Dr. Kate Mathews Hunt
SJD (Bond) LLM LLB (Hons) BA(Hons) Uni Melb
Honorary Adjunct Teaching Fellow
Bond University

Attn: In-service safety for automated vehicles
National Transport Commission
Level 3/600 Bourke Street
Melbourne VIC 3000
Australia

By web submission: www.ntc.gov.au
Email: enquiries@ntc.gov.au

26 August 2019

NTC CONSULTATION REGULATION IMPACT STATEMENT
In-service safety for automated vehicles July 2019[1]

> *U.S. Transportation Secretary Anthony Foxx told Reuters earlier this year he planned to propose regulatory guidelines by mid-July to clear the way for wider deployment of automated driving systems.*
>
> *"This technology is coming," Foxx said. "Ready or not, it's coming."*[2]

For the record, Foxx did not meet that commitment.

Responses to the questions appear on page 6- 13 inclusive.

Introduction

I am a published researcher[3] in the field of consumer law and information technology and completed a doctoral thesis on the consumer and privacy law implications of the internet of things, with specific focus upon smart car, home and wearable technology. I am also formerly a corporate lawyer at a large OEM and have advised extensively on issues pertaining to consumer issues, automotive advertising, product liability and (then) trade practices compliance. I am a member of the Qld Law Society Competition and Consumer Law committee and an Advisory Board member of ACE-EV (an electric vehicle start-up based in Adelaide).

I regard the regulation of the internet of things in terms of consumer privacy, data security and autonomy to be one of the great regulatory issues facing this country, but am concerned that salient consumer issues are often subsumed beneath exponential projections of the value of IoT technology economically, and its many positive benefits for society long term. Those excited

[1] As a honorary academic, please note that this submission is neither endorsed by, nor associated with, Bond University.
[2] http://www.reuters.com/article/us-tesla-autopilot-idUSKCN0ZH4VO?type=companyNews
[3] See for example, Mathews-Hunt, Kate, 'CookieConsumer: Tracking online behavioural advertising in Australia' *Computer Law & Security Review* 32(2016): 55-90; and Mathews-Hunt, Kate. 'CloudConsumer: contracts, codes and the law' *Computer Law & Security Review* 31 (2015) 450- 477 http://dx.doi.org/10.1016/j.clsr.2015.05.006

expectations proceed somewhat illogically in some ideological circles to policy positions based upon permissionless innovation,[4] without adequate regard to the precautionary principle[5] both as to safety, security, privacy and other impacts upon consumer rights. Indeed, the IoT may be said to represent a conjunction between the best and worst features of cloud computing, online security, artificial intelligence and big data.

Automated vehicles (I use the term 'smart cars' in my work) is undoubtedly the future of the automotive industry and is undergoing extensive scrutiny in both the EU and USA. The latter have just committed over USD4 billion over ten years to accelerate development.[6] The EU is actively engaged in investment, research and policy work in this area. Given intentions as to vehicle standards harmonisation, the EU approach is obviously something which Australia ought to follow closely, and should (consistent with NTC recommendations) adapt within our own automated vehicle (AV) regulatory framework wherever feasible.

The NTC is to be commended for its extensive, methodical and high-quality work in this field and I thank them for the opportunity to provide this submission.

I also repeat the fundamental propositions contained within my previous 2016 submission (**attached** for convenience), which remain salient.

Fundamental propositions

> *Former NHTSA chief Joan Claybrook said in an interview the agency needs to set performance standards for electronic systems like [Tesla's] Autopilot. "It's the like Wild West. The regulatory system is not being used," Claybrook said.*[7]

My overall recommendation is that in-service safety for automated vehicles (AV) requires the careful modernisation and adaptation of existing very successful regulatory frameworks as to AV hardware, expanded by specific prescriptive rules, performance-based regulation and a general safety duty, to create regulation specific to the novel aspects of ADS and internal and external interactions of AV technology.

While it seems likely that (absent governmental intervention) vehicle fleets will remain mixed for decade(s), so in-service AVs may well share roads for many years with traditional vehicles and increasingly automated variants. This adds a layer of complication to automotive regulation, but reinforces the need for a national regulator capable of careful monitoring, regulatory flexibility and of maintaining close industry: consumer relationships. There is no capacity to 'wait and see' or to **abdicate regulation to self-**

[4] Adam Theirer for example, is a US academic who argues that this was the Clinton administration approach to internet regulation – which he lauds as a great success. See for example, Thierer, Adam & Ryan Hagemann, 'Removing Roadblocks to Intelligent Vehicles and Driverless Cars' Mercatus Center (17 Sept 2014 accessed 3 Mar 2016) < http://mercatus.org/sites/default/files/Thierer-Intelligent-Vehicles.pdf>; Thierer, Adam, Permissionless innovation: the Continuing Case for Comprehensive Technological Freedom, (2016 accessed 5 Mar 2016) < http://mercatus.org/publication/permissionless-innovation-continuing-case-comprehensive-technological-freedom>

[5] See United Nations Education Scientific and Cultural Organization (UNESCO), 'The Precautionary Principle' (Mar 2005 accessed 2 Feb 2016) < http://www.eubios.info/UNESCO/precprin.pdf>; EU, 'The Precautionary Principle' (21 Sept 2015 accessed 3 Feb 2016) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al32042>

[6] NHTSA, (14 Jan 2016) < http://www.nhtsa.gov/About+NHTSA/Press+Releases/dot-initiatives-accelerating-vehicle-safety-innovations-01142016>

[7] http://www.reuters.com/article/us-tesla-autopilot-idUSKCN0ZH4VO?type=companyNews

certification or a more general 'safety' obligation either: the political and commercial momentum is here as to AV development/ deployment and regulators need to work within that process, not lag behind it. Industry, consumer and multi-regulator work on setting the safety, security, privacy and operational frameworks, conscious of international parameters, is time critical for certainty, safety and smooth deployment in Australia.

