

Telecommunications Legislation and Connected Vehicles

Discussion Paper

October 2023

Contents

Purpose	3
Executive Summary	3
What are CAVs?	4
Connected Vehicles	4
Automated Vehicles	6
Connected and automated vehicles	6
How Vehicles Connect.....	6
The framework for connected vehicles	6
Connected vehicles and the telecommunications market	8
How the Regulations apply currently	10
How should we regulate?	11
Questions for stakeholders.....	14
Appendix 1	16

Purpose

This paper queries how the telecommunications law should apply to connected and automated motor vehicles (CAVs).¹ The Department would like to better understand how the connectivity of these vehicles intersects with telecommunications infrastructure and consider how they should be regulated under the telecommunications law.

The information collected in response to this paper will help the Department in its advice to Government about whether it is desirable to make amendments to telecommunications regulatory settings that could improve regulatory certainty around vehicle connectivity, allow for greater competition and innovation in the marketplace and address any potential gaps in the regulatory framework that could impact consumers or the national interest. We will also consider whether existing key definitions and exemption-making mechanisms in the telecommunications law are well-adapted to the task of managing innovations such as CAVs in the market.

Executive Summary

The global connected vehicle market is expected to grow from US\$42.1 billion (AUD\$61.3 billion) in 2015 to US\$122.51 billion (AUD\$181.76 billion) by the end of 2023.² The Asia-Pacific connected vehicle market alone is expected to reach US\$47.4 billion (AUD\$70.32 billion) by the end of 2023.³ The global autonomous driving market is forecast to be worth US\$173.15 billion (AUD\$256.96 billion) by 2030.⁴

Connected vehicles, and increasingly, automated vehicles, are accessing telecommunications infrastructure to connect to other vehicles, infrastructure and the internet. This connection, as well as the increasing use of SIMs and modems in vehicles to facilitate access, and the movement of data across telecommunications infrastructure raises questions about which entities in this market are Carriage Service Providers (CSPs) or Carriage Service Intermediaries (CSIs), along with the extent to which the standard obligations associated with those definitions should apply to particular parts of the industry.

This paper explores this, as well as other questions, by providing a brief overview of CAV technology, the different ways connected vehicles use telecommunications infrastructure and how the current regulatory arrangements apply. The paper questions whether the current arrangements are appropriate, and whether they need to be changed to better acknowledge the complexities of the CAV environment. In doing so, the application of the fundamental regulatory definitions is discussed in the context of whether there are potential gaps and cases of regulatory overreach.

Finally, the paper raises a series of potential questions for stakeholders. The responses to such questions would assist the Government to consider what reform is necessary to accommodate the increasing prevalence of vehicle connectivity.

¹ Connected vehicles use information and communication technologies to communicate with the driver, other road users, roadside infrastructure and other wireless services. Source: [Connected and automated vehicles | Department of Infrastructure, Transport, Regional Development, Communications and the Arts](#)

² [Connected Vehicle Market Trends 2023 Size Equity, Competitive Landscape, Key Factors, Regional Segments and Forecast to 2030 - MarketWatch](#)

³ [Asia-Pacific Connected Vehicle Market Size 2023 Demands Status, Strategies and Key Dynamics Forecast to 2030 - MarketWatch](#)

⁴ [Connected and Automated Vehicles | Future Transport and Mobility \(austrade.gov.au\)](#)

What are CAVs?

