IPSA AISP
25th World Congress of Political Science
July 21-25, 2018 | Brisbane, Australia

Emerging governance responses to risks associated with autonomous vehicles

Araz Taeihagh and Hazel Lim Si Min

Lee Kuan Yew, School of Public Policy, National University of Singapore

Presented at

RC30.8 Governing Novel Technologies Panel

23-07-2018 | 17:30 - 19:15

Emerging governance responses to risks associated with autonomous vehicles

Araz Taeihagh*,[1] and Hazel Lim Si Min

* Corresponding author: Lee Kuan Yew School of Public Policy, National University of Singapore, 469B Bukit Timah Road, Li Ka Shing Building, Singapore 259771, spparaz@nus.edu.sg

Abstract - The benefits of autonomous vehicles (AVs) are widely acknowledged, but there are concerns regarding the extent of the benefits they bring as well as their risks and unintended consequences. In this article, we first examine AVs and different categories of the technological risks associated with adoption of fully autonomous vehicles. We then explore different types of strategies that can be adopted by governments to address these different types of technological risks introduced by AVs. We then explore various governance responses to these risks in different countries. Our analyses reveal that thus far, in most instances governments have avoided stringent measures with the aim of promoting AV developments. As AV developments are still in early stages, the majority of governance responses are non-binding and focused on creating councils or working groups to better explore the implications of AVs at this stage. United States has been active in introducing and enacting AV-specific legislations to address issues related to safety, liability, privacy, and cybersecurity. UK and Germany, in particular, have enacted laws to

[1] Both authors contributed equally to the development of this conference paper.

address liability issues while other countries mostly acknowledge these issues but have yet to implement specific strategies. To address privacy risks, data privacy laws not specific to AVs have been amended in some countries while other countries have decided to rely on existing laws or have made recommendations on privacy principles. Similarly, a wide range of strategies varying from introduction or amendment of non-AV specific legislation to creating working groups and funding research to better explore issues and make recommendations have been adopted. Much less attention has been paid to addressing risks to employment and other issues.

Keywords: autonomous vehicles, automated driving; policy, governance, risks

Introduction

Autonomous vehicles (AVs) have emerged amidst rapid technological advancements and have attracted much attention due to their potential to transform mobility. Companies have begun developing AVs through software investments, conducting AV trials and forming partnerships with university research centres. At current rates of development, Hillier *et al.* (2015) estimate that companies such as Tesla, Volvo, GM, Audi, Mercedes and Nissan will release AVs for sale by 2020, and West (2016) estimates that 25% of the global market will be occupied by AVs by 2040. However, it is unclear whether the full extent of AVs' benefits can be realised and there are concerns regarding the new risks that may emerge. Governance strategies can help to maximise AVs' potential benefits while minimising the risks that often result from adopting new technologies. It is therefore

crucial for governments to balance the strategic desirability of AVs and their associated risks.

Most studies focus on the effects of AVs, such as on transport demand (Milakis *et al*. 2017b; Bierstedt *et al*. 2014), on the economy (Clements and Kockelman 2017) and on safety (Kalra 2017). Few studies have analysed the country-specific policy implications of AVs and governance responses to AVs. Among those that do (Hillier *et al*. 2015; Clark *et al*. 2016; Brodsky 2016) none have categorised government responses as part of a broader framework. This study addresses the following questions: (a) what are the various types of risks associated with AVs? (b) what actions have governments taken to address these risks and how can these responses be categorised and compared?

In the next section, we review the background of AVs before presenting the main risks of AVs. We then highlight and analyse the various strategies adopted by governments to address these risks before the concluding remarks.

AVs

Autonomous vehicles (AVs) are systems that can assess the driving environment and make decisions with little or no human interference (Brodsky 2016; Collingwood 2017). Supplemented with artificial intelligence (AI), sensors, and vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication abilities, AVs can process information, cooperate with other vehicles and handle complex situations, thus enabling AVs to adapt

to changing circumstances much faster than the human driver, (West 2016; Hörl *et al*. 2016).

AVs entail many benefits for society, such as enhancing road safety, mobility, and a nation's competitiveness in the automotive industry (West 2016; Greimel 2016). AVs can help to meet other national objectives, such as resolving labour shortages in the transport sector (Bloomberg 2016), improving fuel economy (Dunne 2016), reducing congestion and reducing pollution (Dunne 2017). On the other hand, AVs entail various risks and, in this article, we examine the governance of technological risks and unintended consequences associated with AVs.

AVs can be categorised according to its degree of automation. The Society of Automotive Engineers (SAE) defines five levels of automation for AVs that is widely adopted. The driver performs all of the dynamic driving tasks at levels 1 (assisted automation) and 2 (partial automation). At level 3 (conditional automation), the driver is expected to control the vehicle occasionally upon warnings. A vehicle is classified as fully autonomous at levels 4 (high automation) and 5 (full automation), but only at level 5 is the vehicle expected to drive itself under all environmental conditions (Milakis *et al*. 2017a). In our study, we focus on interconnected and fully AVs as they represent a greater fundamental shift in society.