It seems likely that all parties would agree to the following:

- Continuous improvement of vehicle safety is an objective of car manufacturers, consumers, insurers and regulators;
- AVs are the future of consumer motoring (which by definition will include private ownership, but increasingly entail ride share and other user models);
- AVs offer the potential to significantly reduce the road toll, most particularly once the fleet is no longer hybrid – however given the average age of the Australian vehicle on road is 10.1 years,[8] this reduction will increase over time;
- AVs create practical and legal uncertainties as to driver/ control liability issues in levels 3 and 4 as to conditional/ high automation;
- Prima facie, level 5 or level 4 ADS control presupposes manufacturer's liability, subject to unforeseeable environmental or other potentially causative factors;
- AVs offer significant potential social benefits in terms of traffic management and emissions reductions. The impact as to a reduction in traffic remains open;
- AVs collect significant consumer data both as to the state of the vehicle, but also as to the driver/ passenger reactions and behaviours, vehicle location, external information (via cameras) and other matters which may be regarded as potentially significant in determining accident causation,[9] and enhancing AV safety on-road, but which in conjunction with other uses, is significantly privacy-intrusive;
- Persons injured to automotive accidents (autonomous or otherwise) should have rights to access compensation;
- As vehicle autonomy increases, so too does manufacturer liability while consumer 'driver' liability decreases;
- A nationally consistent framework harmonised with the UN-ESE is imperative.

Important Gap – data gathering, use and privacy

> *Until recently, the data collected by companies developing automated driving systems was a closely guarded secret. Automated vehicles (AVs) can collect 4TB or more of raw sensor data every day…*
>
> *At the end of a test day, all the data gets ingested into a data center from the vehicles and the good stuff is analyzed and labeled. Raw data by itself doesn't have much value for training the machine learning systems that form the core of modern AV systems.The objects in the data that are of interest, including pedestrians, cyclists, animals, traffic signals and more. Before any sensor data can be used to train or test an AI system, all of those targets need to be labeled and annotated by hand so that the system can understand what it is "seeing.*[10]

[8] ANCAP submission to NTC, April 2016.
[9] See the submission by Maurice Blackburn (4 Jul 2016), which proposes access for a "vulnerable injured person" to event data.
[10] Sam Abuelsamid, 'Argo AI And Waymo Release Automated Driving Data Sets' Forbes, 19 June 2019.

The only area where the NTC's work has fallen short, in my view, concerns data privacy and use.

This is a critical area both as to information sharing for safety and product performance reasons, as between manufacturers and others, but also, with respect to passenger human rights, autonomy and consent. As with many apps, software and other online 'services', the provision of automated vehicle mobility should not be a coercive experience whereby passengers are forced to consent to data gathering, inferential profiling and other privacy-intrusive actions- simply by taking a ride in their or someone else's car. As with the General Data Protection Regulation, if a service can be provided without data collection, then it should be. Provision of data should be granular, opt in and voluntary. Conversely, privacy should be by design, and default.

At this stage it is difficult to define precisely what data manufacturers and other AV entities are collecting. This should be ascertained and addressed.

Automated vehicles will entail significant data flows between manufacturers, dealers, cloud services and third parties, and it is imperative that the principles of data minimisation and privacy are strictly and clearly applied. The Australian *Privacy Act 1988* (Cth) is, as the recent ACCC inquiry has confirmed, quite inadequate to meet the challenge of data-collection in the digital/ online environment.

The NTC has not properly addressed this issue. The OEMs have not properly addressed this issue. The OAIC has not provided comment or advice to the NTC on this issue. International research has not been considered as to this issue.

Automated vehicles collect 'personal data' from users including location data, user data, driver behavioural data and passenger data. According to *IOT Now*:

> "IDC forecasts that by 2025, the global data sphere will grow to 163ZB (that is, a trillion gigabytes). That's 10 times the 16.1ZB of data generated in 2016. Inside the vehicles themselves the news is daunting too. Autonomous vehicles' data is growing even faster thanks to autonomous test vehicles, which typically generate between 5TB and 20TB of data per day, per vehicle.
>
> This includes cameras, which tend to generate 20 to 60Mbps, depending on the quality of the images that are captured, which ranges from standard definition to higher definition, as well as sonar (10 to100kbps) radar (10kbps), LIDAR systems (10 to 70Mbps) and GPS (50kbps). The key is to ensure that sensors are collecting the right data and it is processed immediately, stored securely and transferred to other technologies in the chain."[11]

[11] https://iotnowtransport.com/2019/02/12/71015-data-storage-key-autonomous-vehicles-future/

UK's Bearing Pont Institute cite estimates as high as 25GB of data per hour from each car.[12] *Globalme* repeats the unremarkable proposition that future cars will run on data (not petrol) and this means mining data from 'driver/ owners' and passengers. As well as the outside world:

> *Passengers in tomorrow's autonomous vehicles will be subject to the focused attention of an advanced vehicular AI, and in many ways the quality and safety of their ride will be dictated by the vehicle's ability to interpret human wishes and needs.*[13]

This article cites voice commands (intentional car inputs) and less voluntary/ involuntary forms of communication. Either way, this "interpretation" involves AI (as for smart home devices) constantly listening and recording passengers, and ultimately, intelligently inferring profiles, information , behaviours and even wants, from that data.

> *More advanced versions could even hear* implied *commands, such as the implicit command to turn around within the exclamation, "I forgot my wallet!"*

The article speculates improving speech recognition could even interpret passenger wants despite the "slur of inebriation". Learning may also come to infer and even modify driving style and other vehicle attributes by gauging passenger reaction; for example, anxiety after a fast turn or annoyance with a slow one. It is a short step from modifying the driving task to interpretative actins; for example, decision-making as to taking a longer route to avoid a road blockage versus saving costs by waiting in the traffic jam.

But involuntary/ behavioural communication is also data for collection.

