ADVI | Australia & New Zealand Driverless Vehicle Initiative

Thought Starter

Connected and Automated Vehicles and Data Use

Introduction

This document provides an overview of the topic to be discussed with the ADVI Hypothetical Webinar on Connected and Automated Vehicles and Data Use. This forms part of a series of hypothetical webinars which ADVI are developing.

Objective

The objective of this paper is to raise awareness of the issues surrounding Connected and Automated Vehicle (CAV) data, including the potential barriers and risks which need to be addressed before the rollout. The intent is to engage thought leaders to encourage discussion on the implications of CAV data and to identify paths forward.

Key questions which need to be asked to address these concerns are: Can we cope with the amount of data generated by CAVs? Will the data be open-access? Who will own the data? Is our digital infrastructure ready for the rollout?

Overview

The protection of personal and sensitive data is more important now than ever before in Australia. With data breach scandals being publicised in the media in recent times, individuals are becoming more aware and concerned about who has access to their data than ever before. How will this issue be addressed now for future deployment?

When CAVs are ready for commercial deployment in the near future, these privacy concerns will present a significant challenge for the Australian Government to resolve. CAVs are expected to generate and store more information than ever before. Will people be willing to purchase CAVs when their personal identifiable information is on the line?

Of concern to consumers will be that there are currently no regulations in Australia for the use of data generated and stored by CAVs. If data privacy concerns are not sufficiently addressed in law, then this will present a significant barrier to the commercial uptake of CAVs. Consumers will need assurances that their personal and sensitive data is protected under law, including how data privacy will be appropriately regulated. What terms of consent will consumers require to override their fears?

What is a Connected and Automated Vehicle?

CAVs involve two components:

- Automated Vehicles
- Cooperative Intelligent Transport Systems

Automated Vehicles are vehicles that have one or more of their primary driving controls (e.g., acceleration, braking and steering) automated for a period of time. There are six levels of driving automation that are defined by the SAE International Standard:

Level 0: No automation. The driver remains in control of the vehicle at all times, with eyes on the road and hands on the steering wheel.

Level 1: Driver assistance. The driver is still in control of the vehicle at all times, with eyes on the road and hands on the steering wheel. However, the vehicle can assist the driver through certain technologies, such as adaptive cruise control or lane centring.

What is a Connected and Automated Vehicle? (Cont.)

Level 2: Partially automated. The driver is still in control of the vehicle at all times, with eyes on the road and hands on the steering wheel. However, the vehicle can assist the driver through certain technologies, such as adaptive cruise control and lane centring.

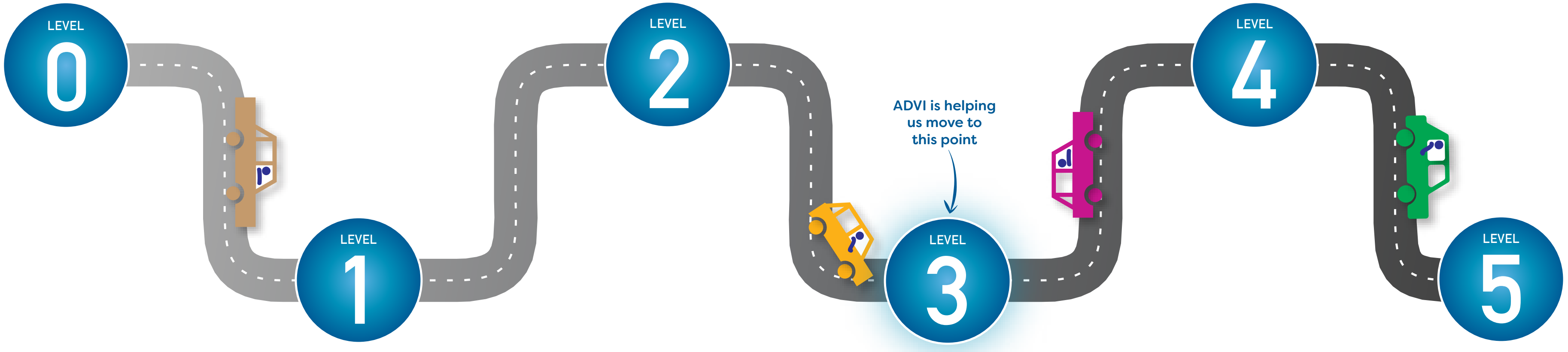
Level 3: Conditionally automated. The vehicle is in control sometimes, with eyes being temporarily off the road and hands temporarily off the steering wheel. However, the driver must remain ready to take over control of the vehicle at any time.