AV risks

Widespread acceptance of innovative technologies may be impeded by their associated risks, which includes environmental risk, market risk, social risk, organisational risk,

political risk, financial risk, technological risk, and turbulence risks (Li, Taeihagh and de Jong 2018). We focus on technological risks, which Renn and Benighaus (2013) defines as potentially negative social, physical, and economic consequences of adopting novel technologies. We identified five main types of technological risks associated with AVs: safety, liability, privacy, cybersecurity and industry influence.

1. Safety

While AVs can potentially eliminate human error, the largest cause of car accidents (Kalra 2017), AVs introduce new safety risks. Firstly, there may be more technical errors as the technology grows in complexity. Currently, AVs still face challenges under complex driving conditions due to the possible failures of machine perception, which can cripple situation recognition, safe action planning and action execution (Maurer *et al*. 2015; Kalra 2017). An emerging issue is the design of "crash algorithms", which make decisions during inevitable collisions (Pinsent Masons 2016). Whether the safety of the passenger or the pedestrian should be prioritised, and when, is still unclear. Regulators have not defined a legitimate way of determining the safety of an AV, nor have they agreed on an acceptable level of safety for AVs (Kalra 2017). Over time, AV performance could improve with real-world driving experience, but this requires public acceptance and trading-off short-term safety (Kalra 2017; CSPC 2017).

2. Liability

As human drivers are not in control of AVs (Collingwood 2017), the AV system will bear some or all of the responsibility during accidents. Most legal systems lack clear frameworks to apportion liability between the human driver and the entities involved in the

AV supply chain, which exposes the latter to product liability lawsuits and reputational risks (Pinsent Masons 2016; Hevelke & Rümelin 2015). While event data recorders (EDRs) may be installed to determine liability, this can undermine AV users' privacy (Dhar 2016). Furthermore, liability assignment influences the assignment of insurance costs – if manufacturers are held liable, they may become the "de-facto" insurers against accidents (Bonnefon et al. 2015). High liability and insurance risks can hinder further AV developments in the long-run (Hevelke & Rümelin 2015; Ben-Shahar 2016).

The responsibilities of software programmers who design "crash algorithms" (Pinsent Masons 2016) and whether algorithmic decision-making criteria should be regulated is still unclear. This raises questions about AVs' impact on public ethics, such as whether its algorithms should be embedded with "moral principles" to guide their decisions (Bonnefon et al. 2015) and what criteria should be prioritised in their decision-making (Fleetwood 2017).

3. Privacy

Sensors, maps, cameras and other connected devices in AVs store and transmit data for safety reasons, but this introduces privacy risks (West 2016). Concerns revolve around why information is collected, the types of information collected, information accessibility and the duration of information storage (Collingwood 2017). Possible scenarios of data misuse include tracking AV users (Glancy 2012), selling personal data to third parties (Dhar 2016), harassing AV users through advertising (Lim & Taeihagh 2018) and identity theft (Glancy 2012). Anonymised data, can be easily re-identified through deanonymisation (Narayanan & Shmatikov 2008). Furthermore, customer consent

frameworks are inadequate as customers often accept the terms and conditions without fully understanding them (Schoonmaker 2016). Without privacy safeguards, AVs could facilitate the concentration of information and power over large numbers of individuals, which could also create political concerns (Glancy 2012).

Another privacy risk arises when organisations access the AV's network to conduct surveillance of AV users (Glancy 2012). In AVs that provide transportation services, which are no longer owned by AV users, surveillance may be allowed without legal recourse. Schoonmaker (2016) recommends clarifying whether the AV is considered a "public" space or if a "reasonable expectation of privacy" should be established.

4. Cybersecurity

AVs also introduce risks to cybersecurity, which encompass both privacy and safety (Lim & Taeihagh 2018). These cybersecurity threats exist for both AVs and conventional vehicles with automated features (Lee 2017), where wireless networks can be hacked to manipulate or disorient the vehicle (Lee 2017). For instance, adversaries could inject fake safety messages, alter the AV's map database, or conduct denial of service attacks, which can cause accidents (Petit & Shladover 2014; Dominic *et al*. 2016; Kalra 2017)

Some have argued that AVs are more vulnerable than conventional vehicles to cybersecurity threats as computers possess greater control over the movements of an AV and the driver is less able to intervene during an attack (Petit and Shladover 2014; Lee 2017). The transaction and lifestyle data stored in AVs can be sold for a profit, and their systems could be controlled to inflict physical harm by extremists (Kiss 2016; Lee 2017).

Other attack scenarios using bright lights and radar interference to blind cameras (Petit & Shladover 2014). This was demonstrated by Miller and Valasek in 2013, where they successfully hacked a Jeep Cherokee's collision avoidance system to trick it into thinking it was parking and paralysed it on a highway (Greenberg 2017).

5. Influence on incumbent industries

Apart from the aforementioned risks, AVs potentially disrupt existing professional driving occupations. Autonomous taxis cost significantly less than those with human drivers (Forrest & Konca 2007), and the trucking and delivery industries can accrue approximately $100–500 billion of economic gains from AVs by 2025, most of which will come from eliminating drivers' wages (Forrest & Konca 2007; Clements & Kockelman 2017). These large cost savings are strong incentives for companies to invest in AV technology (Krueger et al. 2016), with significant impacts on employment. While truck drivers can assume other roles, such as monitoring AV systems, these new jobs barely offset the millions lost (Clements & Kockelman 2017). Bus drivers are also at risk as routes with specific designated stopping points are easily automated (Forrest & Konca 2007).