Regulation is required to control precisely which data may be collected, how it is used and stored, and for what purpose. Consumers should not be obliged to consent by default or for fear that functionalities will be denied. If the OEMs can comply with the EU's *General Data Protection Regulation* (GDPR) across much of Europe, they can readily technically afford identical such privacy protections to Australian consumers. But they may not, unless this requirement is mandated by law.

> ***GDPR – OEM privacy obligations to customers***
> ***Lawful, fairness and transparency*** *(Any information and communication concerning the processing of personal data for individuals must be easily accessible by them)*
> ***Purpose limitation*** *(data to be collected only for specified, explicit and legitimate purposes)*
> ***Data minimisation*** *(Personal data must be adequate, relevant and limited to what is necessary for business purpose)*
> ***Data accuracy*** *(To ensure that personal data are accurate and are kept up to date where it is necessary)*
> ***Storage limitation*** *(Personal data must be kept in a form that makes it possible to identify data subjects for no longer than is necessary for the purposes of the processing)*

[12] https://www.bearingpoint.com/files/BEI008_06_GDPR_Connected-cars-and-privacy-shifting-gear-for-GDPR_final.pdf&download=0&itemId=434626
[13] https://www.globalme.net/blog/autonomous-cars-data-not-gasoline

Integrity and confidentiality *(To protect the individual's personal data against the unauthorised or unlawful processing, destruction and damage)*[14]

This should be the baseline, whether by specific AV regulation, *Privacy Act* amendments, by ADR incorporation or otherwise. Data sales by OEMs, even in anonymised forms should be prohibited. I understand that government use of data remains to be concluded.

Response to Consultation Regulation Impact Statement

Questions	Response to Discussion Paper (May 2016)
1. To what extent has the consultation RIS fully and accurately described the problem to be addressed, including the in-service safety risks? Please provide detailed reasoning for your answer.	Very well- save for its consideration/ identification of ➢ **the risks attendant upon a mixed-fleet on-road**; These risks impact upon the AV fleet as human drivers (sub level 5) may make "human" or unpredictable mistakes or fail to be a reactive fallback-ready user or undergo a non-AV failure which may cause an accident. It will take non-AV drivers and pedestrians time to adapt to these new road users. How AVs respond to this is relevant to AV safety for AV-users and non-users (other drivers, pedestrians, cyclists etc). ➢ **The risks attendant upon road infrastructure** AVs may also make mistakes: for example, where road infrastructure is poor or confusing to AI, or where signs are altered to render them unreadable etc. For example, Tesla's Model S hit a crash barrier on a highway which it did not "see" due to poor road markings. Most OEM companies developing AV now refer to using comprehensive maps to "verify" AV sensor/LIDAR etc technology. In other words, a backup. Changes ➢ **The risks attendant upon algorithmic decision-making** Examples include decisions made in a trolley-problem type scenario; or where differing marques adopt different algorithmic approaches which may create unsafe on-road situations. For example, Tesla's autopilot beta system has safety warnings in its manuals telling consumers it may not work faced with 'white light', snow and heavy rain conditions. ➢ **the privacy impacts and risks of AVs.** It is noted that government use of AV data is under separate inquiry.

[14] https://www.bcs.org/content-hub/gdpr-implementation-in-the-automotive-industry/

	Privacy is not adequately considered or addressed. I strongly recommend that data gathering and privacy become a Statement of Compliance requirement for ADSEs and that the government establish specific privacy legislation/ mandatory industry code (Code) whereby consumers own their own AV car data and consistent with data minimisation, license only 'need-2-know' data to manufacturers, for C-ITS and to road safety authorities/ road managers, under strict consents/ conditions. Consumers might choose to share or sell certain other data to interested parties- for example, to insurers. The Code should also address how ADSEs must collect, use, (securely) store and gather data, as well as minimum encryption or other technical security requirements.
2. Have we correctly identified the parties with an influence on the in-service safety of automated vehicles and accurately described their role? If you identify additional parties, please explain what their role is.	Identification of each potential party is an appropriate technique to identify potential claimants and legal risks of involved parties. All parties appear to be identified. However, while the rationale to underscore responsibility upon ADSE Executive Officers, it is somewhat confusing why these individuals require a separate legal head of liability over and above that which would normally apply to executives engaged in automotive production? I like the idea given clarity is always desirable; but am not sure it is appropriately justified in the report? I would also point out that mid-level managers also have significant responsibility for effecting safety; and as the VW/ Audi case revealed there was involvement in use of the emissions defeat device well beyond the upper echelons (Exec Officers) of the company. However, for avoidance of doubt, I do support this initiative.
3. Have we correctly identified the parties with an influence on the in-service safety of automated vehicles and accurately described their role? If you identify additional parties, please explain what their role is.	Identification of influence is a useful prioritisation approach, but I am not sure that the ratings of levels of influence are all accurate. Depending upon systems, road infrastructure may well have a significant impact upon safety.