Connected Vehicles

Connected vehicles use information and communications technologies to share data and communicate with the driver, other road users, roadside infrastructure and other wireless services.⁵

There are multiple ways a vehicle can be connected to its surroundings and communicate with them:⁶

1. **Embedded Mobile Connectivity** – This involves creating an internet connection through a SIM and modem and can be built into the vehicle or added after purchase. This technology is already in the Australian market, but not yet widespread.
2. **C-ITS connectivity** – Co-Operative Intelligent Transport Systems (C-ITS) use both long range and short range communication, either through mobile network infrastructure or via direct wireless communications, thus allowing vehicle to infrastructure (V2I), vehicle to vehicle (V2V) or vehicle to everything (V2X) connectivity. This technology is likely to be in the Australian market in the near future.
3. **Telematics** – Vehicle telemetry uses a vehicle's embedded mobile connectivity to send data generated by sensors within the vehicle to the manufacturer via existing mobile networks. This technology is already in the Australian market.
4. **eCall or similar** – Some vehicle manufacturers are offering automated crash notification services in the Australian market via their own call centres, but this is not widespread. eCall is mandated in the EU and uses mobile infrastructure to call emergency services when activated. Data from the vehicle is transmitted to emergency services as part of this service.
5. **Connectivity through existing consumer devices** – Devices such as smartphones or satnavs can connect to a vehicle via Bluetooth or USB, and access existing mobile or satellite networks independently to the vehicle. This type of technology is currently in the Australian market but is not being considered as part of this paper, as these are examples of people bringing existing mobile or satellite connectivity to the vehicle.

Not all vehicle connectivity necessarily draws the attention of CSP/CSI obligations under the *Telecommunications Act 1997* (Tel Act). For the purposes of this paper, the Department's concerns are focused on built in telecommunications units that *facilitate access* to telecommunications networks to transmit and receive information, such as embedded mobile connectivity and C-ITS connectivity. It may also include eCall functions. Figure 1 below shows the typical telematic architecture.

⁵ [Connected and automated vehicles | Department of Infrastructure, Transport, Regional Development, Communications and the Arts](#)

⁶ [Connected car - Wikipedia](#). It should be noted that connectivity listed is not mutually exclusive, and will often overlap with other types of connectivity (e.g. V2P will incorporate V2V and V2I connectivity, as well as connecting to pedestrians).