Level 4: Highly automated. The vehicle is in control while the system is in use, with eyes able to be off the road and hands able to be off the steering wheel. Driver intervention is possible but not needed.

Level 5: Fully automated. The vehicle is in control while the system is in use. The driver does not need to be at the steering wheel.

Cooperative Intelligent Transport Systems allow vehicles to become connected to each other (vehicle-to-vehicle) and to the transport network (vehicle-to-infrastructure). In essence, these components of the transport network are able to 'talk' to each other, wirelessly sharing real-time information on road and traffic conditions, etc., to enable a more coordinated flow of traffic along the entire road network.

Combined together, an Automated Vehicle with Cooperative Intelligent Transport Systems is known as a Connected Automated Vehicle or CAV.



ADVI is helping us move to this point

THE PAST
No Automation

Everything is done manually, there's not even power-assisted steering!

THE PAST
Driver Assistance

You complete the majority of the driving task, with assistance for either steering, acceleration or braking.

WHERE WE ARE NOW
Partial Automation

Some automated functions for steering, acceleration and braking - but your hands must still be on the wheel at all times.

2017-2020
Conditional Automation

Hands off the wheel! All aspects of driving are automated - but you must be ready to take back control when prompted.

2020-2025
High Automation

Driver no longer needed! You can take back control if needed, but the car will work fully autonomously.

2026-2030
Full Automation

We won't even need a steering wheel or driver's seat.

Sources:
ERTRAC Automated Driving Roadmap, 21 July 2015 http://www.ertrac.org/uploads/documentsearch/id38/ERTRAC_Automated-Driving-2015.pdf
SAE International's J3016 Levels of Driving Automation, 2014 http://www.sae.org/misc/pdfs/automated_driving.pdf

Core Questions

Can we cope with the amount of data generated by CAVs?

The smart vehicles of today have around 100 sensors, and by 2020 this number is expected to double. This means that the amount of data generated by CAVs by 2020 will be massive enough to be called Big Data. It has even been suggested that CAVs may generate and consume up to 40 terabytes of data per day. In 2017, Intel even estimated that just one million autonomous cars could generate the same data as three billion people.

The sheer volume of data will be such that our current Internet architecture will not be able to cope with the space or bandwidth requirements. Given the importance of real-time processing of this data for safety and traffic management, it is critical that our Internet architecture is able to handle the data generated by CAVs in the future. Will CAV data be stored in the cloud? If so, what are the implications for data sharing and data protection by cloud service providers?

Will the data be open-access?

To improve the availability of data in the transport sector, the Australian government has already made the commitment to provide open-access data to both transport researchers and the general public.

This data is planned to be consolidated and made available through a common portal where it can be accessed for research purposes. However, the availability of this data to the general public raises concerns over privacy and whether even de-identified data can be linked back to a person's identity if multiple data points are made available.

This then raises the question over what kind of data should be available and whether this data should be made truly open-access?

Who will own the data?

Most drivers would assume that the data generated by their vehicle is 100% owned by them. However, this is not the case. As it stands, most of the vehicle's data is owned by the car manufacturer. This is because, when a person signs the contract to purchase their vehicle, they only obtain the right to the vehicle itself, and not the data within the vehicle. But how will this change as CAVs are introduced in the coming years?