Governance of AV risks

This section presents the strategies taken by various governments to govern the five AV-related technological risks described earlier. We employ a framework developed by Li, Taeihagh and de Jong (2018) and Li et al. (forthcoming) to identify governance strategies,

which are classified as *no-response*, *prevention-oriented*, *control-oriented*, *toleration-oriented* and *adaptation-oriented* strategies (Table 1):

Table 1 Categorisation of governance strategies and AV-related examples (based on Li, Taeihagh and de Jong 2018; Li et al. forthcoming)

Strategy	Definition and AV example
No-response	Policy-makers do not take any specific actions to address risks, and may delay decisions due to their uncertain nature. For example, the US federal government has not taken any measures to address the risk of mass unemployment when AVs displace human drivers in future. In this scenario, policy-makers may not have any back-up plans or robust institutional frameworks to address impending threats. For instance, the criteria and provisions of unemployment insurance have not been amended to incorporate technological unemployment. Furthermore, most governments have yet to outline training programmes specifically for displaced drivers. No-response might also imply that policy-makers are ignorant about the potential negative consequences of risks.
Prevention-oriented	The main aim of this strategy is to avoid risks by taking preventive action. Prohibiting the adoption of innovative technologies is one such display of risk avoidance, as it seeks to prevent the existence of risk. One example is to temporarily prohibit or restrict AV testing on certain routes if a safety concern is identified (PennDOT 2016). This strategy is suitable to address risks of a more predictable nature, but is ineffective when risks are unexpected.
Control-oriented	Policy-makers allow for the existence of risks, but take steps to control them by implementing formal policies and regulations. Traditional methods of risk assessment are adopted to predict and regulate risks. One example is the regulation of safety risks is introducing new geographical parameters for the use of AVs on roads and introducing new eligibility standards for the authorisation of manufacturers to make on-demand automated vehicle networks available to the public (HFA 2016). Another example is imposing a host of requirements on AV testers, such as application requirements, compulsory training programmes and emergency plans (California DMV (2017) article 3.7).
Toleration-oriented	Policy-makers take action to ensure that the system or organisation's performance is robust to risks in a wide range of situations. For instance, the UK government's Vehicle Technology and Aviation Bill (HC Bill 143, 2017) lays out a comprehensive list clarifying the liability of insurers and AV owners in the event of an accident and under a wide range of circumstances. Policy-makers also make forward-looking plans to mitigate potential consequences, such as by developing alternative solutions.
Adaptation-oriented	This strategy aims to improve the adaptive capability of the system or organisation. It emphasises on embracing uncertainty and improving its performance in response to shocks. One example is the Singapore government's intentions to adapt to the employment risks that AVs pose to other industries. The Singapore government intends introduce programmes that retrain future displaced workers progressively, help them acquire new skills and enable them to get higher value-added jobs (Channel News Asia 2017). Here, policymakers view risk as an opportunity to change the system for the better, rather than as a threat that should be ignored, suppressed, controlled or tolerated.

1. Safety

South Korea displays no response towards regulating AV safety issues, whereas Japan's National Police Agency (NPA) released draft AV testing rules in 2017, which will be implemented after the prefectural governments' public safety commissions have revised its

current rules (Japanbullet 2017). Japan's draft rules rely heavily on human oversight to avoid the risk of collisions caused by technical faults, such as requiring police approval and AV testers to always be prepared to apply brakes (Kyodo 2017), reflecting a prevention-oriented strategy.

Governments in Singapore and Germany adopt control-oriented strategies. Germany has integrated the amended 1968 Vienna Convention into its national law in 2016 to legalise AVs, and is also experimenting with AV safety standards (FMEAE 2017). Singapore's Road Traffic Act (RTA) was amended in 2017 to include new AV test rules, such as requiring AVs to pass safety assessments, and for testers to submit accident mitigation plans before road testing (Road Traffic (Amendment) Bill 2017). The Land Transport Authority (LTA) may waive the requirement for a human driver and allow AVs to trial on increasingly complex roads once higher competency is displayed (CNA 2017). Singapore has also created a five-year regulatory sandbox to promote innovation, before enacting further legislation in future.

Some countries adopt light control-oriented strategies. The US and UK released voluntary guidelines for AV testing (NHTSA 2017; DOT 2015), which suggests their intentions to align companies' expectations regarding safety standards without stifling innovation. The EU also pursues a light control-oriented strategy by amending the 1968 Vienna Convention on Road Traffic in 2016 to legalise AVs, and the European Parliament recommends further amending the convention to relax the requirement for a human driver (Pillath 2016). During the Declaration of Amsterdam in 2016, EU Member states have

jointly committed to regulate AVs through regular meetings and maximum collaboration (ERTRAC 2017).

