and storage of personal

[1] Kaur, Kanwaldeep and Rampersad, Giselle, 'Trust in driverless cars: Investigating key factors influence the adoption of driverless cars', *Journal of Engineering and Technology Management*, Vol. 48 (2018) 87-96.
[2] Barret, Lindsey, 'Herbie Full Downloaded: Data-Driven Vehicles and the Automobile Exception', *The Georgetown Law Journal*, Vol. 106 (2017) 181-208.
[3] McCauley, Dana, 'My Health Record opt-out deadline extended after system crash', *Sydney Morning Herald*, 14 November 2018, <https://www.smh.com.au/politics/federal/my-health-record-opt-out-deadline-extended-after-system-crash-20181114-p50g01.html>.
[4] Edelman, *2018 Edelman Trust Barometer Global Report*, <https://www.edelman.com/sites/g/files/ aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report _FEB.pdf>
[5] Unisys, *Australians believe telcos and government organisations more likely to suffer a data breach than other industries, Unisys research finds*, <https://www.unisys.com.au/offerings/security-solutions/news%20release/au-australians-believe-telcos-and-government-organisations-more-likely>.

information to avoid unnecessary data collection and limit the risk of data breaches occurring, we predict reduced or delayed take-up of automated and connected vehicles by Australian consumers.

- ***Local Government capabilities***

2.6 Local governments are a key stakeholder in the future roll-out and functionality of automated vehicles within the community. Often absent from consideration of the national regulation of automated and connected vehicles, local governments have a key role to play in the adoption of automated vehicles in each community across the country through their jurisdictional purview in planning, amenity impacts, traffic congestion and local road management.

2.7 In our practice, we engage with local governments regularly. Through this engagement we have identified a common concern across multiple local governments regarding the increased cybersecurity risk associated with the introduction of connected and automated vehicles. While local governments are excited by the prospect of being able to introduce adaptive automated vehicle projects, such as small-scale automated public transport initiatives, there is growing concern about the cost of managing and protecting personal information associated with the use of automated and connected vehicles. Unlike State and Federal governments which have the resources necessary to collect substantial amounts of data and to protect that data with robust cybersecurity measures, local government considers that the cost of managing personal data associated with automated vehicles may force local governments to delay or avoid implementing automated vehicle projects within their community.

2.8 In light of these comments we consider that there needs to be a shift in the way privacy regulation arguments are framed when considering reform proposals for automated and connected vehicles. The Discussion Paper explores the tension between governments, who need information to ensure road systems operate smoothly moving forward, and individuals, who want and are entitled to their privacy. However, the comments we have received from local governments imply that the driving forces behind legislative reform might not be as binary. In the case of local governments, a reduction in the amount or type of information that governments may collect is potentially as beneficial to them, from a cost and risk perspective, as it is to individuals from a privacy retention perspective. We recommend that the NTC considers the additional burden imposed on state and local governments in handling and using personal information obtained from automated and connected vehicles when proposing legislative reform.

- ***The application of the GDPR to automated vehicle data in Australia***

2.9 The Discussion Paper, drawing on conclusions made in the Report, states in section 5.4.5 that the European Union's General Data Protection Regulation (**GDPR**) could limit the information that private sector third parties hold. The Report concludes at section 8.1.1 that this was the case given that some automated vehicle manufacturers or service providers may have an establishment in the European Union.

2.10 With respect, we disagree with the conclusion outlined in the Report and consider that the GDPR is irrelevant for the purposes of data collection from connected and automated vehicles in Australia.

2.11 The GDPR's scope is outlined in Article 3 of the GDPR. As stated in the Report, the GDPR applies to the processing of personal data by a business with an establishment in

the European Union. However, this provision does not mean that any business with a branch or establishment in the European Union must comply with the GDPR with respect to all personal information they collect, hold and use around the world. The wording of Article 3(1) specifically states:

- *"(the GDPR) applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor* ***in the Union****, regardless of whether the processing takes place in the Union"*.[6]

  The key phrase in that provision is "in the Union". We consider that by this phrase, the GDPR is limited to the activities of businesses in relation to their conduct within the European Union. While this position is not yet fully settled at law, there is significant legal commentary that supports this view. While the GDPR does operate with extraterritorial effect due to Article 3(2), the GDPR's extraterritorial reach is limited to international businesses that offer goods and services to the European Union or who monitor the activity of individuals within the European Union. Additionally, the extraterritorial effect is limited to the data processing of individuals who are *"in the Union"*. What this means is international companies that operate automated vehicles will have to comply with the GDPR, but only in relation to their activities within the European Union and only with respect of individuals actually present in the European Union. While automated and connected vehicle companies will need to comply with the GDPR, for example, when collecting and using information connected with advertising campaigns in Europe, or from vehicle users in the European Union, they will not have to comply with the GDPR when collecting and processing information from individuals in other jurisdictions, including Australia.

2.12 Therefore, we do not consider the GDPR to be relevant to privacy issues arising out of the use of automated and connected vehicles in Australia.

[6] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*, Article 3(1).

3 Submission Questions

3.2 Outlined below are our submissions in response to questions raised by the NTC in its Discussion Paper.[7]

- ***Are the assumptions the NTC has identified for this discussion paper reasonable?***

3.3 In framing its discussion paper, the NTC proceeded on the basis of three assumptions;

(a) first, that it is difficult to irreversibly de-identify personal information;

(b) secondly, that international frameworks for data privacy in automated and connected vehicles are inconsistent and should not be used as a model form; and

(c) thirdly, that safety assurance systems will most likely include data recording and sharing criterion and that the NTC may propose specific legislative powers to access relevant automated vehicle information.

3.4 These submissions consider that each of the assumptions outlined above are reasonable, however, the first assumption outlined at paragraph (a) above is open to further consideration.