Will the right to data ownership become less clear when more stakeholders come into play – cloud service providers, telecommunication service providers, intelligence agencies, map service providers, etc.? In the case of accident, the ownership of the data may be of critical importance, for example police and / or insurers may wish to access the vehicle's data to determine who is at fault.

The European Union implemented new privacy regulations last year called the General Data Protection Regulation (GDPR). Much of the data generated by CAVs will fall within the scope of the new regulation, and the entities which collect and store this data will be required under law to have consent from the driver before using or passing on the de-identified data to third parties.

In essence, under the GDPR, the driver of the CAV will have ownership of the data. At this stage, Australia has no such regulations in place for the protection of data. Should Australia follow the EU or should they take a different approach to data regulations?

Core Questions (cont.)

Uses for the data

Obviously, vehicle manufacturers will very keen to have this data, because it will enable them to continuously improve the safety and performance of vehicles.

However, this is not its only use. Knowing how a driver is acting on the road, where that individual is and matching it with a broader understanding of the customer could be a valuable source of consumer data.

This is particularly the case given that people will be engaged in activities such as watching movies, shopping etcetera while driving. For road agencies, data from CAVs will enable them to significantly improve the efficiency of their management of road networks.

Is our digital infrastructure ready for the rollout?

The current state of our digital infrastructure in Australia is a major challenge to the rollout of CAVs. If our vehicles can't communicate with our roads and other infrastructure, then managing the road network in real-time will be impossible for our road authorities.

For V2I communications to work, the government needs to consider how they will be investing in the technologies required for this rollout. For example, how will they integrate cabling, sensors and transmitters into the existing road network and how will they manage the disruption to the current network that this will cause? V2I communication will also require access to long-range Wi-Fi, mobile data service and mobile satellite communication. How will the government manage reliable connectivity in a country with such an extensive road network which includes mobile data blackspots?

Enhanced connectivity and reliable backup systems are crucial. What are the safety implications if these services fail? The Australian Government is supporting the deployment of 5G networks across the country this year. How will the introduction of the new 5G network change this discussion?

Core Questions (cont.)

Concerns

Community acceptance and public trust over privacy concerns are major barriers to the successful commercial deployment of CAVs and their data collection and storage.

There are a number of scenarios relating to security and CAVs which may weaken community trust. For example, there is the possibility for users of autonomous vehicles to have data relating to their spending and travel habits passed on to advertisers without their permission.

There is also the possibility that personal data could be hacked from a CAV used as a taxi and used in identity theft for financial gain. Alternatively, biometric information used to lock and unlock vehicles through facial recognition software could be hacked and used for other applications, such as logging into bank systems or even unlocking the front door of someone's house.

Already in July 2015, two white-hat hackers demonstrated a security flaw in a Jeep Cherokee, shutting off the engine while the Cherokee was being driven down the highway. More than 1.4 million cars were recalled after that demonstration to have anti-hacking software installed. From a security standpoint, new in-vehicle connected technologies – including laser range finders, cameras, ultrasonic devices, wheel sensors, and inertial measurement systems – could all be used as access points for hackers. Hackers are posing an ever-increasing threat based on their ability to take control of Internet of Thing devices, so with the network connectivity required by CAVs they too could be a target.

There are also risks associated with inadvertent disclosure of information through poor cyber security, such as location information being inadvertently made available online, which do not involve deliberate hacking. The overall benefits offered by CAVs significantly outweigh any costs. However, the above scenarios do serve to demonstrate the seriousness of data security and privacy issues as they relate to CAVs.

Personal vs. sensitive data

There are concerns over the kinds of data collected and stored by CAVs. Personal and sensitive data are likely to be the most concerning kinds of data to the community. But what exactly is personal and sensitive data?

The Privacy Act 1988 defines 'personal information' as:
"...information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a) whether the information or opinion is true or not; and
b) whether the information or opinion is recorded in a material form or not."