Australia and China adopt a mix of strategies to govern AV safety risks. Both countries adopt light-control oriented strategies – Australia has released safety guidelines for AV testing (NTC 2017b), while China intends to close regulatory gaps by reviewing existing regulation (ERTRAC 2017). These efforts stem from both governments' support for the commercial deployment of AVs (Shaub 2017). Australia also adopts an adaptation-oriented approach by consulting the public to choose one among four regulatory options to address AV safety (NTC 2017c), marking an attempt to build consensus among various stakeholders. China has, instead, pursued a prevention-oriented strategy by imposing requirements that avoid exposing AVs to safety risks, such as temporarily prohibiting AV testing under actual road conditions (Business Sweden 2016).

2. Liability

China, South Korea, the US and the EU have displayed no response in addressing liability and insurance risks of AVs. The US federal government has not created any rules, but urged state governments to take action in allocating liability and vehicle insurance (NHTSA 2017). The EU is still exploring AV liability risks, and the European Parliament made recommendations in 2017 to create a compulsory insurance scheme for victims of AV accidents and making robots legally accountable for accidents (EP 2017; EPCLA 2016).

Germany enacted legislation in 2017 to address AV liability risks, reflecting a control-oriented strategy. The new law mandates installing black boxes in all AVs (Reuters 2016; JDSUPRA 2017) and apportions liability between the human driver and the manufacturer: the latter is made responsible for accidents where the AV system is in charge and a system failure is the main culprit (Reuters 2016). There is, however, ambiguity regarding the "adequate time reserve" that drivers may utilise before taking control of the AV during accidents (JDSUPRA 2017). Germany's Ethics Commission has also published ethical guidelines for AVs, which recommends having appropriate definitions of the driver and outlines which algorithmic decision-making criteria are deemed unethical (FMTDI 2017).

Several governments pursue light control-oriented strategies. Singapore's amended RTA now recognises that entities other than the human driver may be held liable for accidents (CNA 2017), and their General Insurance Association (GIA) has collaborated with the LTA to gather facts on AVs' implications for insurance and its wider developments (Siong 2016). Australia intends to regulate AVs in future by first following a timeframe to clarify definitions of control, review existing laws, and potentially update compulsory injury systems (NTC 2017a). Japan's NPA released guidelines to apportion liability, such as holding the manufacturer responsible for system defects and holding the human driver responsible for operational mistakes (Jiji 2017; Japanbullet 2017). Overall, these efforts reflect a gradual approach towards regulatory reform.

The UK enacted the HC Bill 143 (2017), which clarifies the liability of insurers and AV owners or lessees under a wide range of accident scenarios and thus, represents a toleration-oriented strategy. The bill limits insurers' liability under clearly specified

scenarios where the AV owner caused the accident, and it ensures compensation for AV accident victims by classifying liability involving AV accidents under the existing motor vehicle insurance scheme. In accidents where the AV is defective, manufacturers are not liable as long as the defect did not exist and was not discovered at the time it was supplied (HC Bill 143 2017).

3. Privacy

The UK created key principles for AV privacy and Cybersecurity, reflecting a light control-oriented strategy. The principles recommend that manufacturers follow ISO standards, ensure the proper management of personal information and to enable AV users to delete "sensitive data" (DfT 2017). However, what is considered "proper" management and "sensitive" data is not defined. Considering the UK's plans to lead the world in AV research and development (DfT 2017), these guidelines appear intended to establish expectations around AV privacy standards without stifling innovation. South Korea's amended Vehicle Management Act mandates an approval process before using vehicle data such that vehicle owners' privacy is preserved but lacks explanations of how this will be done (MVMA 2016).

Germany and Australia adopt a mix of strategies. Both countries pursue a light control-oriented strategy by providing guidelines for AV privacy – Germany recommended that entities clarify the types of data that businesses can use and that drivers retain full control over the use of their personal data (Pinsent Masons 2017), while Australia's privacy guidelines suggest following existing privacy principles (NTC 2017c). In addition,

Germany intends to regulate privacy concerns through future legislation (Wacket et al. 2017), suggesting a progression towards a control-oriented strategy. In contrast, Australia adopts an adaptation-oriented approach by holding a public inquiry on AVs' societal impacts, which then recommended investigating the data rights of various stakeholders (NTC 2017a).

Most countries have adopted control-oriented strategies to address privacy risks either in all vehicles or in general. The US SPY Car Act (2017) regulates the data stored in all vehicles. AV owners must be able to terminate data collection and manufacturers cannot use the vehicle's data for marketing or advertising without the AV user's consent. In 2017, Japan amended its Privacy Protection Law (The Japan Times 2017) and China introduced a new Cybersecurity Law to strengthen personal data protection in all systems (KPMG 2016). Singapore also made plans to modify the Personal Data Protection Act (PDPA), and the Public Sector (Governance) Bill was enacted in 2017 to regulate data usage specifically by public agencies (Lim & Taeihagh 2018). Prior to these, the EU ratified the General Data Protection Regulation (EU GDPR) (EU 2016) to regulate privacy and cybersecurity throughout the region. The GDPR protects citizens' rights to review certain algorithmic decisions (Metz 2016), increased penalties for violations (EU 2016) and has demonstrated its commitment by fining Google on several occasions (West 2016). However, it is argued that excessive data regulation may hinder future AV developments and disadvantage European auto manufacturers (Pinsent Masons 2016).