3.5 It is well established that the de-identification of information, while effective on a superficial basis, often fails when scrutinised either internally by an individual within the organisation or externally by third parties. As stated in the Discussion Paper, a number of mundane facts, when taken together, often suffice to isolate an individual. The most prominent example of this is provided as a case study in the Office of the Australian Information Commissioner (**OAIC**)'s guidance note on 'What is Personal Information', this example is outlined below:

- "*In 2006, AOL, a search engine provider, released apparently anonymous web search records for 658,000 users. However, some journalists working for the New York Times were able to link the search terms to identify users and contacted them. For example, "Subscriber 4417749" was able to be identified as a 62-year old woman, through her searches for local real estate agents and gardeners, her use of dating sites, health queries she had about her 'numb fingers' and questions about her dog's behaviour*".[8]

This example indicates that with a number of connected data points, it is possible to identify an individual without common identifying information such as that person's name, date of birth or address.

3.6 We consider that GPS vehicle location data, even when anonymised, is likely to be personal information. We note that the Discussion Paper shares this conclusion. An anonymised GPS vehicle location data set, particularly over a substantial period of time, will likely reveal the vehicle owner's home address, the address of family members, work address, working hours through commute times, hobbies such as social sport or classes and activities such as exercise, shopping or entertainment. Additionally, GPS vehicle

[7] Please note, where a question included in the Discussion Paper is not addressed below, we have elected not to comment. Our decision not to comment should not be taken as an admission of agreement or disagreement to any effect.
[8] Example extracted from Michael Barbaro and Tom Zeller Jr, 2006, 'A Face is Exposed for AOL Searcher No. 4417749', New York Time <http://www.nytimes.com/2006/08/09/technology09aol.html> , as referenced in Office of the Australian Information Commissioner, 2017, 'What is personal information?' https://www.oaic.gov.au/resources/agencies-and-organisations/guides/what-is-personal-information.pdf

location data may indicate that an individual is attending a specialist medical centre. Inferences that can be drawn from such information may be considered 'sensitive information' as well as personal information under the Privacy Act. With substantial data amounts, we consider that a consistent anonymised (or pseudonymised) data set will inherently disclose the identity of individuals when subject to sufficient scrutiny.

3.7 However, the issues around de-identifying personal information only apply to 'connected data' sets that is data that is connected to a particular pseudonym or is connected by multiple interconnected data points. As indicated above, the more data points available for analysis, the more likely it is that an individual can be identified from such data. In contrast, the less data points available for analysis, the less likely it is that an individual can be identified. While we do not purport to specialise in data analysis or data de-identification, we consider that it is unreasonable to conclude that all automated or connected vehicle data is incapable of de-identification. We consider that there are distinct differences in the type of data that may be collected, for the purposes of these submissions we have included the following examples of potential data types:

(a) 'abstract data' would be data that a particular number of vehicles where located at an intersection, or that a number of vehicles were travelling along a portion of a major highway at a particular point; whereas

(b) 'connected data' would be data sets that distinguish between particular vehicles and assign them unique data identifiers such as vehicle make and model or a pseudonym or identifier.

We consider that where information is collected and stored as 'abstract data', unconnected to other data, there is less potential for such information to be identified as personal information where appropriate de-identification or anonymous collection measures have been implemented.

3.8 The NTC has indicated in the Discussion Paper that governmental purposes for collecting automated and connected vehicle data are law enforcement, traffic management, and infrastructure planning. To the extent that the pursuit of such purposes can be fulfilled through the collection of 'abstract data' at key collection points (as opposed to end-to-end data collection which could identify and single out a specific vehicle's movements from point to point), then data de-identification procedures are likely to be more effective.

3.9 We would recommend that government adopts a policy approach that limits the collection of 'connected data' where possible and focusses on the collection of abstract data points which are more suitable to de-identification procedures in order to reduce the amount of personal information collected, ensure individual privacy and reduce the risk associated with cybersecurity events or data breaches.

- ***Have we accurately captured the new privacy challenges arising from information generated by C-ITS and automated vehicle technology relevant to government collection and use?***

3.10 The NTC outlined three new privacy challenges arising out of the information generated by automated and connected vehicles, in summary these challenges are:

(a) that connected and automated vehicles produce new types of data, such as in-cabin video and audio recording data, biometric data, biological and health sensor data;

(b) that, while government may currently collect limited C-ITS data through means such as road safety cameras, automatic number plate recognition, infrared traffic loggers and roadside collection devices, the increased uptake of connected vehicles will allow for more widespread direct collection of information; and

(c) that connected and automated vehicles will produce a greater breadth and depth of information which provides more opportunity for 'data linking' by government through the combination of multiple data sets available to the government.

3.11 We consider that the privacy challenges identified by the NTC (as outlined above) adequately reflect the potential privacy challenges arising from the widespread up-take of automated and connected vehicles.

3.12 In addition to the challenges outlined above, we also consider that Australia's current fragmented approach to privacy on a state by state basis is another key privacy challenge that will arise with the introduction of automated vehicles and the further integration of connected vehicles. As indicated in the Report, Australia's current privacy regime, when it comes to state governments, is outdated and fractured. Western Australia has no specific privacy legislation, South Australia's privacy guidelines are buried in cabinet circulars and of the remaining states, a majority of privacy statutes are based on the previous National Privacy Principles, the outdated precursor to the APP contained in the Privacy Act. If this regulatory landscape were to continue, an individual driving from Perth to Sydney for a holiday would have their personal information collected:

(a) at all times by the automated driving system entities (**ADSEs**) – automated and connected vehicle manufacturers and operators – in accordance with the Privacy Act;

(b) as they are leaving Perth by the Western Australian Department of Transport Main Roads in accordance with the limited privacy protections offered by the *Freedom of Information Act 1992* (WA);

(c) as they enter South Australia by the Department of Planning, Transport and Infrastructure in accordance with the Information Privacy Principle Instructions published as Premier and Cabinet Circular No.12 of June 2016; and

(d) as they drive towards the Harbour Bridge in Sydney by the New South Wales Department of Transport pursuant to the *Privacy and Personal Information Protection Act 1998* (NSW).