4. Have we accurately described the regulation that already applies to relevant parties that would help ensure the in-service safety of automated vehicles?	Yes mostly. Do you discuss the FCAI Code of Practice for Recall? One query - some of the conclusions as to the operation of the CCA are questionable. Note also there are some important changes to this legislation shortly, which are relevant to liability. I would recommend these be revised in anticipation..
5. Do you think there are any new risks posed by second-hand ADS components, after-market modifications or the transfer of ownership of automated vehicles, which may not be adequately addressed by existing regulation designed for conventional vehicles?	YES. I think the current regime with respect to these items is too permissive for an AV context. 2nd hand ADS components may include software one assumes, so question the capacity to fully safety-check 2nd hand software? Also question the interchangeability of ADS componentry as between different models or other vehicles? Could this result in incompatibilities, etc. After-market modifications are surely a very risky exercise. Obviously, these will need not to interfere with the Statement of Compliance standards (and ADRs) but one wonders if there should be a more formal certification or other scheme for modifications, given their capacity to interfere with extant systems (often inadvertently), or to otherwise compromise AV integrity and safety. One simple example might be a bull bar applied to interfere with vehicle sensors. It should be noted that while AVs are expected to be safer, they will still need to address road challenges such as kangaroos etc; albeit they may be able to stop faster than a human driver – but they may also be driving faster too. Re transfer of ownership, vehicle roadworthiness remains important. This should include ensuring all software updates are performed, as well as tyre safety etc as per usual. Arguably, hand-over of manuals may be easier in an autonomous context as they will be on-board via the computer one would think. However, I question if additional training is required to familiarise buyers with AVs and their technology; this could be an online requirement (simulations, tests etc) provided by the manufacturers (and roads authorities with respect to road rule implications for passengers- if any). It could be a mandatory prerequisite to registration. It may also be necessary to consider other road user education: for example, do motorcyclists/ cyclists need to know what to expect from AVs? Wiping prior user data may need to be addressed as a mandatory requirement, to protect the previous user's information (for example)? The new owner may also have an interest in making their own data story; for example, where vehicles infer behaviours, driving style, routes, restaurants or wants from previous owner's behaviours?
6. Do you think the parties with an influence on in-service safety are sufficiently covered by Australia's current legal frameworks?	I agree with and adopt the report'conclusions in this respect.
7. Do you think that a general safety duty to ensure the	A general safety duty is appropriate and necessary principle-based regulatory approach. But it is one element in a mix.

safe operation of the ADS 'so far as reasonably practicable' is appropriate to address the safety risks?

So while one suspects it may be the endgame regulatory approach, it should partner with prescriptive and performance-based approaches,

It is also consistent with impending amendments to the CCA, so is consistent policy-making as to consumer rights in the 21st century context.

The phrase **"so far as is reasonably practicable"** is not that familiar in an automotive context (c/f trains, WHS etc). This causes me concern. As the NTC notes, it does not require safety at any cost, as the safety level (reasonably practicable) hinges on situation and context.

As the NTC suggests, in WHS contexts it entails a process of risk management:

"In essence, it requires weighing the risk against the resources needed to eliminate or reduce the risk. It does not require every possible measure to be implemented to eliminate or reduce risk, but it places the onus on the person holding the duty to demonstrate (or be in a position to demonstrate) that the cost of additional measures to control the risk (over and above those risk controls already in place) would be grossly disproportionate to the benefit of the risk reduction associated with the implementation of the additional risk control."

These should not be foreign concepts to automotive manufacturers, or even, designers. But the application of SFAIRP standard to technology risk (software, AI and algorithms interacting with hardware and other systems) , especially at a design and in-service stage, is difficult. I am not sure it works as well given the many unknown attributes of AVs and AI systems on-road; and disparity between vehicle models and designs.

I am not sure that the example applications: certain commercial vehicles, marine vessels and rail are sufficiently analogous.

Appendix C: This is helpful and a good start BUT I also comment that software updates enable constant safety improvements to be effected. If reasonably practicable to be effected does this oblige a manufacturer to forthwith roll out updates immediately and repeatedly? In other words what if reasonably practicable changes constantly courtesy of technology developments; at what point is liability fixed or when does it

Other approaches:

The CCA product liability provision (s 138) as to safety refers to a standard "safety such as persons generally are entitled to expect". It is also expected that a general safety provision will be inserted into the CCA shortly; the NTC may benefit from reviewing/ participating in, that process and outcomes.

It should be noted that software is 'goods' under the CCA and motor vehicles are generally covered under the Act. Note the 'state of the art' defence is problematic in an AI context:

The fundamental question is whether there should be some minimal 'safety' standard as to system safety which all manufacturers must meet as a baseline? Does this bring us back to more prescriptive approaches as well as a more general overriding duty?

For example, when dealing with level 4 vehicles, where the fallback-ready user is required to take-over the driving task, there must also be an obligation to use safety systems to ensure such drivers do not become bored, distracted, or otherwise lacking in

	attention. Tesla's systems at the time of the accident of Joshua Brown (2016) did not force a driver to resume control (whereas subsequent iterations ultimately will stop the car if the driver does not put hands on wheel!)
8. **If a general safety duty were introduced, which parties should it apply to?**	Every entity who supplies anything (part, component, software etc) to make up an AV should have a concurrent safety duty. Ultimately the manufacturer / ADSE must be responsible to the consumer and regulator for the interaction of all supplied parts/ components. However any individual component failure, should be sheeted home to the responsible supplier, and if appropriate, the manufacturer. In other words the duty must be concurrent. **The levers of liability cannot be underestimated in terms of driving the safety message home.** One comment as to Executive liability. Fines for companies have a significant deterrent effect and adversely impact reputation and the share price which adversely impacts management. Yes, shareholders are less able to influence safety but the market is a powerful mechanism and shareholders do not usually enjoy investing in companies which are subject to large regulatory fines. Having said that the tech giants seem somewhat immune to the taint c/f VW/ Audi. Tesla seems to fall somewhere in-between after several accidents which occasioned bad press. Yes. Boards and Execs should be accountable; but one might imagine certain technical safety-related decisions which are dispersed across various technical department, and to which no due diligence can readily reach. This liability should thus require some standard of personal culpability, such as conspiracy, misconduct or negligence (etc).
9. **If a general safety duty were introduced, should it apply on public and private land (such as residential driveways)?**	Yes. AVs will be expected to work in all the same places as conventional vehicles. If an AV runs a child over in a driveway, for example, through a sensor defect, should that child be uninisured? What about AV utes which farmers may use on private off-road environments, such as paddocks? Given AVs remove the driving task from humans, they must be safe in all reasonable applications surely.
10. **Should people injured by breaches of the general safety duty have a cause of action, or should the ability to enforce a general safety duty be limited to a regulator?**	Individual and regulator cause of action. A general safety duty can be breached with respect to one vehicle but not the entire model range or class. There are precedents for this under the CCA which have not been subject to overuse, misuse or abuse. **Note: the NTC conclusions to qus 7-10 inclusive on pages 87-88 are sensible and it is correct to assert that a mixed approach will allow greater flexibility which is clearly needed and desirable.**