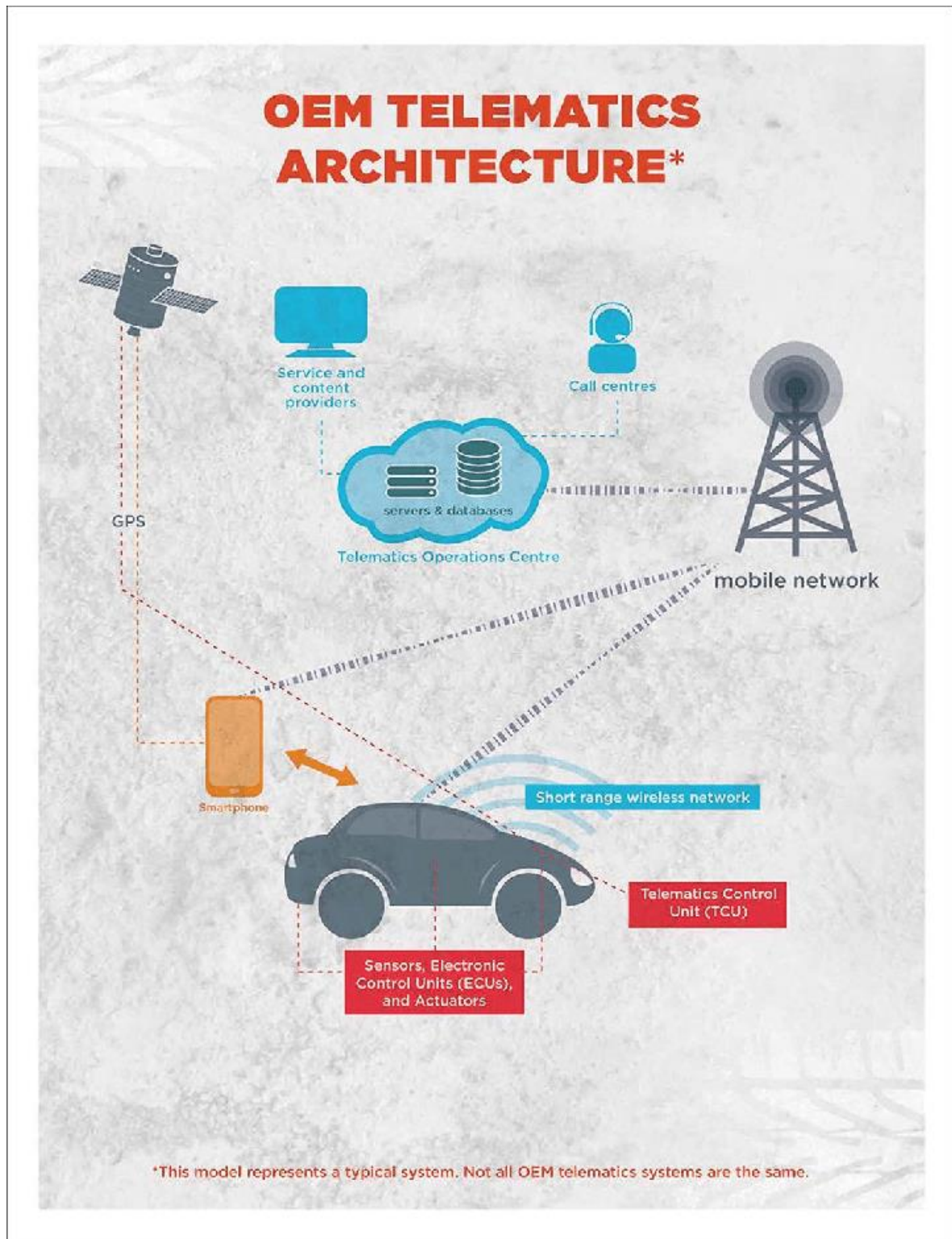


Figure 1: Typical telematic architecture used by connected vehicles.⁷

⁷ [A typical telematics architecture in a connected vehicle. | Download Scientific Diagram \(researchgate.net\)](#)

Automated Vehicles

Automated vehicles have an automated driving system (ADS) - that is, a system of hardware and software collectively capable of performing the entire dynamic driving task on a sustained basis without human input.

Vehicles are classified into six different levels, according to a taxonomy developed by the Society of Automotive Engineers (SAE). Automation levels are based on the amount of human input required to operate the vehicle, from Level 0 (driver must perform all driving tasks) to Level 5 (vehicle can drive itself without any human involvement).⁸

Connected and automated vehicles

Vehicles are likely to become connected before they become automated, but in the future vehicles are expected to be both. CAVs are vehicles that are equipped with ADSs and use information and communications technologies to share data and communicate with other vehicles, other road users, roadside infrastructure and other wireless services.

Connectivity is increasing in vehicles, with 93 per cent of new passenger vehicles forecast to have embedded mobile connectivity by 2031, and 25 per cent of new vehicles to have C-ITS connectivity.⁹ Highly automated vehicles are being developed but are not yet able to legally operate on Australian public roads (although on-road testing is currently available, subject to stringent rules). Passenger vehicles capable of highly automated driving (early operational design domains) are forecast to form 2 per cent of new car sales by 2031.¹⁰

It is unclear to what extent connectivity will be embedded in key automated vehicle systems like steering and braking, and therefore the extent to which CAVs will rely on connectivity to drive safely. However, C-ITS connectivity is expected to help CAVs undertake cooperative manoeuvres in the future.

This paper uses the term 'connected vehicle' to refer to a vehicle with some form of connectivity, whether or not the vehicle is also automated.

How Vehicles Connect

The framework for connected vehicles

Embedded Mobile Connectivity

Typically, connected vehicles can be divided into vehicles with either a built-in or a brought-in connection system. A built-in system commonly uses a proprietary internet connection via a global eSIM and modem that is integrated into the vehicle's IT system. A brought-in system is an after-market device that usually plugs into the vehicle's on-board diagnostics system. It then uses either the customer's smartphone or a proprietary internet connection via a SIM and modem.