3.13 We consider that this fragmented approach is likely to disadvantage individuals and impose more difficult compliance requirements on ADSEs operating across state lines. Accordingly, we consider that a national approach to the privacy challenges arising out of the introduction of automated vehicles and the widespread implementation of connected vehicles is of paramount importance. We note that the Discussion Paper is proposing a national legislative approach to address these issues and we submit that such approach is the only viable approach open to ensure the privacy of the Australian public moving forwards.

- ***What information generated by C-ITS and automated vehicle technology is "personal information" and/or "sensitive information" under current law?***

3.14 For the purposes of these submissions, our analysis of what is personal information, and subsequently sensitive information, will be framed within Australia's national privacy legislation, the Privacy Act. While there are minor differences in the definitions of personal information across State legislation, and Western Australia and South Australia do not have specific privacy legislation, these submissions consider that a uniform approach to privacy protection is most appropriate when considering national transport issues.

3.15 Section 6 of The Privacy Act defines 'personal information' as:

- *"information or an opinion about an identified individual, or an individual who is reasonably identifiable:*

  (i) *whether the information or opinion is true or not; and*

  (ii) *whether the information or opinion is recorded in a material form or not"*.

3.16 The definition of personal information is significantly broad, covering any information that is about a person where that person is identified or reasonably identifiable. While there are many commonly understood examples of personal information, such as names, addresses, date of births and financial information, the scope of personal information is much wider in practice. In the context of connected and automated vehicles, the Discussion Paper has identified a number of examples where the data generated by connected and automated vehicles is likely to be personal data.

3.17 The definition of personal information is effectively a two-part test, is the information 'about' an individual, and is the individual identifiable or reasonably identifiable? Ultimately, the question of whether particular data is or is not personal information is an issue of context as the answer to both tests is a question of context. When considering the personal nature of information generated by connected and automated vehicles, the fact that government collects the information is contextually significant. Given that governments may potentially have access to substantial amounts of data, the ability to cross-reference data with other data bases, such as vehicle registration, employment records, tax records or birth records, and the ability for government to link data with other data they hold increases the likelihood that data they collect will be about an individual who is identifiable or reasonably identifiable. While not every piece of automated or connected vehicle data will be personal information, there is substantial scope for data to fall within the definition of personal information.

3.18 We agree with the conclusions drawn in the Discussion Paper on the potential status of automated and connected vehicle data as personal information, which include:

(a) in cabin video or audio data that may identify drivers and passengers;

(b) data from biometric, biological or health sensors where such data identifies rare traits or where the data can be cross referenced against other data bases;

(c) vehicle location data when connected to an identifier, such as vehicle registration plate number, when connected to a pseudonym identifier with a substantial data set that allows re-identification based on trend or pattern analysis or when linked to other data that allows trend or pattern analysis; and

(d) other C-ITS data that, when analysed or cross referenced to other data bases, may isolate a particular individual in the community.

3.19 The issue that arises out of a contextual based definition, such as the definition of personal information, is that what is and isn't personal information is fluid. Data that was collected from an automated or connected vehicle on its first trip may not be personal information, however it may become personal information at a later date when government eventually establishes a significant cache of data relating to that vehicle that begins to identify trends and patterns in the data. Alternatively, when data is accessed by an employee or department with access to other data bases to cross reference data the data may be personal information but may not be personal information if accessed by a government employee who does not have access to other data bases. Governments must comply with collection, notification use and disclosure protocols when collecting, handling and using personal information. Accordingly, whether automated and connected vehicle data is personal information is a pivotal compliance issue. As whether automated and connected vehicle data is personal information is a fluid issue dependent on context, governments are forced to act as if all data collected is personal information or risk breaching the Privacy Act (or equivalent legislation).

3.20 Automated and connected vehicle data produces varying information outputs and data types. Some of these data types will always be personal information, such as in-cabin video, while other data types are likely to be personal information when considering the context of the data's collection including the breadth of data collected by the government, the potential for government to link data sets and the ability for government to cross reference against other data bases. Given the possibility of automated and connected vehicle data to be personal information, governments must treat all automated and connected vehicle data as personal information or risk breaching its privacy obligations. We recommend that governments must treat all data collected from automated or connected vehicles (unless adequately de-identified as discussed at 3.9 above) as personal information in their approach to collection, management and use. In light of this recommendation, we would support legislation, similar to the provisions regarding metadata in the *Telecommunications (interception and Access) Act 1979* (Cth), which explicitly legislate that automated and connected vehicle data is considered personal information.

3.21 Section 6 of the Privacy Act defines 'sensitive information' as:

(a) information or an opinion, that is also personal information, about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices or criminal record; or

(b) health information about an individual; or

(c) genetic information about an individual; or

(d) biometric information and biometric templates.

3.22 Information that is considered 'sensitive' under the Privacy Act is afforded additional protections and entities must comply with additional requirements when collecting and using personal information.

3.23 The discussion paper identifies three possible circumstances where automated and connected vehicle data could constitute sensitive information, which include:

(a) the potential identification of an individual's racial or ethnic origin from in-cabin video recordings;

(b) the revelation of health information from biometric, biological or health sensor data; and

(c) sensitive information about an individual based on venues visited by the individual drawn from vehicle location data which may reveal sensitive information such as places of worship, hospitals and brothels.

3.24 In addition, we consider that in-cabin audio recordings also have the potential to elicit sensitive information where recordings capture discussions regarding individuals' sexuality, race, political or philosophical opinions, religious affiliation, association membership, criminal record or health information.

3.25 We consider the sensitive nature of some automated and connected vehicle data to be a significant issue regarding government data collection methods and powers. The Privacy Act provides under APP 3.3 that a government entity must not collect sensitive information about an individual unless the individual has consented to the collection and the collection is reasonably necessary for, or directly related to, the government entity's functions or activities.