4. Cybersecurity

South Korea, Japan, Australia and Germany adopt a no response strategy in addressing Cybersecurity risks of AVs. South Korea's amended MVMA (2016) lacks provisions on AV cybersecurity, and Japan intends to gather more information before adjusting laws on AV-related liability and Cybersecurity risks (Nikkei Asian Review 2015). In Germany, working groups were created to research AV-related cybersecurity and data protection issues, whereas in Australia, recommendations were made for the National Cybersecurity Strategy to incorporate research into AVs' potential vulnerabilities (SCIISR 2017).

The EU, China and the US adopt control-oriented strategies to address Cybersecurity risks that are not specific to AVs. The EU first introduced the Cybersecurity strategy in 2013, before enacting the NIS Directive in 2016 to regulate cybersecurity (European Commission 2017). The EU Agency for Network and Information Security (ENISA 2016) also made recommendations on methods to strengthen cybersecurity in connected but non-AVs. Similarly, China's Cybersecurity law strengthens the Cybersecurity of all systems. It emphasises on securing critical infrastructure and protecting "national cyberspace sovereignty and security", such as by conducting annual security risk assessments before moving data out of China (Yan 2017). In contrast, the US SPY Car Act (2017) enhances specifically vehicle Cybersecurity by imposing system requirements, such as securing data at all stages of storage and transmission and requiring malfunction detection capabilities in all vehicles. The NHTSA also established a new electronics systems safety research department to analyse vehicle cybersecurity and recommended existing Cybersecurity best practices for AVs (NHTSA 2017).

Singapore adopts a mix of strategies. It amended the Computer Misuse and Cybersecurity Act in 2017 to strengthen businesses' responses to cyber threats (Srikanthan 2017), representing a control-oriented approach. Supplementing this are steps to educate the public of Cybersecurity risks, such as forming partnerships with academia and the private sector. The government views this as an opportunity for Singapore to become a leading cybersecurity service provider (Srikanthan 2017), which reflects an adaptation-oriented approach.

Among the surveyed countries, the UK is the first to focus its efforts purely on an adaption-oriented strategy. The government has attempted to increase the adaptive capacity of the nation in addressing general cyber threats, such as providing cybersecurity principles that recommend designing the AV system to be resilient to attacks during system failures (DfT 2017) and funding projects in the private sector to enhance vehicle safety and to boost the nation's Cybersecurity industry (Chakravarti 2017). These efforts form part of the UK's latest National Cybersecurity Strategy 2016–2021, which aims to enhance citizens' responses to cyber threats and to strengthen UK's position as a world leader in this area by 2021 (Cabinet Office 2016).

5. Influence on incumbent industries

Most governments have displayed no response towards AV-specific employment risks. Australia's SCIISR (2017) acknowledged concerns from organisations such as the Australian Academy of Technology and Engineering regarding the risks that AVs pose to driving occupations and other sectors and recommended transitioning the Australian

workforce as soon as possible. Australia's attempt to gain awareness of these risks represents a light-control oriented strategy. Singapore intends to retrain future displaced workers through skills acquisition programmes to help them to adapt to inevitable disruption (CNA 2017). Instead of viewing AVs as a threat, Singapore's government perceives AVs as economically beneficial by enabling higher productivity, cost savings, and better deployment of manpower resources (Roberts 2016), reflecting an adaptation-oriented strategy towards AV-specific employment risks. AVs can resolve the shortage of bus drivers in Singapore and are being researched as potentially useful for street-cleaning purposes (CAN 2017).

Conclusion

This study examined the strategies taken by various governments in the world to govern AV-related technological risks. We identified the five main risks associated with AVs: safety, liability, privacy, cybersecurity, and the influence on incumbent industries.

To address AV safety risks, most governments tend to avoid imposing overly restrictive regulations to promote innovation. The US, UK and Australia released voluntary guidelines to align expectations about AV safety, China has begun reviewing existing laws, Australia has sought consensus from the public, whereas Germany and Singapore have begun regulating AV safety. All countries, save the UK and Germany, have yet to implement regulations to address AV liability and insurance risks. However, several countries acknowledge the need to update liability laws and have begun reviewing them or

releasing guidelines. Governments have used legislation, guidelines, or consulted the public to address privacy and cybersecurity risks that are mostly not AV-specific. In particular, governments are moving towards formal regulation of general privacy risks, and a minority have taken actions to adapt to general Cybersecurity risks. While little has been done to address other risks, Singapore plans to help displaced workers to adapt to technological disruption, while research exploring AVs' implications for other areas is still emerging.

References

Ben-Shahar, O. (2016). Should Carmakers Be Liable When A Self-Driving Car Crashes? *Forbes*. https://www.forbes.com/sites/omribenshahar/2016/09/22/should-carmakers-be-liable-when-a-self-driving-car-crashes/#1d4eecf448fb

Bierstedt, J., Gooze, A., Gray, C., Peterman, J., Raykin, L., & Walters, J. (2014). Effects of next-generation vehicles on travel demand and highway capacity. *FP Think Working Group*, 10–11.

Bloomberg (2016). SoftBank's self-driving buses are coming soon to Japan's country roads. *The Japan Times*. http://www.japantimes.co.jp/news/2016/09/07/business/tech/softbanks-self-driving-buses-coming-soon-japans-country-roads/#.WVRVJ8ap3-Z.