⁸ [Connected and automated vehicles | Department of Infrastructure, Transport, Regional Development, Communications and the Arts](#)

⁹ [AP-R654-21 | Austroads](#), p. 27 & 28

¹⁰ [AP-R654-21 | Austroads](#), p. 17-19

C-ITS

There are currently two non-compatible and non-interoperable C-ITS systems, despite widespread preference for a globally consistent solution.¹¹

- DSRC - uses an IEEE 802.11p protocol (an extension of the common Wi-Fi standard) to facilitate the real-time, precise, and trustworthy transmission of safety messages within a range of typically 400 meters, between vehicles and Roadside Units (RSUs).
- Cellular V2X – supports both direct communication in the 5.9GHz ITS band and communication via cellular base stations using LTE or 5G. It is expected that this will provide enhanced performance in non-line-of-sight scenarios and provide high-capacity data transmission.

Example: embedded or after-market vehicle connectivity

A vehicle may have a SIM and modem embedded during the manufacturing process, or plugged in after purchase. A user interface such as an app is linked to the modem, an account is set up, and the vehicle becomes activated. To facilitate connected vehicle services, data is sent from the vehicle's connection system through local mobile infrastructure to a contracted overseas carrier, then to company servers for analysis. Information can then be sent back to the vehicle or the end-user through those same networks, or to a third party company, such as the vehicle manufacturer/distributor. Vehicle connectivity is usually offered on a subscription basis, although third parties may also arrange for connectivity in return for access to the vehicle data.

The following data may be sent from the vehicle via connected services:

(a) before activation, vehicle identification number (VIN); Electronic Serial Number of the modem; SIM serial number; diagnostic and maintenance data;

(b) after activation, data on how the vehicle is operated and used (e.g. use of steering, acceleration, seat belt status, operation of internal controls);

(c) Wi-Fi and mobile network connection; software and firmware versions of vehicle systems; performance and use of systems and vehicle cabin technology such as navigation, infotainment systems, phone/Bluetooth pairings, climate control, seat position; connectivity setting changes;

(d) real time latitude and longitude of the vehicle; and

(e) software updates.

From a regulatory perspective, most vehicle connectivity is governed by distributors arranging for ongoing contractual arrangements with established CSPs for access to mobile infrastructure for the transfer and analysis of data to and from the vehicle. This makes those distributors CSIs, and hence CSPs under the Tel Act (s87(5)). While it is possible to exempt individuals and specific classes from CSP obligations under s95 of the Tel Act, there may be obligations that should continue to apply to connected vehicle services. These could be managed through amendments to regulations specifying connected vehicle services and the obligations that should apply, or through a s96 exemption, which would allow specific obligations to be exempted for a class.

¹¹ [Connected vehicles | Transport and motoring | Queensland Government \(www.qld.gov.au\)](http://www.qld.gov.au)

Example: emergency call systems

Some connected vehicles have an emergency call (eCall) system. This system may be provided for free or as part of a subscription. In the event of an accident, the car connects to an emergency call centre and transmits the GPS position, driving direction and number of passengers, and notifies emergency services if the passengers cannot be contacted. Outside of collisions, eCalls can also be triggered manually via a button if, for example, there is a medical emergency. eCall technology has been mandated for all new vehicles and light vans in the EU since 2018.

CSPs who offer eCall features may be subjected to further regulatory obligations. Part 8 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999 (TCPSS Act)* requires the Australian Communications and Media Authority (ACMA) to make a determination imposing requirements on CSPs (among others) in relation to emergency call services. The ACMA must consider a number of objectives in making these determinations, including that access to the eCall service should be free of charge to the end-user and to the emergency service organisation.

Vehicle eCall systems could meet the definition of a standard telephone service under the *TCPSS Act*, despite them not being a traditional phone service.¹² Suppliers of standard telephone services are subject to a host of regulatory requirements that would be imposed on the CSP alongside their ordinary CSP obligations. If the ACMA were to adopt this view, they would be required to make a determination. eCall subscriptions may contravene such a determination, unless the ACMA considered it unreasonable for CSPs to provide free eCall services.