3.26 Under the Privacy Act, consent may be express or implied, however consent will only be considered valid where; first, the individual was adequately informed prior to giving consent; secondly, the individual gave consent voluntarily; thirdly, consent was current and specific; and fourthly, the individual had the capacity to understand and communicate their consent. It is difficult to conceive a practical method of government obtaining individual consent to collect sensitive information from automated or connected vehicle users that is at all times informed, voluntary, current and specific and communicable. Potential methods of obtaining consent are outlined below:

(a) Sign-posting notifications by infrastructure that automated and connected vehicle data is being collected. Importantly, consent cannot be inferred merely because an entity has provided an individual with notice of the collection of their personal information. Therefore, governments cannot infer implied consent from individuals whose data is collected by merely relying on notices. While notification may inform an individual of the potential collection, they have no agency to respond to the collection while travelling in a motor vehicle along a public road.

(b) Providing written consent when obtaining a licence to operate or own an automated or connected vehicle. This alternative would likely fail the third element of consent outlined above as such consent is unlikely to be current months or years later when data continues to be collected or new data collection methods are implemented. Additionally, assuming that an individual cannot opt-out of giving consent (which would lead to practicalities when collecting information on the roads), then consent may reasonably be determined to be involuntary.

(c) Pop-up consent disclaimers that appear within the automated or connected vehicles digital interface may provide informed, current and communicable consent. However, responding to disclaimers while a vehicle is driving, particularly a connected vehicle only, may become impractical and increase safety risks. Additionally, significant questions would be raised regarding the voluntariness of

consent if individuals are unable to travel on public roads without electing to opt-in to providing their personal information.

We do not consider any potential consent method outlined above will adequately satisfy the requirements for valid consent under the Privacy Act. In the absence of alternative methods of obtaining consent, other than those outlined above, we do not consider that government will be able to collect sensitive information from individuals when collecting automated or connected vehicle data. Additionally, we consider it is unlikely that the collection of sensitive information by government in this context will ever be reasonably necessary for, or directly related to, governments' legitimate purposes.

3.27 The potential for automated and connected vehicle data to include sensitive information creates a significant issue for government collection. Whether a particular part of vehicle location data or in-cabin video data will constitute sensitive information is fluid and can only be determined on a case-by-case basis. More importantly, automated and connected vehicle data is unable to be identified as sensitive prior to collection and will only be discovered to be sensitive after the fact of collection. Therefore, in the process of collecting automated and connected vehicle data, governments will breach the Privacy Act in circumstances where data is later identified as sensitive. In order for governments to comply with the Privacy Act (or similar legislation) they will need to implement safeguards to prevent the collection of sensitive information. Given the types of sensitive information we have indicated above, such safeguards could include:

(a) not collecting in-cabin audio or video recordings;

(b) not collecting data from vehicle health or biometric sensors; and

(c) not collecting 'end-to-end' vehicle location data so as not to identify venues visited by automated and connected vehicles or by sufficiently amalgamating or anonymising information as discussed further at paragraph 3.9 above).

3.28 We note that governments may collect data in spite of the safeguards outlined above where the data collection is permitted under one of the five exceptions contained in APP 3.4, which include:

(a) where collection is required or authorised by or under an Australian law or a court or tribunal order;

(b) where a permitted general situation exists, such as lessening or preventing a threat to life or safety, acting in relation to suspected unlawful activity or misconduct, locating a missing person, defending legal or equitable claims, or where collection is necessary for alternative dispute resolution procedures, diplomatic or consular activities or defence activities;

(c) where a permitted health situation exists, such as providing a health service or conducting research;

(d) where related to an enforcement related activity; or

(e) by a non-profit organisation in certain limited circumstances.

3.29 In the interest of individual privacy, we would not recommend legislating for more lenient restrictions on the collection of sensitive information from automated and connected

vehicles and would recommend that governments remain restricted to collecting sensitive information in circumstances where one of the exceptions outlined above applies.

- ***Is the current information access framework for government collection sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology?***

3.30 The data generated by automated and connected vehicles is distinct from previous motor vehicle data collected by governments both in its nature and in number. These differences establish a new frontier of available data that is unframed within current data collection regulations. The Discussion Paper outlined three potential avenues through which current regulations may govern the collection of automated and connected vehicle data:

(a) government collection in light of state surveillance laws;

(b) government collection in accordance with privacy legislation; and

(c) law enforcement collection pursuant to privacy legislation exceptions.

3.31 In consideration of each of the current potential regulation frameworks outlined above, the Discussion Paper concluded as follows:

(a) surveillance device laws are unlikely to adequately regulate the collection of automated and connected vehicle data given that surveillance device laws differ on a state-by-state basis. It is unclear whether automated and connected vehicle data will be covered by the legislation where legislation may apply and that governments may rely on express or implied consent to excuse collection from the reach of surveillance device laws;

(b) Australia's privacy legislation may allow governments to collect automated and connected vehicle data on the basis that collection is necessary for one or more of the government's functions; and

(c) enforcement-related activity exemptions contained in Australia's privacy legislation generally allows law enforcement agencies to collect automated and connected vehicle data without complying with standard privacy provisions.

3.32 It is apparent that the current framework for government collection is insufficient to regulate the privacy challenges arising from government collection of automated and connected vehicle data. In this vein, each of the conclusions outlined at paragraph 3.31 above are addressed in the proceeding paragraphs below.

3.33 We consider that framing the regulation of privacy issues associated with automated and connected vehicles as a surveillance device issue would raise more questions than it addresses. The Report provides details on the variety across state approaches to surveillance legislation, however it is satisfactory for these purposes to highlight that this legislation is too divergent to offer a national solution to the privacy issues explored in these submissions. Additionally, the Discussion Paper's conclusion that governments could rely on implied consent arguments to excuse government collection from the operations of surveillance laws is an insufficient response to achieving long-term, stable policy implementation. Given these factors, we consider that a legislated approach to automated and connected vehicle regulation is necessary to avoid both reliance on exclusions from, and potential breaches by governments, of domestic surveillance device legislation.