	One comment as to repairers – for non-dealer repairs, it will be necessary to have access to substantial information in order to assume such a duty. In particular, if a repairer diligently repairs a hardware item but in so doing causes damage (in some unexpected way) then to what extent should the repairer be liable?
11. Do you think there should be specific driving rules for ADSs like the Australian Road Rules, or would it be sufficient to simply require them to 'drive safely'?	This is a very interesting question. I can only speculate but suspect a staged transition would be the safest approach to such a significant change. Hypothetically, I suspect the answer is that road rules be required until such time as all vehicles are autonomous and separate grade roads keep (non-connected) pedestrians and cyclists away from AV movements. The question is predicated on the idea that C-ITS will enable AVs to read each other's positions and to rapidly adapt accordingly. This clearly cannot apply unless all road users are using C-ITS – and presumably human drivers have no place in what looks externally, like a chaotic road environment. The main concern would be in defining what "safely" means and how human passengers, pedestrians and cyclists might cope (at least initially) in what may seem like a random pin-ball experiment. I cannot answer the question of whether it really is technically possible to have a road where cars are careening all about (seemingly) randomly, in reliance upon their systems being good enough to detect each other and avoid collisions. Surely these systems are not fail-safe; a car travelling at 100 kms an hour cannot stop on a dime if a pedestrian suddenly steps out?
12. What approach to regulating the dynamic driving task for ADSs most efficiently achieves safe outcomes? Please provide reasons	Given technological uncertainties and prospects for rapid continuous improvement, one questions if prescriptive rules would be comprehensive enough or adequate to achieve this outcome. To some extent, regulators may be in the hands of the innovators, which suggests that a **performance-based approach** coupled with a **general safety duty** may provide the best and most comprehensive option. As para 6.6.2 suggests, the AV industry is insufficiently developed to satisfy the "best use" criteria. Ultimately, when the technology is well developed and risks more clearly known and systems better understood, a general safety duty may be appropriate.
13. What functions and powers does the regulator need to effectively manage in-service safety? Would these differ depending on whether the regulator is enforcing a general safety duty, or only prescriptive duties?	Yes. Refer earlier comments re ACCC enforcement of a general product safety duty.
14. Have we accurately described the scope of the regulatory task? Please	Yes wit respect to methods to reguate. It may have been useful to drill into para 7.8 and explain the TR68 approach in Singapore and where that fits with the regulatpry approaches proposed.

provide data and evidence where possible to support your answer.	
15. Have we accurately captured the benefits of the regulator being: a. a government body or an independent body? b. a national body or state and territory level bodies? c. an existing body or a new body?	Yes. The regulator should be a government body.
16. What are your initial views on how the regulator should be funded?	Well. Through federal govt funding and through penalties awarded via prosecutions. The ACCC illustrates the benefits of creating a properly funded and effective regulator, capable of international outreach and of generating a culture of compliance through regulation and enforcement. The OAIC illustrates a (previously) inadequately funded regulator, largely unable to fulfil its functions properly or in such a way as to enforce privacy compliance and regulation in Australia. For example, the OAIC has published Guidelines as to the Privacy Act which are rarely used or referred to, and are not subject to enforcement – rendering them less than effective.
17. Have we adequately and accurately captured the key legislative implementation models for in-service safety of automated vehicles?	Yes.
18. Do you think there are any transitional or constitutional issues that could arise when Australia establishes a national law for automated vehicles? If so, please explain what the issues are, and if they differ depending on the legislative implementation model used.	I will leave this for constitutional lawyers to comment upon. However, I must emphasise the desirability of a national law system preferably overseen for cost and consistency reasons, by a national regulator.
19. Have we accurately described how each option could work, as well as the advantages and disadvantages of each option?	Yes.
20. Which option most effectively addresses the problem statement? Please consider your answer in conjunction with the PwC cost–benefit analysis.	OPTION 4 (subject to comments above) BUT states and territories need to commit to the national scheme. If the state and territories regulate identically to fill the gaps consistently, can they assign enforcement responsibilities to the national regulator.
21. Is there another option, or combination of options,	OPTION 3.

which could more effectively address the problem statement? In particular, please consider whether there is a preferable combination of the elements of each option (governance arrangements, duties, legislative implementation)	**I have an important point which is perhaps not specifically addressed by this question.** As to DUTIES, the latest thinking in a technology law context with respect to product design and in-service operation is observance of these principles: 1. Safety by design 2. Privacy by design 3. Privacy by default 4. Security by design 5. Security by default These should be written into the Compliance principles and self-certification should require evidence of adherence to these principles. For example, safety-related updates should be mandatory and occur without passenger involvement, to avoid people failing to conduct updates. They above principles are not foreign to designers, manufacturers or developers, enable risk management from cradle to grave and may change as products age in the consumer environment. For example, AV security may be an ever-updatable feature for so long as AVs are supported. What will be the requirements as to spare parts and availability, software updates and other standards pertaining to these vehicles?