The Privacy Act 1988 defines 'sensitive information' as:
"...information about an individual's:

a) race or ethnic origin; or
b) political opinions; or
c) membership of a political association; or
d) religious beliefs or affiliations; or
e) philosophical beliefs; or
f) membership of a professional or trade association; or
g) sexual orientation or practices; or
h) criminal record;
that is also personal information; or
i) health information about an individual; or
j) genetic information about an individual that is not otherwise health information; or
k) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
l) biometric templates."

Majority of data collected by CAVs is expected to be either personal or other data, rather than sensitive data. However, the more sources of information gathered and linked together through other data sets, the more likely it is that an individual can be identified. This presents a privacy concern as to what technologies in CAV are collecting personal or sensitive data.

Data collection technology in CAVs

A diverse range of technologies exist in CAVs, including sensor input units, electronic control units, external cameras, in-cabin cameras, event data recorders, navigation systems, vehicle-to-vehicle and vehicle-to-infrastructure communication, biometric, biological or health sensors, in-cabin microphones and external microphones. Many of these technologies present no more challenge to data privacy than current vehicles available on the market. However, the technologies which may present new data privacy challenges include:

In-cabin cameras

The purpose of internal video recording in CAVs is to monitor the driver for unsafe events, such as distraction and fatigue. The type of data that is collected in this case would be video recording of the driver's face, as well as the location of the vehicle and the vehicle's travel speed.

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication

V2V and V2I communication enables the sharing of information wirelessly between vehicles and the road network on real-time traffic conditions with the overall goal of optimising the performance of the road network. The type of data that is collected here would be vehicle intelligent transportation system station ID, position, speed, direction, class of vehicle, time and critical or emergency events.

Biometric, biological or health sensors

Biometric, biological or health sensors are used in CAV to monitor the status of the driver and how this may impact on their driving. For example, they could be used to monitor distraction, fatigue or intoxication. The type of information collected by these sensors could reveal personal health information, as well as the driver's emotional, cognitive and behavioural state.

Data collection technology in CAVs (cont.)