3.34 As concluded by the Discussion Paper, Australia's various privacy regulations, including the Privacy Act and state based legislations will generally allow governments to collect automated and connected vehicle information that is reasonably necessary for their legitimate purposes, such as road and infrastructure management. However, we consider that implementing a responsive approach to automated and connected vehicle data privacy issues founded in Australia's current privacy framework would be insufficient on the following grounds:

(a) primarily, that although Australia's privacy regulations are relatively consistent across Australia, the lack of privacy legislation in Western Australia and South Australia and minor variations between legislation on a state-by-state basis, means that any approach limited to Australia's current privacy legislation would be unsatisfactory when compared with a uniform approach possible with national legislation implementation; and

(b) secondarily, as outlined in further detail in paragraphs 3.14 to 3.29 above, there are significant issues regarding the fluidity of personal information arising out of automated and connected vehicle data. Given the possibility for automated and connected vehicle data to contain sensitive information, there are substantial grounds for governments to breach current privacy regulations when collecting personal information for legitimate government purposes such as traffic and infrastructure management. Proceeding with automated and connected vehicle implementation while relying merely on current legislation would force governments to either substantially limit the types of data they may collect on an ongoing basis or risk breaching privacy regulations regarding the collection of sensitive information.

In our view, Australia's current privacy framework is <u>not</u> suitable to regulate the privacy issues arising out of automated and connected vehicle data.

3.35 The law enforcement-related exemptions contained in Australia's various privacy regulations are sufficient to address privacy concerns regarding law enforcement related automated and connected vehicle data. Generally, law enforcement bodies will be collecting information from ADSEs who would ordinarily be private businesses captured by the Privacy Act. Under the Privacy Act, ADSEs would be able to disclose personal information of drivers to 'enforcement bodies, including state and territory police forces and other agencies tasked with enforcing laws and offences, where they reasonably believe disclosure is necessary for 'enforcement related activities'.[9] However, while current privacy regulations may allow for the adequate pursuit of law enforcement related purposes when dealing with automated and connected vehicle data, there are arguments that law enforcement powers may be potentially too broad when considering the potential widespread use of automated and connected vehicles and the amount of data that may be produced. The Discussion Paper highlighted a point raised by the Report that automated and connected vehicle data could potentially facilitate mass surveillance. One of the 'enforcement related activities' prescribed by the Privacy Act is the conduct of surveillance and intelligence gathering services. Given the large quantity of data produced by automated and connected vehicles, and the revealing nature of such data which could easily reveal the location, habits, opinions and health of any individual using an automated or connected vehicle, the possibility of misusing data is relatively high. Given this potential

[9] Please note, please see section 6 of the Privacy Act for the full definition of an 'enforcement related activities'. In summary, enforcement related activities include the prevention, detection, investigation, prosecution or punishment of criminal or penalty/sanction provisions, to conduct surveillance activities, intelligence gathering or monitoring, to conduct protective or custodial activities, to enforce laws relating to the confiscating of proceeds of crime, to protect public revenue, to prevent, detect, investigate or remedy serious misconduct, or to prepare for proceedings before a court or tribunal.

for misuse, we consider that current privacy regulations are insufficient to protect individual privacy and we recommend that limitations on mass surveillance are implemented in draft legislation to address automated and connected vehicle data privacy issues.

- ***Is the current information access framework for government use, disclosure and destruction/de-identification sufficient to cover privacy challenges arising from C-ITS and automated vehicle technology?***

3.36 The Discussion Paper identified three main areas of the current information access framework regarding government use, disclosure and destruction/de-identification which may contribute towards privacy challenges with automated and connected vehicles moving forward. These three areas are summarised as follows:

(a) law enforcement use and disclosure of automated and connected vehicle data may result in increased surveillance opportunities because:

(i) law enforcement is exempt from complying with many use and disclosure principles where such non-compliance is reasonably necessary for the performance of law enforcement functions; and

(ii) the breadth and scope of data collected from automated and connected vehicles provides more detailed information to law enforcement agencies than may have previously been available to them;

(b) road transport laws around Australia contain provisions to facilitate information sharing between agencies and police which support road agencies disclosing information to police upon request; and

(c) requirements to destroy and de-identify personal information are unlikely to practically reduce the amount of personal information held and used by governments because the requirements to do so are narrow, they are not present across all states and territories and de-identification practices are often imperfect in practice.

3.37 As outlined at paragraph 3.35 above, the Discussion Paper proposes that law enforcement based exceptions to privacy laws may create an environment that allows mass surveillance. We consider that this proposition is accurate and that, not only will law enforcement based exemptions allow the potential for mass surveillance, they may also encourage it. Under the Privacy Act, an ADSE may disclose personal information to law enforcement bodies if it reasonably believes that disclosure is necessary for an enforcement related activity, which includes the conduct of surveillance activities and intelligence gathering services. The operation of the law enforcement exception in the Privacy Act is relatively broad. There is no requirement for ADSEs to only disclose information where those police activities are approved by a court or tribunal decision and accordingly there may often be no checks and balances placed on law enforcement collection beyond an ADSEs decision to dispute a request for information. As indicated in the Discussion Paper, not only is it unlikely that ADSEs will dispute law enforcement requests, but many privacy policies, such as that of Tesla, specifically outlines that the company will co-operate with enforcement bodies when requested to do so. In addition to collection from private entities, sub-paragraph (b) above highlights the simplicity in which information may be transferred between government departments to law enforcement. The explanatory memorandum to the *Privacy Amendment (Enhancing Privacy Protection)*

Bill 2012 (Cth) (**Explanatory Memorandum**),[10] outlines that the law enforcement exception was included to allow "limited use and disclosure" of personal information for criminal law enforcement purposes "in the public interest when balanced with the interest in protecting an individual's privacy". We consider that, although there is obviously a strong public interest in enabling police forces to enforce the criminal law, the potential scope of information available from automated and connected vehicles goes beyond the *limited* use and disclosure contemplated by the Explanatory Memorandum. Unlike the examples contemplated by the Explanatory Memorandum, such as requesting an entity to provide information unknown to police, such as an individual's name or address, police agencies may have the capacity to request information from ADSEs and government agencies that identify sensitive and revealing information across a substantial amount of data. Additionally, access to sensitive and revealing information may potentially be provided not only about an identified individual the subject of an ongoing investigation, but about the public broadly in the pursuit of general or broad surveillance. Consider the potential scenario outlined below:

Scenario: Potential abuse of law enforcement collection exception[11]

The Local Police Force receive an unconfirmed report of a robbery that has just occurred at the Main Street Shopping Centre involving an XYZ automated vehicle.