Connected vehicles and the telecommunications market

Companies selling connected vehicles generally contract with a telecommunications network provider¹³ ('provider') to manage connection with the internet, and to provide the connection system (i.e. modem and SIM). These providers, often based overseas, contract with Australian MNOs to carry data from the overseas provider to the vehicle. The local MNOs are CSIs because they provide the carriage service that the vehicle seller has contracted to provide with a third party.¹⁴ The overseas provider then carries the data to servers (ostensibly servers belonging to the company selling the vehicle connection) to be processed or analysed. That data is then sent either back to the vehicle, or to a third party (i.e. a fleet manager). These interactions are shown in figure 2 below.

¹² Section 6 of the *TCPSS Act* defines a standard telephone service as a carriage service for the purpose of voice telephony where an end-user supplied with the service is ordinarily able to communicate, by means of the service, with each other end-user who is supplied with the same service for the same purpose, whether or not the end-users are connected to the same telecommunications network.

¹³ This paper uses the term *telecommunications network provider* for these providers rather than the catch all term 'carrier'. This is due to the Tel Act defining a carrier as 'the holder of a carrier licence' (Section 7). As these providers may be based overseas and may not hold an Australian carrier licence, we have opted not to use the term carrier.

¹⁴ Section 87(5) of the Tel Act provides that a CSI is a CSP for the purposes of the Tel Act.

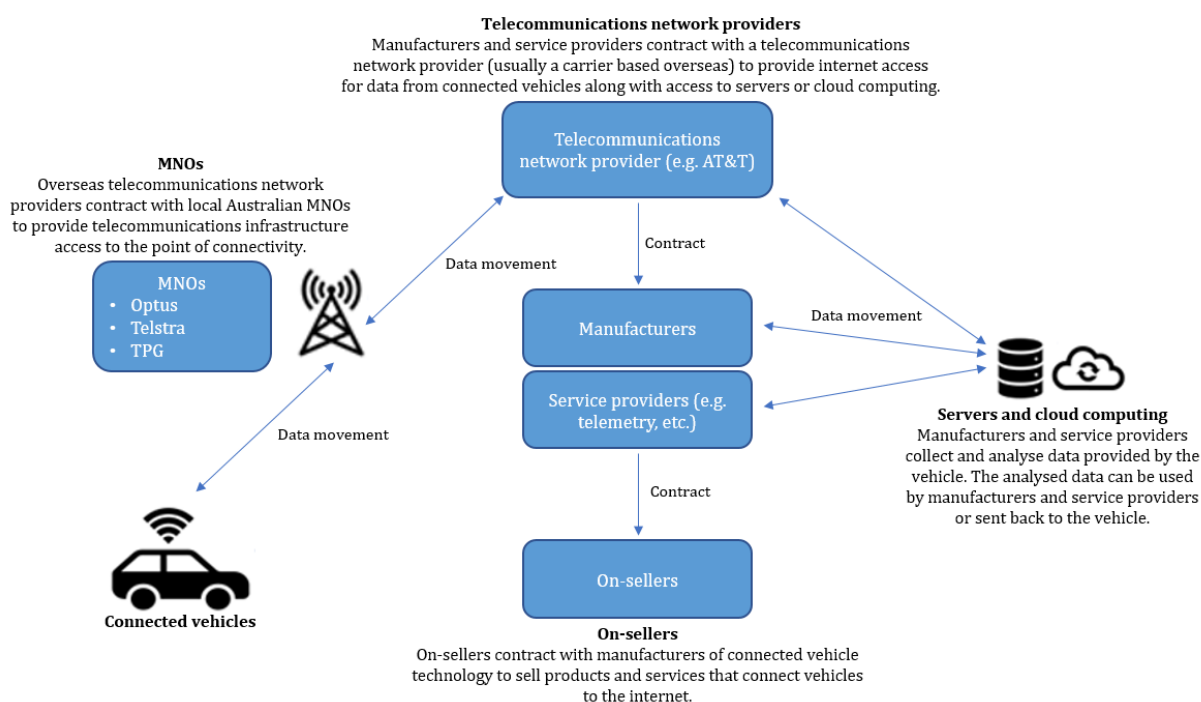


Figure 2: Interactions that facilitate connected vehicle services.