Other miscellaneous comments

Page No.	Comment
1 Glossary	**ADS & ADSE & Manufacturer** Is this distinction in consumer's best interests? I am unsure why this distinction is being made given AVs are, like current fleet, an amalgam of software and hardware. In Australia an importer is deemed 'manufacturer' of the vehicle- in its entirety. This is subject of course to insurance and liability arrangements as between parts/ systems suppliers and manufacturers – but this distinction is largely irrelevant for consumers who deal with the dealer/ manufacturer. Do these definitions subvert this position and is that in consumers' best interest?? - Modern cars already contain huge amounts of software, but consumers are not directed to software developers/ manufacturers should their car develop a software issue/ defect - AVs will still have tyres, physical safety technology, and other physical components which carry direct manufacturer liability aspects - Does this distinction enable liability battles between software and hardware developers as to accident causation? Did the AV malfunction and drive straight at a wall, or did the tyres fail causing an accident? Will one supplier have information asymmetry over another- and over the passengers? [Note this is another argument for consumer ownership of all vehicle data.] As a side comment, from the early discussions surrounding liability, the manufacturers indicated that they would assume crash/ defects liability once consumers were in AVs. See e.g. Volvo

	https://fortune.com/2015/10/07/volvo-liability-self-driving-cars/ and Mercedes/ Google/ Volvo: https://jalopnik.com/mercedes-google-volvo-to-accept-liability-when-their-1735170893 In practice, for autonomous technology failures, Tesla has tended to deny liability based upon human misuse (and US laws) claiming that the driver should always be ready to take charge (fall-back ready user), even on highway situations. Assuming the *Seeing Machines CAN Drive trial* (page 29) as well as significant human behavioural literature as to distraction/boredom/etc and systems driver alert capabilities, this is perhaps a questionable outcome. Is this distinction enabling liability to be hived off or reducing Manufacturer responsibility for software? Is this transferring risk to the software developers, who traditionally, do not have a responsive liability culture? It seems to me that there is a distinct advantage is retaining the auto manufacturers as the overseer of vehicle safety through strict liability? Are they in the best position to coordinate, test and create the AV for safety; especially where systems must interact safely? It is however noted that often the ADSE will also be the Manufacturer.
10 Point 1.3	**"The opportunity"** The US data (94%) cited is questionable or at least undifferentiated. The NTC should identify all individual factors and their role in fatalities to accurately paint the picture. Note also my research as to recalls already being predominantly software-related. This is relevant to risk, data ownership/ access and disclosure & causation attribution. "…A MUARC Study identifies driver error - intoxication (13.5%), falling asleep (11.8%), fatigue (10.9%) as the dominant causation - the US Department of Transport claims (questionably) that 94% of accidents are attributable to driver error: Vanessa Beanland, Michael Fitzharris, Kristie L. Young, Michael G. Lenné, Corrigendum to "Driver inattention and driver distraction in serious casualty crashes: Data from the Australian National Crash In-depth Study" *Accid. Anal. Prev*. 54C (2013) 99–107 [626]. The remaining 6% are attributed to poor maintenance and environmental error. Product defects are the "unique cause" in less than 1% of accidents." Source: K. Mathews-Hunt, thesis, at page 28 (Annexed)
Privacy	This is a critical issue which has not been fully considered in the Discussion Paper. It would be most useful to set the AV privacy parameters now so that industry has certainty. It is unlikely - even were Australia to set stricter parameters to other nations - that the industry could not adapt their data collection/ use practices here to reflect Australian law. There are two important aspects to this question: the data collected by AVs and the capacity of the Privacy Principles regime to adequately protect consumers. Consumers neither know or understand the sort of data which AVs may collect and which manufacturers will ultimately use under privacy consents. The German group ADAC recently reported on the wide range of data collected by one model BMW: it included trip and distance data, maximum engine revolutions, the status of vehicle lights, length of time the driver used different driving modes, when the seatbelt tightened due to sudden braking, latest destinations entered into the car's navigation system, and personal information such as contacts synchronized from mobile phones. The Privacy Principles (PPs) are inherently flawed insofar as they rely upon a consent model as to consumer data collection and use, and the OAIC often issue non-binding (sensible) guidance as opposed to mandatory guidelines. This flaw becomes even more significant in the context of a privacy-intrusive technology, such as those within the internet of things. A second, related point is that the PPs are generally quite poorly enforced by the OAIC – initially as a result of issues in terms of its regulatory powers (which have since been improved) but secondly, as a result of difficult budget cuts in the past few years. Sole reliance upon the OAIC would

presuppose a far more active and aggressive privacy regulator – which may take some years to emerge, if at all.

Some thoughts on privacy-protective Options –
Option One

Personal information (and sensitive PI) may either continue to be regulated under the PPs, but subject to a specific industry code of practice approved by the OAIC, which imposes additional and specific restraints. It may for example identify specific types of information collected by vehicles and prescribe limited categories of use or address consistent and acceptable forms and methods of consent. While this does impose a greater privacy burden upon the automotive industry, consumer trust is important in a privacy-intrusive context and the industry must already comply with the PPs and adapt to the forthcoming EU Data Protection Directive and Regulations. Further, the rationale for this is that AV data is uniquely intrusive both at the point of collection but also, if subjected to other (non-anonymised) uses by insurers or via big data analysis. It is almost as intrusive as personal data collected by smart home systems. The key is perhaps agreed de-identification standards or processes for specific data types, and a specific Code ought to prescribe how the industry is permitted to use consumer data – a recommended approach is to provide services to the specific (identifiable) consumer, but any other uses (for example) such as third party transfers or consumer data analytics should be in de-identified form or subject to a very specific separate form of consent.

The US Consumer Privacy Protection Principles, were specifically drafted to avoid imposed regulation and perhaps reveal how industry will draft self-regulation principles to optimise their position and options, while minimising practical effect. While acknowledging that "consumer trust is essential" and averting to concepts such as "context of collection" (which includes "reasonable expectations"), the Code still has significant flaws and weaknesses from a privacy perspective – including reliance upon consents and allowing the use of biometric data, geolocation and behavioural (driving) data in some contexts, without proximate and affirmative consent.

There are innumerable academic studies and materials which evidence that consumers neither read nor understand Privacy Policies, nor how their data may be used and in whose hands it may ultimately end up. Indeed, there is clear evidence that privacy policies are drafted to optimise widespread data use and monetisation by collectors, while consumers have little chance (even were they to read thousands of words) of understanding their true implications.