In order to respond as quickly as possible, the Local Police Force contact XYZ to request information regarding all XYZ vehicles that were in the vicinity of the Main Street Shopping Centre within the previous hour. XYZ, having received an official request from a law enforcement agency have a reasonably belief that the disclosure of personal information is necessary for the conduct of an enforcement related activity and hands over automated vehicle data to the Local Police Force of all vehicles in the area within the requested time.

XYZ provides the Local Police Force with automated vehicle data relating to fifteen XYZ automated vehicles that recorded vehicle location data in or around the Main Street Shopping Centre within the last hour. Upon receiving this information, the Local Police Force is able to review in-cabin audio, in-cabin video and vehicle location data of each vehicle, revealing both personal information and potentially sensitive information of the inhabitants of each vehicle.

The scenario outlined above indicates the potential scope of the law enforcement exception to the collection of automated and connected vehicle data on a relatively small scale. A best-case result out of the above scenario is that police are able to identify a robber among the individuals from a stolen bag in the passenger seat of the automated vehicle and are able to locate and arrest the individual. In this best-case example the personal information of other individuals driving XYZ automated vehicles are not compromised further than an initial review by police officers. However, worst-case examples potentially include:

(a) that police are unable to identify any compromising evidence from in-cabin audio or video and have to make an assessment on which automated vehicle to pursue

[10] <https://www.legislation.gov.au/Details/C2012B00077/Explanatory%20Memorandum/Text>.
[11] Please note, we do not purport to have significant experience in the conduct of police investigation matters, nor knowledge of police department internal policies and the above scenario is provided for illustrative purposes only.

and search in the short-term to prevent escape or potential further offences. Based off of in-cabin video, a biased police officer elects to pursue a particular automated vehicle containing a passenger they deem to be 'suspicious', for example, whose racial or ethnic origin has been revealed by in-cabin video or whose political opinions have been revealed by in-cabin audio. Following such identification, the automated vehicle is stopped and searched exposing the passenger to fear or embarrassment, despite not having committed the alleged offence; or

(b) that the initial report of an offence was a hoax, and none of the individuals whose personal and sensitive information has been disclosed to police who were involved in the offence.

The scenario outlined above, and the potential ramifications of that scenario are an example of why we consider that the current framework regarding the disclosure and use of personal information in law enforcement scenarios is insufficient in light of the new privacy challenges posed by automated and connected vehicles. We consider that the revealing nature of automated and connected vehicles, both because of new data types that are generated by automated and connected vehicles and because of the amount of data generated, is not adequately contemplated by the current law enforcement exemptions contained in the Privacy Act and other privacy statutes across Australia. We recommend that steps need to be taken to ensure that governments and entities are unable to unnecessarily invade the privacy of automated and connected vehicle users through general or mass surveillance measures, while still retaining the ability for police forces to pursue legitimate criminal enforcement in the public interest.

3.38 The Discussion Paper highlights that the destruction or de-identification requirements imposed by privacy statutes across Australia are unlikely to practically reduce the amount of data held by governments. As discussed in more detail at paragraph 3.5 above, de-identification procedures are of limited practical use, with de-identified data sets being able to be re-identified when cross-referenced against external data points or where substantial enough in number to identify trends and patterns in data. Additionally, due to the fragmented nature of Australia's privacy statutes on a state-by-state basis, requirements to de-identify or destroy personal information are not uniform across states and are even absent in some state jurisdictions. On this basis, we do not consider that the current framework regarding destruction and de-identification of personal information is sufficient to address the privacy issues arising out of the use of automated and connected vehicles.

3.39 For the reasons outlined in paragraph 3.37 and 3.38 above, we consider that the current framework surrounding use and disclosure of personal information is insufficient to address the privacy issues surrounding automated and connected vehicles and their increased roll-out in Australia moving forward.

- ***Are separate options for addressing the privacy challenges of C-ITS technology and of automated vehicle technology reasonable for achieving any future reform?***

3.40 While these submissions have generally addressed automated and connected vehicle data as a single collated data type, and it is true that there is a degree of overlap between the two, there are also unique differences between the subsets of data produced by automated vehicles and that produced by connected vehicles (otherwise referred to as C-ITS data).

3.41 C-ITS technology produces data when connected vehicles communicate with other vehicles and infrastructure. Generally the type of data this information creates is limited to vehicle speed, location and direction. Alternatively, automated vehicles produce large amounts of data from various data recording sources. The type of information produced by an automated vehicle may include audio and image data, external sensor data, electronic control unit data, event and crash recorder data, navigation data and biometric, biological and health sensor data. Generally automated vehicles will also include C-ITS technology of some kind, however connected vehicles may only include some or none of the information generally produced by automated vehicles.