Bonnefon, J. F., Shariff, A., & Rahwan, I. (2015). Autonomous vehicles need experimental ethics: Are we ready for utilitarian cars?. arXiv preprint arXiv:1510.03346.

Brodsky, J.S. (2016). Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit The Brakes on Self-Driving Cars. *Berkeley Technology Law Journal,* 31(2):851–

878.

Business Sweden (2016). Autonomous Driving & The Next Generation Of Transport In China. https://www.business-sweden.se/contentassets/dfd94f9060af4d499f98de5237bae251/industry-insight---autonomous-driving.pdf

Cabinet Office, National security and intelligence, HM Treasury, and The Rt Hon Philip Hammond MP. (2016). National Cyber Security Strategy 2016–2021. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

CSPC (2017). The Autonomous Vehicle Revolution Fostering Innovation with Smart Regulation. Center for the study of the Presidency and Congress. Washington, D.C.

Chakravarti, S. (2017). Government awards funding to automotive cyber security consortium. *TEISS*. https://teiss.co.uk/2017/04/12/government-awards-funding-car-cyber-security-consortium/

CNA (2017). Regulations in place to ramp up driverless vehicle trials in Singapore. http://www.channelnewsasia.com/news/singapore/regulations-in-place-to-ramp-up-driverless-vehicle-trials-in-sin-7622038

Clark, B., Parkhurst, G. & Ricci, M. (2016). Understanding the Socioeconomic Adoption Scenarios for Autonomous Vehicles. Project Report. The University of the West of England, Bristol. http://eprints.uwe.ac.uk/29134

Clements, L.M. & Kockelman, K.M. (2017). Economic Effects of Automated Vehicles. *Presented at the 96th Annual Meeting of the Transportation Research Board, January 2017.*

Collingwood, L. (2017). Privacy implications and liability issues of autonomous vehicles. Information & Communications Technology Law. 26(1):32–45.

DMV (2017). Department of Motor Vehicles, State of California. Initial Statement of Reasons Title 13, Division 1 Chapter 1. https://www.dmv.ca.gov/portal/wcm/connect/7342a60f-4953-48e4-9372-51abe905913f/avinitialstatementofreasons_31017.pdf?MOD=AJPERES

DfT. (2017). The key principles of vehicle cyber security for connected and automated vehicles. https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles

Dhar, V. (2016). Equity, Safety, and Privacy in the Autonomous Vehicle Era. *Computer*, 49(11):80–83.

Dominic, D., Chhawri, S., Eustice, R.M., Ma, D., & Weimerskirch, A.(2016). Risk Assessment for Cooperative Automated Driving. 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (pp.47-58). https://pdfs.semanticscholar.org/61cc/e71b6ff9e83d6020f48d197ea5d85affc679.pdf

Dunne, M. J. (2016). China Aims To Be No. 1 Globally In EVs, Autonomous Cars By 2030. *Forbes*. https://www.forbes.com/sites/michaeldunne/2016/12/14/chinas-automotive-2030-blueprint-no-1-globally-in-evs-autonomous-cars/#325ed6de1c6e.

Dunne, M. J. (2017). China Deploys Aggressive Mandates To Take Lead In Electric Vehicles. *Forbes*. https://www.forbes.com/sites/michaeldunne/2017/02/28/china-deploys-aggressive-mandates-to-stay-no-1-in-electric-vehicles/#4411d8256a82.

ENISA (2016). Cyber Security and Resilience of smart cars. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

EP (2017). Robots and artificial intelligence: MEPs call for EU-wide liability rules. European Parliament. http://www.europarl.europa.eu/news/en/press-room/20170210IPR61808/robots-and-artificial-intelligence-meps-call-for-eu-wide-liability-rules

EPCLA (2016). Draft report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), European Parliament Committee on Legal Affairs. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-582.443+01+DOC+PDF+V0//EN

ERTRAC (2017). Automated Driving Road Map. *ERTRAC Working Group "Connectivity and Automated Driving"*. http://www.ertrac.org/uploads/images/ERTRAC_Automated_Driving_2017.pdf

EU (2016). GDPR Key Changes. European Union GDPR Portal. https://www.eugdpr.org/key-changes.html

European Commission (2017). The Directive on security of network and information systems (NIS Directive). https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Fleetwood, J. (2017). Public health, ethics, and autonomous vehicles. *American journal of public health*, 107(4):532–537.

FMEAE (2017). Pegasus Research Project. Pegasus, Federal Ministry for Economic Affairs and Energy http://www.pegasus-projekt.info/en/about-PEGASUS

FMTDI (2017). Ethics Commission on Automated Driving press release, Federal Ministry of Transport and Digital Infrastructure https://www.bmvi.de/SharedDocs/EN/PressRelease/2017/084-ethic-commission-report-automated-driving.html

Forrest, A. & Konca, M. (2007). Autonomous Cars and Society. Worcester Polytechnic Institute, Worcester.

Glancy, D.J. (2012). Privacy in Autonomous Vehicles. *Santa Clara Law Review,* 52(4):1171–1239.