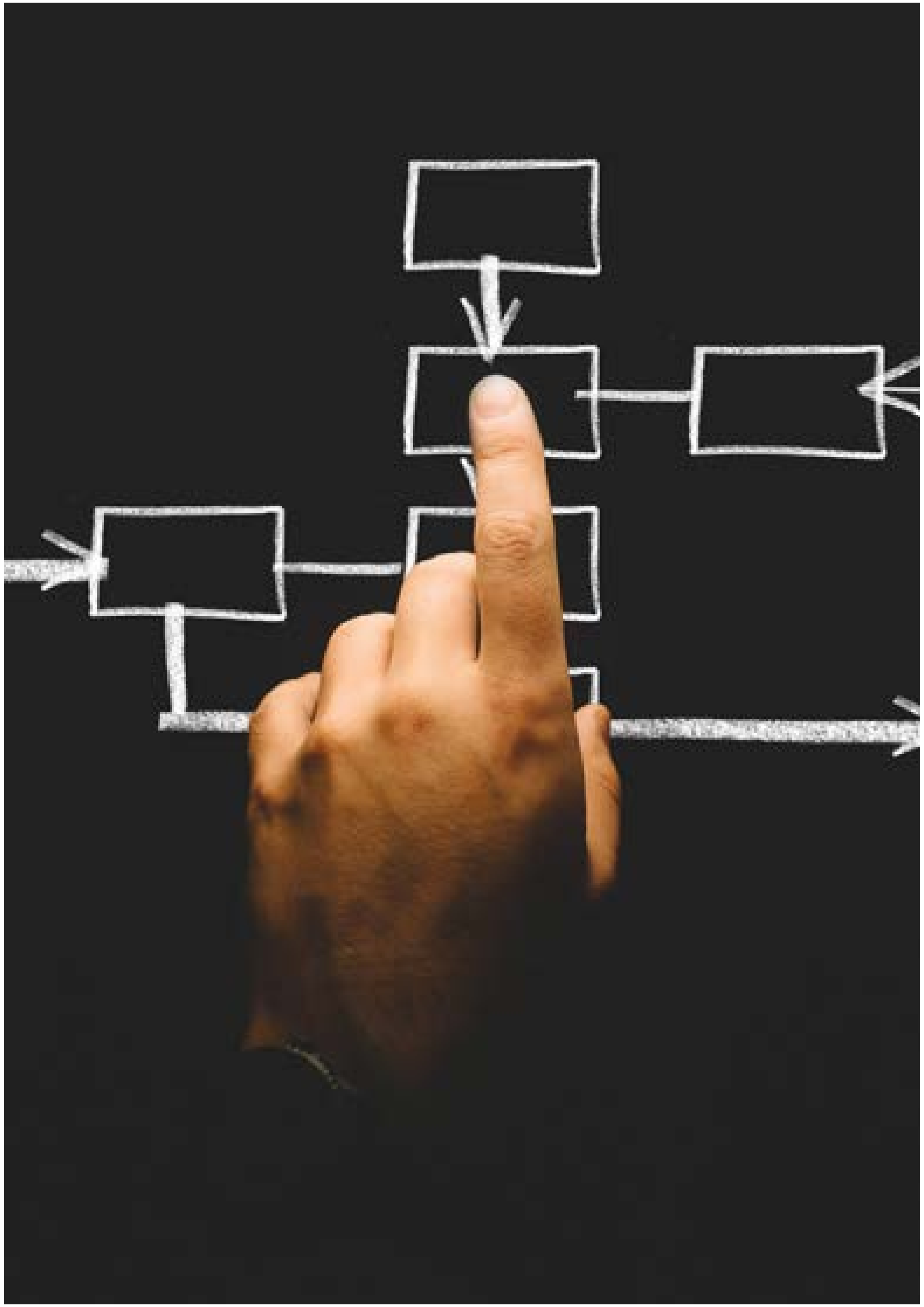
The fact that this personal and sensitive data will be stored and used by both public and private sector entities means that consumers are imparting a level of trust on these entities to keep their data protected. How will their personal information be made safe from cyber-attacks and malicious data mining? How many entities will have access to their data? Consumers will need assurances that their data privacy will not be breached, and this will require careful consideration from the government in terms of the actual rollout of CAVs. It may be that part of this responsibility will fall on the equipment manufacturers to ensure that data remains private. Could ANCAP play a role here too?

Because more data will be generated and stored than ever before, it will become easier for multiple sources of CAV data to be linked together to identify an individual. For example, if biometric sensors detect a heart condition and the driver's location pin points them to a health clinic, this information may be linked together to determine that the driver may be receiving treatment for a heart condition, which could be used by insurance providers to influence the driver's insurance premiums. This would be a major breach of trust if the owners of this data (i.e., private or public sector entities) were to divulge this kind of information to external parties for purposes other than what they were intended for. And because of the breadth and depth of information collected, it would be very difficult for this information to be de-identified.

With these concerns in mind, how can the government successfully manage the risks and unintended consequences of data use in CAVs?

With public trust over privacy concerns being a major barrier to the uptake of CAVs, careful consideration must be given to regulating who can have access to this information. According to the National Transport Commission (NTC), current privacy regulations may not sufficiently address these concerns. This is because current privacy regulations permit government road authorities to collect personal information if that information is deemed necessary for the authority's functions. And while the driver's must be informed that such information is being collected, consent is not necessarily required. However, some regulations surrounding the collection and de-identification of personal information are unclear and differ according to state. Current privacy regulations may not sufficiently address these concerns for the private sector either. Private sector entities are allowed to pass on personal information to government agencies at their discretion. This is especially concerning if more private sector entities end up having access to CAV data than the government.

In most cases, the privacy regulations allow both government and private entities to pass on personal information at their own discretion. A reasonable way forward would be to tighten the privacy regulations so that consumers can be assured that their personal and sensitive information will be protected except in circumstances where there are serious legal reasons for disclosure.