3.42 The Discussion Paper questions whether it is reasonable to pursue separate options to address the regulation of C-ITS data and automated vehicle data. We submit that a separate regulatory approach to C-ITS data and automated vehicle data is unnecessary. As outlined at paragraph 3.23 above, automated and connected vehicles may produce a variety of sensitive information from different sources including in-cabin audio and video recording, health sensors and biometric systems and vehicle location. Importantly, both automated vehicles and connected vehicles produce these sensitive data types. Connected vehicles produce location data which may elucidate sensitive information, while automated vehicles may contain in-cabin audio and video recording and health sensors. Additionally, automated vehicles will generally incorporate C-ITS technology and are therefore likely to also record location data. Both automated and connected vehicle technologies have the capacity to produce information that is sensitive and deserving of substantial protections, in addition to each producing general personal information which is also worthy of protection. We consider that any separate approach would therefore need to incorporate equal provisions to protect individuals and manage the use of collected data. Accordingly, we consider that separating the regulation of C-ITS data from the regulation of automated vehicle data would unnecessarily split legislative approaches and would likely lead to consumer confusion. We do not recommend separate approaches to regulating automated and connected vehicles.

- ***Is there a need for reform to address the identified problem and the privacy challenges of automated vehicle technology, and, at this stage of automated vehicle development, which option best addressed these privacy challenges while recognising the need for appropriate information sharing?***

3.43 Fundamentally, we consider that there is a significant need for reform to address the privacy issues arising out of the substantial uptake of automated and connected vehicles in Australia. Throughout these submissions we have identified a number of issues with the current framework regarding the collection, use and disclosure of personal information, which include:

(a) significant government distrust currently permeates Australian society and the uptake of automated and connected vehicle will likely be limited or delayed if reforms are not implemented that ensure the public can trust their privacy to government agencies;

(b) that Australia's privacy statutes on a state-by-state basis are fractured and insufficient to deal with the privacy challenges arising out of the use of automated and connected vehicles and that national reform is necessary to ensure individual privacy is consistent across state lines and for ADSEs operating in multiple state jurisdictions;

(c) the fluid nature of data types potentially collected by governments, such as vehicle location data which may lead to the collection of sensitive information where data is collected on as an end-to-end basis or when a sufficient quantity of data is collected. Given the potential for data to be sensitive and the associated breach of privacy regulations (assuming standards commensurate with the Privacy Act apply) when collecting that information without the individuals consent, reform may be necessary to limit the types of data governments can collect or risk ongoing breaches of privacy legislation;

(d) that legislative reform is necessary to ensure that governments do not potentially breach and do not potentially have to rely on implied consent arguments to exclude the collection of automated and connected vehicle data from state surveillance laws;

(e) due to the revealing nature of data, and the scope for substantial amounts of data, to be collected from automated and connected vehicles, the current exceptions form privacy legislation applying to law enforcement related activities have the capacity to promulgate general or mass surveillance of individuals and that legislative reform is necessary to limit the scope of disclosure to and use of personal information by law enforcement agencies with regard to automated and connected vehicle data;

(f) destruction and de-identification standards imposed on governments in relation to data obtained from automated and connected vehicles are piecemeal and, where applicable, unlikely to practically reduce data held by government and that legislative reform is necessary to impose stricter destruction and de-identification protocols on governments and to ensure they apply to all entities that may hold or collect automated and connected vehicle data; and

(g) that best practice cybersecurity and information management requirements are imposed across all government agencies that may collect, hold and use automated and connected vehicle data.

3.44 As outlined in paragraph 3.42 above, we do not consider that separate reform options for automated vehicles and connected vehicles are necessary or sufficient and recommend that reforms address all data collected from both automated and connected vehicles.

3.45 The Discussion Paper outlines the NTC's preliminary preferred option for legislative reform, referred to as 'Option 2' which involves the agreement of broad principles covering the following:

(a) that automated and connected vehicle information is most likely personal information;

(b) when establishing a regulatory framework to support lawful access, use and disclosure of automated and connected vehicle information, additional privacy protections are likely needed to appropriately limit the collection, use and disclosure of automated and connected vehicle information to specific purposes;

(c) that privacy protections should be legislative;

(d) that privacy protections will need to specify;

(i) the automated and connected vehicle data covered, noting that sensitive data types may warrant further protection;

(ii) the specific purposes this information can be used for; and

(iii) the parties to whom specific limitations apply; and

(e) that privacy protections could cover additional elements (such as destruction and notification) to address other identified gaps.

3.46 We consider that reform Option 2 generally addresses the issues we identified as driving reform necessity in paragraph 3.43 above. However, we consider that potential reforms must go further in order to address the privacy concerns identified in these submissions. We would recommend adoption of reform Option 2 with the following amendments:

(a) that regulatory frameworks providing for the lawful access, use and disclosure of automated and connected vehicle data should be founded in the APP established by the Privacy Act to ensure that general standards are commensurate across each State and across the government-private sector divide, with applicable additional limitations as discussed in this paragraph and in paragraph 3.45 above;

(b) that specific data types, such as in-cabin video and audio, vehicle data where it provides an 'end-to-end' transect capable of identifying departure points and destinations and biometric or health sensor data are defined as particularly sensitive data (in addition to general sensitive information definitions that apply broadly to any automated and connected vehicle data) with additional limitations on collection, use and disclosure of such information. Similarly to limitations proposed in the NTC's 'Option 3' we would recommend limitations to the collection, use and disclosure of this information, as outlined below:

(i) limitations would apply to all government agencies, including road agencies, law enforcement agencies, local governments and other government bodies engaged in the collection or use of automated and connected vehicle data;

(ii) that such information would be limited for the purposes of automated vehicle compliance and enforcement; and

(iii) that such information could not be used for other purposes, such as general law enforcement, road safety or infrastructure planning or other purposes unless:

(A) the government agency has a warrant or court order authorising a different use; or

(B) the individual in question has provided informed, current, voluntary and communicable consent; and

(c) that reform options impose data security and management standards at least commensurate with, and preferably superior to the standards imposed under APP 10 of the Privacy Act.

3.47 We support a reform option based on Option 2 and including the amendments outlined at paragraph 3.46 above and consider that such reform would recognise and address the privacy challenges imposed by the increased roll-out of automated and connected vehicles, allows for the beneficial use of data by government to enforce automated vehicle laws and plan for infrastructure and transport while restricting uses that may be exploited, such as mass surveillance, and provides flexibility to develop additional bespoke policies to address automated and connected vehicles distinct from other privacy issues.