Greenberg, A.(2017). Securing driverless cars from hackers is hard. Ask the ex-uber guy who protects them. *Wired*. https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/

Greimel (2016). Japan Inc. steps up autonomous-drive push. *Automotive News*. http://www.autonews.com/article/20161106/OEM06/311079960/japan-inc.-steps-up-autonomous-drive-push

Hevelke, A., & Nida-Rümelin, J. (2015). Responsibility for crashes of autonomous vehicles: an ethical analysis. *Science and engineering ethics*, 21(3):619–630.

Hillier, P., Wright, B., & Damen, P. (2015). Readiness for Self-driving Vehicles in Australia. In Workshop Report, February, ARRB Group Ltd. http://advi.org.au/wp-content/uploads/2016/04/Workshop-Report-Readiness-for-Self-Driving-Vehicles-in-Australia.pdf

HFA (2016). Legislative Analysis Autonomous and Self-Driving Vehicles. *Michigan House Fiscal Agency*. https://www.legislature.mi.gov/documents/2015-2016/billanalysis/House/pdf/2015-HLA-0995-55DA0D6E.pdf

SCIISR (2017). Social issues relating to land-based automated vehicles in Australia. *Parliament of the Commonwealth of Australia*. Canberra. http://www.aph.gov.au/Parliamentary_Business/Committees/House/Industry_Innovation_Science_and_Resources/Driverless_vehicles/Report

Hörl, S., Ciari, F., & Axhausen, K.W. (2016). Recent perspectives on the impact of autonomous vehicles. ETH Zurich, Institute for Transport Planning and Systems.

Japan Bullet. (2017). New Guidelines To Allow Driverless Vehicle Tests On Public Roads. http://www.japanbullet.com/news/new-guidelines-to-allow-driverless-vehicle-tests-on-public-roads

JDSUPRA. (2017). Germany Permits Automated Vehicles. http://www.jdsupra.com/legalnews/germany-permits-automated-vehicles-15610/

Jiji. (2017). Japan sets approval criteria for driverless vehicle road tests. *The Japan Times*. http://www.japantimes.co.jp/news/2017/06/01/business/japan-sets-approval-criteria-driverless-vehicle-road-tests/#.WVRcRcap3-Y

Kalra, N. (2017). Challenges and Approaches to Realising Autonomous Vehicle Safety. Testimony submitted to the House Energy and Commerce Committee, RAND, Santa Monica, California.

Kiss, J. (2016). Your next car will be hacked. Will autonomous vehicles be worth it? *The Guardian*. https://www.theguardian.com/technology/2016/mar/13/autonomous-cars-self-driving-hack-mikko-hypponen-sxsw

KPMG (2017). Overview of China's Cybersecurity Law. *KPMG Advisory Limited.* https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

Krueger, R., Rashidi, T., & Rose, J. (2016). Preferences for Shared Autonomous Vehicles. *Transportation research part C: emerging technologies*, 69:343–355.

Kyodo. (2017). NPA drafts rules for testing driverless cars on public roads. *The Japan Times*. http://www.japantimes.co.jp/news/2017/04/13/national/npa-drafts-rules-testing-driverless-cars-public-roads/#.WVRYVMap3-Y

Lee, C. (2017). Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars. *Federal Communications Law*, 69:25.

Li, Y., Taeihagh, A., & Jong, M. D., Klinke, A. (forthcoming). Reviewing and analysing the rise and spectrum of risk coping strategies – A public policy perspective.

Li, Y., Taeihagh, A., & Jong, M. D. (2018). The Governance of Risks in Ridesharing: A Revelatory Case from Singapore. Energies, 11(5), 1277.

Lim, H. S. M., & Taeihagh, A. (2018). Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications.

Maurer, M., Gerdes, J.C., Lenz, B. and Winner, H.(2015). Autonomous Driving: Technical, Legal and Social Aspects. Springer.

Metz, C. (2016). Artificial Intelligence is setting up the internet for a huge clash with Europe. *Wired*. https://www.wired.com/2016/07/artificial-intelligence-setting-internet-huge-clash-europe/

Milakis, D., van Arem B. & van Wee, B.(2017a). Policy and society related implications of automated driving: A review of literature and directions for future research. *Intelligent Transportation Systems*, 0:1–25.

Milakis, D., Snelder, M., van Arem, B., Homem de Almeida Correia, G., & van Wee, G. P. (2017b). Development and transport implications of automated vehicles in the Netherlands: scenarios for 2030 and 2050. European Journal of Transport and Infrastructure Research, 17(1).

Ministry of Transport (MOT). (2017). Opening Speech by Second Minister for Transport Ng Chee Meng for the Road Traffic (Amendment) Bill Second Reading. https://www.mot.gov.sg/News-Centre/News/2017/Opening-Speech-by-Second-Minister-for-Transport-Ng-Chee-Meng-for-the-Road-Traffic-Amendment-Bill-Second-Reading/

Motor Vehicle Management Act (MVMA). 2016. *Statutes of the Republic of Korea*. http://elaw.klri.re.kr/eng_service/lawView.do?hseq=35841&lang=ENG

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. Presented at *IEEE Symposium on Security and Privacy*.

National Highway Traffic Safety Administration (NHTSA) (2017). Automated Driving Systems 2.0 A Vision for Safety. National Highway Traffic Safety Administration, U.S. Department of Transportation.