The Department has received several requests from distributors of connected vehicles and related products to be exempted from CSP obligations under section 95¹⁵ of the Tel Act. The arguments for exemptions generally acknowledge that while the distributor may be a CSP (usually by being a CSI), they do not believe that they were meant to be caught by the telecommunications framework and that they do not have the necessary resources to comply with obligations.

A common query is what difference there is between a market selling a pre-paid SIM card, and what distributors and manufacturers are proposing to do (i.e., selling a modem and SIM that plugs into, or is built into, a vehicle). While the market is a part of the transaction, it is merely an intermediary in the supply chain. Once the transaction is completed, that seller no longer has any relationship with the purchaser in regards to that SIM, such as support, or taking complaints about service. With CAVs, there is often an ongoing relationship between the manufacturer/distributor and the consumer, either through invoicing, being the first point of contact for assistance or accessing the vehicle’s telemetric data for business purposes.

Given the nature of connected vehicles and their interaction with telecommunications infrastructure, along with significant growth in the connected vehicle market, clarification around which, if any, obligations apply to distributors of connected vehicles (or vehicle connectivity) is needed to provide certainty to industry and end-consumers. It is anticipated that all members of the Federal Chamber of Automotive Industries have, or will have in the near future, connected vehicles that may give rise to obligations as CSPs.

¹⁵ Section 95 allows the Minister to exempt a specified carriage service or a specified person from a specified eligible definition provision. In this instance, exempting an entity from being a CSP/CSI.

How the Regulations apply currently

Over 30 types of obligations under the telecommunications law fall within four broad groups: competition, consumer protection, national interest and universal services. These are listed in **Appendix 1** for reference. Those obligations attach to two types of regulated entities: 'carriers' and 'carriage service providers'.

Carriers

Under the Tel Act, carriers are entities that have a carrier licence. A network unit cannot be used to supply a carriage service to the public, unless the owner of the network unit holds a carrier licence, or there is a nominated carrier declaration in place in relation to the network unit, or an exemption applies.¹⁶ Communications networks within individual businesses are not considered 'supply to the public' and fall outside the regulatory scope.¹⁷ There are four types of network units: single or multiple line links connecting distinct places in Australia, designated radiocommunications facilities or a facility specified in a Ministerial determination.

Carriage service providers

A CSP is a person who supplies a listed carriage service.¹⁸ A listed carriage service is a service for carrying (including transmitting, switching and receiving) communications (in essence, any form of signal) by means of electromagnetic energy between points in Australia, or a point inside Australia and another point outside Australia.¹⁹ The activities of CSPs are regulated.

CSPs supply carriage services but do not necessarily own physical telecommunications transmission infrastructure. The definition is broad and open ended, covering persons supplying listed carriage services to the public using network units owned by carriers (and nominated carriers). This includes international CSPs, who provide carriage services either between points inside and outside of Australia using a line link, or via a satellite-based facility.²⁰

A CSI is a subset category of a CSP. A CSI is a person who arranges the supply of a carriage service by a CSP to a third person. A commercial relationship exists between these parties relating to the continuing supply of the service.²¹

A Content Service Provider is a person who uses a listed carriage service to supply a content service to the public.²² Connected vehicle distributors or service providers may become Content Service Providers if they provide certain services over the vehicle's connection. The telecommunications regulatory regime regulates the activities of CSPs and Content Service Providers.

¹⁶ Tel Act s 42.