Vision for Resolution

There are several key benefits to addressing the challenges arising from storing and using data from CAVs. These include allowing the government to collect data from the CAV to analyse and improve the road network, optimise traffic flow and improve road safety by analysing driver behaviour. While government road authorities already use data on traffic conditions to improve network operations, receiving this information from CAVs will enable them to manage the network in real-time. Once this data has been received by the road authorities, it can either be used to manage the network directly or it can be provided to road users to alert them of potential hazards along the route.

However, governments will have to balance the need for road agencies to easily and routinely access data from CAVs in real time with security and privacy considerations.

Another potential benefit to CAV data is the ability for police and insurance agencies to determine who was at-fault in the event of a crash or other altercation. CAV data collection is also an enabler of First Notification of Loss (FNOL) capability which has been commonplace in the UK where insurance carriers have used wired telematics for some time. For example, internal and external cameras can capture the sequence of events which lead up to the crash, including both driver's states, any criminal behaviour and who was in control of the vehicle at the time of the crash. For the driver not at-fault, this would give peace-of-mind that the legal and insurance outcomes were correct and fair.

Having greater breadth and depth of data than ever before also means that government road authorities can use this information for infrastructure and network planning. For example, identifying 'hotspots' for crashes to implement safety measures or allocating funding for new infrastructure according to road use patterns.

The reality of moving forward is that the biggest barrier will not be figuring out the technical aspects of the CAV rollout in Australia. It is community trust that will determine how quickly CAVs enter the vehicle fleet. The government needs to ensure that community expectations of data security and privacy are appropriately considered before this can happen.

Government Consultations

The National Transport Commission (NTC) is currently developing options to manage government access to C-ITS and automated vehicle data.

The NTC is undertaking this project as part of its responsibility for establishing end-to-end regulation by 2020 to enable the introduction of autonomous vehicles. In November 2016, Australian transport ministers agreed to a phased reform program so that conditionally automated vehicles can operate safely and legally on our roads before 2020, and highly and fully automated vehicles from 2020.

Information on the NTC's project on C-ITS and automated vehicle data may be found here:

https://www.ntc.gov.au/current-projects/regulating-government-access-to-c-its-and-automated-vehicle-data

Further material and analysis may be found in **The privacy and data protection regulatory framework for C-ITS and AV systems: Report for the National Transport Commission** written by The Allens Hub for Technology, Law and Innovation for the NTC.

Based on the feedback received during this consultation, the NTC will develop recommendations and next steps to implement the recommendations for the Transport and Infrastructure Council meeting, to be held in August 2019.

Overseas developments

In March 2019, Singapore released Technical Reference 68 (TR68) that provides provisional national standards to guide the industry in the development and deployment of fully autonomous vehicles. Section 3 of TR68 addresses cybersecurity principles and assessment.

While TR68 relates to cyber security as opposed to use of data per se, it may still be relevant Australia's policy development in this space. In August 2017, the UK government released **The key principles of vehicle cyber security for connected and automated vehicles**, comprising eight main principles, with sub-principles.