AV enables a new and potentially highly intrusive form of data collation, and while it may be used positively by manufacturers for vehicle-related consumer services (such as telematics and vehicle logbook/ repair information) or used to enhance discerning accident causation, it may be misused if sold or passed on to third parties or related corporations (such as manufacturer's finance company arms) in a non-anonymised form.

Automotive manufacturers ought not become data brokers or enable mass data analytics or consumer profiling - by default.

It is however important to note that data has a tangible value and the question of consumers potentially trading their data uses in return for a benefit (such as reduced insurance premiums or vehicle costs) is one which might be investigated. The real issue remains that consumers must fully understand the implications of sharing – and present methods utilising privacy policies are failing in this task.

Option Two
Alternatively, and preferably for clarity, specific regulation as to data ownership in an AV context to address the issues above is required. This accords with part of the recommendation of Maurice Blackburn, who recommend the regulation of third-party access to event data information for prescribed purposes.

That regulation might take account of the FIA Region I principles which "…demand that car manufacturers publish a list specifying all vehicle data collected, processed, stored and transmitted externally for each model. This list must be easily available and understandable to consumers. Carmakers must commit to state-of-the-

art data security. Drivers must have the option to easily deactivate the processing and transmission of data that are not absolutely necessary for safe vehicle operation. Ultimately, motorists should not be locked into the manufacturer's system. Consumers are paying for the hardware that makes connectivity possible and therefore deserve the freedom to access a variety of services from a variety of service providers. It is within a fair and open market that consumers benefit from the lowest prices and the most innovative products."

Possibly. Consistent with goals to harmonise standards and international approaches, Australia's classification system should follow the 22 June 2016 WP 29 Definition of Automated driving and general principles for developing a UN-regulation.
Other Important Regulatory Issues:

Who owns the data?
Vehicle data should belong to the consumer with a defined license to the manufacturer to use for specific industry-agreed and regulated purposes. There is already evidence that AV manufacturers regard vehicle data a trove for them to use and exploit, for purposes which may go well beyond primary collection purposes or those within 'consumer expectation'. The US Consumer Privacy Protection Principles (which are not binding upon signatories and use the word 'may' a great deal) clearly demonstrate that the industry wants to 'use' data for purposes well beyond those legitimately relating to the driving and monitoring of the vehicle. VW's Chairman said: "the car must not become a data monster…" and unless steps are taken in an opt-in methodology, then AV data privacy will be poor indeed.

If ownership were regulated; that is, to specify which bodies may access the data and for what purposes, then consumer trust and confidence in their vehicle data privacy would be greatly enhanced. It should be clearly identified as to what data is being collected, how much of this belongs to the owners, the manufacturer and how much can be (automatically) shared with other legitimately interested parties. Many parties have an interest and these require a balance: consumers, manufacturers, repairers, insurers, police, courts, traffic control, (etc). Specified access to certain types of data and other access to anonymized data could enable broader uses by less-entitled parties – such as traffic volume via geolocation for example - without transgressing consumer privacy. This certainty would remove the consumer burden of Privacy Policy consent, which as research suggests, is a failed system in terms of genuine informed consent, in any case.

The other option is an 'opt-in' system, which while privacy-protective, still suffers from all the same negatives as PP consents. The FIA Region I provides three consumer principles: Free Data, Free choice and Free competition – see Option 2 under Qu 9. Above.

Ethics:
The UN and EU factor ethical considerations into law and policy-making frameworks and there is no reason why Australia should not explicitly inform consumers as to ethical issues pertaining to AV. Issues such as the fact that "people will die" in AVs – due to software defects, algorithmic issues and the like – require serious discussion, to ensure the public is fully informed that such risks exist. That less people may ultimately die – may depend upon the time taken for AVs to become the dominant vehicle type – but is also an issue for public awareness and discussion.

Beta software & other data-gathering exercises
In my view, beta software should be banned from release upon an unsuspecting AV public. While beta is designed to accelerate overall deployment time and to garner product data in the field, automotive safety is a vastly different context than IT.

This is illustrated by the recent fatal Tesla Model S accident in the US, which was caused (according to Tesla) in the following manner:

"…a tractor trailer drove across the highway perpendicular to the Model S. Neither Autopilot nor the driver noticed the white side of the tractor trailer against a brightly lit sky, so the brake was not applied. The high ride

height of the trailer combined with its positioning across the road and the extremely rare circumstances of the impact caused the Model S to pass under the trailer…"

While Tesla utilised a range of methods to 'remind' consumers that Autopilot was a beta technology and requires driver monitoring, there is evidence that consumers are treating it a little like a cruise control on steroids. This includes a youtube video of one man supposedly 'asleep' whilst his car navigates traffic. If reports are correct though, Elon Musk purportedly stated that ""The probability of having an accident is 50 per cent lower if you have Autopilot on… Even with our first version, it's almost twice as good as a person." If true (and the author cannot verify this beyond media reports) then it illustrates how public representations may be misconstrued by over-eager consumers – despite numerous others which offer clear Tesla warnings to the contrary. In other words, despite software warnings, alerts and the like, Tesla's efforts to remind consumers of their duty to remain in control appear not to be succeeding with some drivers.

This is also yet another variant of the 'consent' issue – consumers consent/ agree to drive Autopilot in one way, but after either not paying heed or after gaining false confidence, they are using it in ways which contravene manufacturer's instructions and expose themselves and others to safety issues.