- ***Would the draft principles adequately address the privacy challenges of C-ITS and automated vehicle technology?***

3.48 We consider that the draft principles prepared by the NTC broadly address the privacy challenges faced with the introduction of automated and connected vehicle technology in Australia. In order to ensure Australian consumers are adequately protected, informed and continue to be protected for the future, we recommend the following amendments to the draft principles:

(a) **Principle 1** should be amended to specify that the definition of C-ITS and automated vehicle data must be defined in *technology neutral terms* to ensure that individuals continue to be protected despite progressing or adapting technology;

(b) **Principle 3** should be amended to specify that a regulatory framework that supports lawful collection, use and disclosure of automated and connected vehicle information *must be founded in the standards imposed by the APP under the Privacy Act, with additional protections as specified in these principles* to ensure commensurate standards across state governments and across the public-private divide.

(c) **Principle 6** should be amended to specify that government should consider notifying users of how data will be used, disclosed and stored *by providing a plain-English notice that is simple to read and understand*; and

(d) **Principle 7** should be amended to specify that consent should be obtained from automated and connected vehicle users *at or prior to collection of information and, if that is impracticable or unsafe, at regular intervals and when collections methods change*.

3.49 We also recommend that the following additional principles should be included:

(a) **Principle 9**, *that best practice data security and data management standards, that are at least commensurate with those required under APP 11, should be legislatively mandated to governments when storing and using automated and connected vehicle data to reduce the risk of data breaches or misuse*;

(b) **Principle 10**, *that information such as in-cabin video and audio, vehicle data where it provides an 'end-to-end' transect capable of identifying departure points and destinations and biometric or health sensor data be specified in proposed legislation as particularly sensitive information*; and

(c) **Principle 11**, *that the sensitive information outlined in Principle 10 be restricted form collection, access and use by government bodies for all purposes other than automated vehicle compliance unless otherwise authorised by a warrant or court order*.

3.50 In implementing the amendments outlined at paragraphs 3.48 and 3.49 we consider that the NTC will adequately address the privacy challenges posed by automated and connected vehicles.

4 Conclusion

Automated and connected vehicles have the capacity to provide substantial benefits to Australian society, reducing motor vehicle casualties, contributing to emission reduction and traffic decongestion and providing autonomy of movement to the nations' must vulnerable individuals. Accordingly, ensuring the successful rollout of automated and connected vehicles in Australia should be the primary focus of government bodies when considering regulatory and policy changes in the automated and connected vehicle sphere to contribute towards future societal advancement.

A significant road-block to automated and connected vehicle uptake across Australia is the genuine concerns regarding privacy permeating Australia's population. Automated and connected vehicles have the capacity to generate previously un-disclosed information and data on such a scale that the privacy of individuals will undoubtedly be compromised without governments taking active steps to protect privacy. However, Australians currently do not trust their government to use their data properly or to protect it from security breaches. In order to protect the privacy of individuals and enhance community digital trust, in the interests of ensuring automated and connected vehicles are successful in Australia, privacy protections must be specifically included in proposed automated and connected vehicle legislation.

5 About Squire Patton Boggs

Squire Patton Boggs is a global law firm providing insight at the point where law, business and government meet. With 47 offices across 20 countries, we offer access to expertise and invaluable connections both locally and across the world.

We provide legal and strategic advice to clients engaging with regulatory bodies at all levels and across all judicial and administrative forums. Our advice is grounded in a comprehensive and extensive understanding of the law, industry and how governments operate, including how to engage with policy makers and policy enforcers at all levels. We also help clients to assess, in advance or in real time, what government policies could affect their business interests and how to respond to those policies.

In the Automotive Sector

Squire Patton Boggs provides cross-disciplinary legal services to the automotive sector, regulators and suppliers across the world.

Clients include OEMs/manufacturers, tier 1 and tier 2 component suppliers, retailer dealer groups, distributors, motor traders, fleet providers, logistics financiers and finance companies. We also advise regulators, industry associations and consumer organisations in this arena.

Our highly regarded Transportation Infrastructure and Local Government Practice provides strategic counsel to clients on a wide range of policy, legislative and regulatory matters. Key members of our team include former US Secretary of Transportation, Rodney Slater, as well as a former Assistant Chief Counsel for the US NHTSA. In Australia John Poulsen and Margie Tannock lead our Public Policy Practice, which coordinates our HAV working group.

Our expertise includes advising the automotive sector on issues highly relevant to the development and deployment of HAVs, including:

1. Data Privacy and Cybersecurity
2. Communications
3. Insurance and Products Liability
4. Research & Development, Intellectual Property, Strategic Alliances and Collaboration Arrangements
5. Infrastructure and Public Finance

Margie Tannock I Partner & Head of the Cyber Security & Data Privacy Team in Australia

T: +61 8 9429 7456
E: margie.tannock@squirepb.com

Margie's practice focuses on advising clients from all sectors on statutory approvals, corporate governance, compliance and public law. She works closely with clients to resolve regulatory risk across all aspects of corporate decision making.

Margie also delivers strategic advice and commercial solutions involving property and infrastructure developments. Margie has advised on regulatory permitting and licencing for major resource and energy projects, including port, rail and electricity generation. She works for a number of major property developers, in planning, land compensation and environmental litigation.

Margie has worked for the Commonwealth Director of Public Prosecutions in corporate criminal prosecutions, and has significant understanding of the legislative framework that governs the actions of company boards.

With long-term experience in public law, she advises many statutory authorities, including universities, private colleges, redevelopment authorities, local governments and state government departments. She has a particular focus on governance within these organisations, including advising executive councils and officer holders on obligations and liabilities.

Local Connections
Global Influence

SQUIRE PATTON BOGGS

squirepattonboggs.com