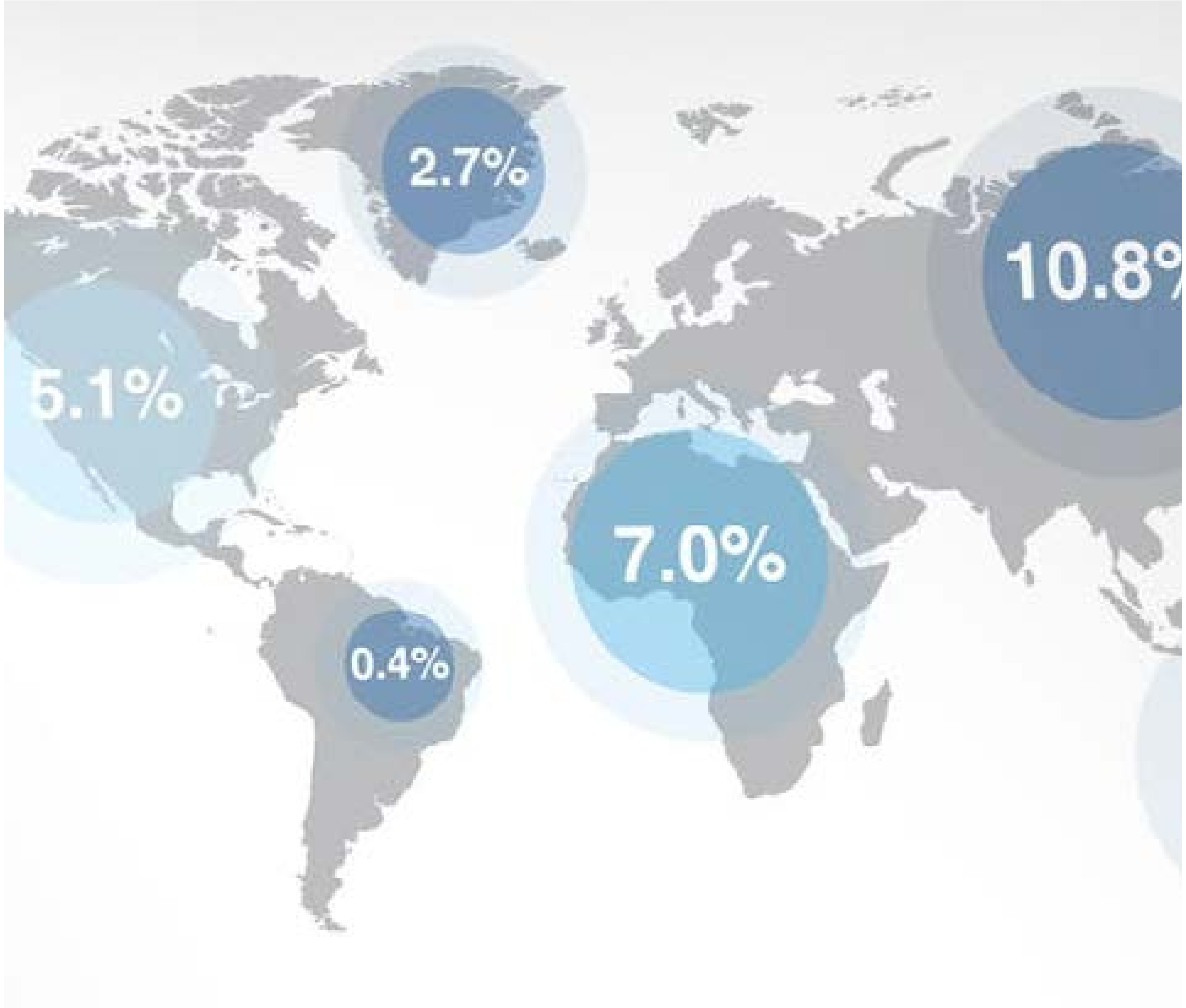
The US's **Self Drive Act**, which was passed by Congress and is currently being considered by the Senate, requires that automakers set up "a process for identifying and mitigating 'reasonably foreseeable' vulnerabilities," and "have cybersecurity managers, training, and intrusion prevention and response systems in place."

Some observers have declared that the UK and US approaches are overly vague, while others believe they are appropriate given that rapid technological developments render a more prescriptive approach problematic.

The European Commission is apparently considering going even further with its regulation. Under its **e-Privacy Regulation** it could force manufacturers to use a privacy-by-design approach to building cars. Ultimately, this would mean data in cars is seen as "personal information," which could draw very significant fines if automotive companies lost it.

Dangers in lack of consistency

There may be a potential danger in different jurisdictions adopting diverging approaches to CAVs and data, with a resulting lack of consistency. Ultimately, this could impose additional costs on consumers, as CAVs may have to be differently configured for different markets. This could particularly be an issue of for relatively small markets like Australia, given that it is likely that CAVs would be designed / set up with larger markets in mind.



Want more infomation?

find out more at: www.advi.org.au

ADVI | **Australia & New Zealand** *Driverless Vehicle Initiative*