Human Factors: Research has already revealed human behavioral, technology and vision-related factors, (as well as others identified in chapter 12) which may adversely affect the safety of conditionally/ highly automated vehicles driven by human beings. This area requires significant closer examination, both by regulators and manufacturers. These include:

- Behavioural/ Human factors: research suggests that drivers who no longer actively 'drive' but are required to actively monitor road conditions and take back control in low notice, potential emergency situations rapidly deteriorate in their monitoring task. Evidence also suggests that humans are not "particularly good at long term monitoring" and complacency may set in where past (positive) experience generates false confidence;

- Technology factors: Autonomous computer sensor technology requires "significant further study… to model the sensors and the underlying recognition technologies on which these systems rely". That point is underscored by Tesla's own warnings, which explicitly identify Autopilot as a "beta product" and describe numerous entirely foreseeable road scenarios (fog, direct sunlight, etc) when Autopilot sensor capabilities may be degraded (or non-functional as it appears in the recent fatality);

- Driver vision research: this suggests that the side-on tray truck crash scenario is a "well-known perceptual problem for human drivers", so should have been a foreseeable issue for Tesla in its design and safety assessments.

It is not appropriate to leave manufacturers to discern the human-machine interface without some form of prescriptive guidance. This issue is critical for vehicle safety at all levels prior to full autonomous, both for drivers and pedestrians and other road users. Proposals on page 54 provide possible solutions, all of which require government-led involvement in safety assessment. The report suggestion on page 56 that a fuller regulatory review might be more appropriate when such vehicles are closer to deployment in Australia, is not recommended. As Tesla's Autopilot case study suggests, vehicle capabilities are increasing rapidly, software will be enabled increasing vehicle autonomy update by update and the question is – can regulators and consumers (responsibly) respond to this market-driven evolution.

The dynamics of road-use will change with these vehicles and above all else, the road-using community needs to be educated as to how these vehicles work, how humans must work with them and what AVs are trained to 'see' – and what they do not.

Data & realistic plain English consumer warnings

In addition to the genuine comprehension issues and the general lack of diligence with which many consumers read manufacturers' warnings, there is an obligation upon manufacturers for warnings to be clear and comprehensible. It is not acceptable for consumers to be exposed through premature release of technology,

	ring-fenced by an array of unrealistic product warnings. It is to be hoped that the NTC will closely watch the NHTSA investigation into the Tesla S crash, within a prism informed by Australian law: it may be an illustration that drivers are too cavalier or alternatively, that some 'exclusions' are evidence alone that a product may be unsafe for consumer use. **Hacking etc**. This is a feature of modern software and a risk factor in AVs insofar as software controls the vehicle's operations. Cases have already been evidenced in most internet of things contexts where software system defects or vulnerabilities enable intrusion and vehicles have been effectively highjacked. Obviously this is an area appropriate for standards regulation. A corollary with AVs is their potential use in terrorism, which seems an extreme example but is one which ought not be ignored. It is unclear whether or not that risk is any greater than traditional car bombing scenarios. Another related issue is vehicle software ownership. If the US tractor industry is a potential guide, what is the impact of manufacturers asserting ownership over the AV software such that ultimately, vehicle purchasers may only hold a product use license – without permission to modify programming or make repairs. This overlaps with third party repairer's rights to access vehicle data as per the AAAA submission to NTC. **Licensing educated 'drivers'** Consumer risk associated with these vehicles increases whilst they remain in the conditionally/ highly automated categories. Consumer education in these phases is vital to safety and to overcome the over-confidence and flouting of manufacturer warnings, as seen (for example) currently with the Tesla Model S on YouTube. There should either be a mandatory industry Code as to specific steps for consumer education as generations adapt to AV, or licensing regulation ought adopt such a programme. Methods are innumerable and subject only to then extant technology, but may include virtual reality training, seminars, online training, etc. It would be worthwhile, given the significant change looming, that licensing and vehicle delivery/ registration transfer procedures include off anf online requirements as to this type of educative work. Some consideration ought be given to incentivising AV take-up in an attempt to reduce the 'hybrid' period when we have a range of differing vehicle levels on road. The faster the fleet transitions, the greater the benefits to society.

Conclusion

Autonomous vehicles are an exciting innovation in road safety and efficiency, which will genuinely change the face of human transportation and logistics within the next few decades. But I would respectfully urge regulators to take a precautionary principle[15] approach with AV regulation, which in my (somewhat dated) automotive industry experience, is usually consistent with the zealous automotive industry approach to product design and safety. This would include taking regulatory steps to carefully control and advance AV testing and deployment and features such as data collection and use – taking into account human frailty - and not risking lives in the over-amped fear of appearing to stifle innovation.

[15] United Nations Education Scientific and Cultural Organization (UNESCO), 'The Precautionary Principle' (Mar 2005 accessed 2 Feb 2016) < http://www.eubios.info/UNESCO/precprin.pdf>

It seems clear that the industry is innovating very well, and injecting privacy controls over vehicle data use together with discouraging (in my view) beta software releases (or indeed anything 'beta' when it comes to vehicles) and fostering clear consumer education, warnings and training, will do much to enhance the regulatory environment within which AVs will rapidly emerge.

The automotive industry has a long and largely positive history in this country as a responsible corporate citizen. If government works closely with the industry, provides sufficient regulatory 'sticks' and 'carrots', adopts legislation backed by mandatory rules and codes of practice, and takes into account consumer education and vulnerabilities, as well as consults with all stakeholders, then the future of AVs in this country is assured.

A reluctance to engage – or a desire to be seen as a light touch or principle-only based regulator – will not enhance AV development, which is essentially, an internationally-driven exercise. Rather it will lessen industry incentives to be responsive and may lead to damaging outcomes for a new technology which is going to require significant consumer trust, confidence and adjustment (as well as regulatory and infrastructure adjustment) to accommodate.

I recommend that the government be a bold but responsive regulator, closely aligned to European approaches, in the interests of protecting Australian consumers to at least international standards and enabling a positive implementation of a truly remarkable technology to this country.

Thank you for the opportunity to make this submission.

I take this opportunity to reiterate that all views are my own.

Yours sincerely,

Dr. Kate Mathews Hunt
Honorary Adjunct Assistant Professor| Bond University
Senior Counsel| Mathews Hunt Legal
Advisory Board| ACE-EV Group