¹⁷ Such networks are referred to as communications within the 'immediate circle' of the owner of the network units, and are not considered 'supply to the public' under section 44 of the Tel Act.

¹⁸ Tel Act s 87.

¹⁹ Tel Act ss 7, 16. A listed carriage service is a carriage service between: a point in Australia and one or more points in Australia; a point and one or more other points, where the first-mentioned point is in Australia and at least one of the other points is outside Australia; or a point and one or more other points, where the first-mentioned point is outside Australia and at least one of the other points is in Australia.

²⁰ Tel Act s 87(2).

²¹ Tel Act s 87(5).

²² Tel Act 97. It is understood that this provision has yet to be used.

How should we regulate?

Current arrangements

The telecommunications regulatory framework currently captures connected vehicle manufacturers and distributors, or those who arrange for vehicle connectivity as CSIs (and hence a CSP under the Tel Act) – that is, they have arranged for the ongoing supply of a carriage service by a CSP to a third person. CSPs are subject to obligations in relation to consumer safeguards, security matters, and telecommunications-specific competition restraints. CSPs do not need a licence but are expected to understand and comply with their obligations.²³

It is highly likely that the roadside units used for direct, short range C-ITS communications between vehicles and infrastructure would be considered a network unit and would require the owners of those units to have either a carrier licence, or a nominated carrier declaration to supply that service to vehicles. This could lead to government entities becoming ‘carriers’ under the Tel Act.²⁴

Carriers are subject to a range of other obligations, beyond those required for CSPs. Entities involved in the creation of C-ITS communications networks will need to be aware of any licencing or other obligations related to the ownership and use of those networks. This work is outside the scope of this particular discussion.

Anti-competitive conduct obligations

Under the *Competition and Consumer Act 2010 (CCA)*, CSPs are subject to both a framework that prohibits anti-competitive behaviour²⁵ and a telecommunications access framework.²⁶ These operate alongside general competition protections in Part IV of the *CCA*. There are questions as to whether existing general competition protections are sufficient in the context of connected vehicles.

We are interested in views from stakeholders as to whether there are competition issues that have arisen or are likely to arise in relation to connected vehicles. For example, while currently vehicle manufacturers and the carriers they use are separate entities, competition issues could arise if vehicle companies and the corporate groups to which they are part of start to own or control other parts of the telecommunications ecosystem, possibly bringing these entities into the scope of a ‘telecommunications market’.²⁷

²³ As a general rule, where a CSP does not provide a service that is subject to an obligation, they do not need to fulfil the obligation related to that service.

²⁴ NB: C-V2X can enable short range communication through mobile infrastructure, however DSRC does not. As mentioned previously, ownership of network units and their use in the supply of a carriage service requires either a carrier licence or a nominated carrier declaration. If C-ITS were to require the deployment of specialised units to enable connectivity, then the owners of those units would require a carrier licence and hence be classified as carriers, a definition that could potentially capture government entities if those entities built and maintained ownership of the C-ITS infrastructure.

²⁵ Part XIB sets up a regime for regulating anti-competitive conduct in the telecommunications industry.

²⁶ Part XIC allows the ACCC to declare a service. Carriers and CSPs who provide declared services are required to comply with *standard access obligations* in relation to those services. The *standard access obligations* facilitate the provision of access to declared services by service providers so that service providers can provide carriage services and/or content services.

²⁷ *CCA* s 151AF. A telecommunications market is one in which carriage services, goods or services for use in connection with a carriage service, facility access, or content services are supplied or acquired. It could be argued that a vehicle intended to be connected to a carriage service such as the internet, and any ongoing services that require the use of a carriage service is a ‘goods and service.’

Further, related corporate entities may respectively own a connected vehicle manufacturer, and a telecommunications company (either a traditional MNO or a Low Earth Orbit (LEO) satellite company). Conceivably these companies could combine their products to create a potential competition bottleneck, where purchasers of these connected vehicles could only maintain connectivity through their telecommunications infrastructure.