National Transport Commission (NTC) (2016). Regulatory reforms for automated vehicles *Policy Paper*

———— (2017a). National Transport Commission submission to the Standing Committee on Industry, Innovation, Science and Resources inquiry into the social issues relating to land-based driverless vehicles in Australia. Melbourne: NTC.

———— (2017b). Guidelines for Trials of Automated Vehicles in Australia. Melbourne: NTC. http://www.ntc.gov.au/Media/Reports/(00F4B0A0-55E9-17E7-BF15-D70F4725A938).pdf

———— (2017c). Regulatory options to assure automated vehicle safety in Australia. Melbourne: NTC. http://www.ntc.gov.au/Media/Reports/(6608D654-9FBD-175D-D067-AC80AECE5FB8).pdf

Nikkei Asian Review (2015). Japan working on law aimed at governing autonomous vehicles. *Nikkei Asian Review*. https://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-working-on-law-aimed-at-governing-autonomous-vehicles

PennDOT (2016). Pennsylvania Autonomous Vehicle Testing Policy: Final Draft Report of the Autonomous Vehicle Policy Task Force. Pennsylvania Department of Transportation.

(http://www.penndot.gov/ProjectAndPrograms/ResearchandTesting/Documents/AV%20Testing%20Policy%20DRAFT%20FINAL%20REPORT.pdf

Petit, J. & Shladover, S.E. (2014). Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):546–556.

Pillath, S. (2016). Automated vehicles in the EU. *EPRS, European Parliamentary Research Service*, *Members' Research Service*, PE 573.902, 2–12. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/573902/EPRS_BRI(2016)573902_EN.pdf

Pinsent Masons. (2016). Connected and Autonomous Vehicles: The emerging legal challenges. https://www.pinsentmasons.com/en/media/publications/connected-and-autonomous-vehicles-the-emerging-legal-challenges/

Pinsent Masons. (2017). German data protection watchdog makes recommendations for autonomous and connected cars. https://www.out-law.com/en/articles/2017/june/german-data-protection-watchdog-makes-recommendations-for-autonomous-and-connected-cars/

Piao, J. & McDonald, M. (2008) Advanced Driver Assistance Systems from Autonomous to Cooperative Approach. *Transport Reviews*, 28(5):659–684.

Renn, O., & Benighaus, C. (2013). Perception of technological risk: Insights from research and lessons for risk communication and management. *Risk Research*, 16(3-4):293–313.

Road Traffic (Amendment) Bill. (2017). http://statutes.agc.gov.sg/aol/search/display/view.w3p;ident=0c04aa1f-50dd-4078-987d-c6733dd67ec8;page=0;query=DocId%3A9fd1d504-52ec-4bf0-bb3b-3bc39a551a85%20Depth%3A0%20ValidTime%3A10%2F01%2F2017%20TransactionTime%3A10%2F01%2F2017%20Status%3Apublished;rec=0

Roberts, F. (2016). Singapore government wants self-driving vehicles to clean the streets. https://internetofbusiness.com/singapore-government-self-driving/

SAE International. (2014). International Standard J3016 Taxonomy and Definitions for Terms related to On-Road Motor Vehicle Automated Driving Systems. https://www.sae.org/misc/pdfs/automated_driving.pdf

Schoonmaker, J. (2016). Proactive privacy for a driverless age, *Information & Communications Technology Law*, 25(2):96–128.

Shaub, M. (2017). China - Speeding towards Self-driving Cars? *Lexology*. http://www.lexology.com/library/detail.aspx?g=1f0737fb-eae3-4e3f-b700-9808684b91b9

Siong, O. (2016). Policies, regulations, liability: Getting on track to a 'driverless future'. *Channel News Asia*. http://www.channelnewsasia.com/news/singapore/policies-regulations-liability-getting-on-track-to-a-driverless--7656084

SPY Car Act (2017), S. 680, 115th United States Congress https://www.congress.gov/bill/115th-congress/senate-bill/680

Srikanthan, T. (2017). Commentary: Cybersecurity is the next economic battleground. http://www.channelnewsasia.com/news/singapore/commentary-cybersecurity-is-the-next-economic-battleground-8591642

The Japan Times. (2017). Amended privacy protection law. The Japan Times. https://www.japantimes.co.jp/opinion/2017/06/01/editorials/amended-privacy-protection-law/#.WrHx-mZ7H-Z

HC Bill 143. (2017). *UK Parliament*. https://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0143/cbill_2016-20170143_en_2.htm#pt1-l1g2

Wacket, M., Escritt, T., & Davis, T. (2017). Germany adopts self-driving vehicles law. Reuters. Retrieved from http://www.reuters.com/article/us-germany-autos-self-driving-idUSKBN1881HY

Watzenig, D., & Horn, M. (2017). Automated driving: Safer and more efficient future driving. Cham: Springer.

West, D. M. (2016). Moving forward: Self-driving vehicles in China, Europe, Japan, Korea, and the United States. https://www.brookings.edu/research/moving-forward-self-driving-vehicles-in-china-europe-japan-korea-and-the-united-states/

Yan, S. (2017). China's new cybersecurity law takes effect today, and many are confused. *CNBC*. https://www.cnbc.com/2017/05/31/chinas- pnew-cybersecurity-law-takes-effect-today.html