We note that the *CCA* has both general and telecommunications-specific anti-competitive conduct provisions, in Parts IV and XIB respectively. We are interested in views as to whether there would be advantages or disadvantages to connected vehicles being captured by telecommunications-specific anti-competitive conduct provisions.

Along with those frameworks, which aim to prevent monopolistic behaviour and prevent activities that would substantially lessen competition in a telecommunications market, there are three other categories of obligations that face CSPs. These are detailed below.

Consumer protection obligations

Australian Consumer Law: The Australian Consumer Law²⁸ includes general provisions that may extend to connected vehicles. These include prohibitions on misleading and deceptive conduct and unfair contract terms, protections against unfair practices (including pricing, false and misleading representations, and harassment and coercion) and consumer guarantees relating to the supply of goods and services. The Minister may also make information standards related to goods or services of a particular kind.

Telecommunications Consumer Protections Code: CSPs are expected to adhere to the Telecommunications Consumer Protections (TCP) Code. The TCP Code provides supplementary consumer protections that operate over and above the general obligations provided in the Australian Consumer Law.

The protections relevant to connected vehicle services include ensuring customers can:

- understand the telecommunications service and its inclusions – by requiring the provision of a critical information summary; and
- understand billing and charges specific to the telecommunications product.

The TCP Code also requires sales representatives to be appropriately trained to help consumers understand the telecommunications products they are purchasing.

Telecommunications Industry Ombudsman scheme: CSPs are obliged to become members of the Telecommunications Industry Ombudsman (TIO) scheme. The TIO is the external dispute resolution body that offers telecommunications consumers and small businesses a pathway to have complaints about their carriage service heard and resolved by an independent organisation if they cannot resolve it directly with the CSP. The ACMA has the discretion to declare that a CSP is exempt from having to join the TIO scheme.²⁹

We are interested in whether there are advantages or disadvantages to imposing these obligations on carriage service intermediaries in the connected vehicle service delivery continuum. Is there a regulatory gap that would justify extending the application of telecommunications consumer protections to these entities beyond those found in Australian

²⁸ *CCA* schedule 2.

²⁹ *TCPSS Act* s 129(1).

Consumer Law? Alternatively, is it efficient or sufficient to impose those obligations on others, like MNOs?

Security obligations

Interception and data retention obligations

Under the *Telecommunications (Interception and Access) Act 1979*, all CSPs must meet mandatory data retention obligations, and ensure that their services can be intercepted in accordance with an interception warrant.

The Communications Access Coordinator (CAC) in the Attorney-General's Department can grant exemptions from these obligations. In considering exemption applications, the CAC must take into account the interests of law enforcement and national security agencies.

In practice, security agencies will typically serve interception notices to the local MNOs that provide the mobile infrastructure that connects to the connected vehicles. As a vehicle will simply connect to the nearest mobile infrastructure, it becomes difficult for security agencies to determine which MNO to serve notice on. This could require them to serve notice on all three MNOs (Telstra, Optus and TPG Telecom), especially where the contracted provider is based overseas.

CSPs are also required to provide notification of critical cyber security incidents as they become aware of them.³⁰

We are interested in views from stakeholders as to whether there are advantages or disadvantages in applying the interception and data retention obligations to carriage service intermediaries in the connected vehicle service delivery continuum. Is there an information or regulatory gap that would justify extending the application of those obligations to these entities? Alternatively, is it efficient or sufficient to impose those obligations on others, like MNOs?

Network security and assistance obligations

CSPs are required to do their best to prevent telecommunications networks and facilities from being used to commit offences, and to do their best to protect telecommunications networks and facilities owned, operated or used by a carrier or CSP from unauthorised interference or unauthorised access.³¹

CSPs must also provide such help as is reasonably necessary to officers and authorities of the Commonwealth and the States and Territories in relation to the enforcement of criminal law and pecuniary penalties, safeguarding national security, protecting public revenue and nationally declared emergencies.³²

We are interested in whether there are advantages or disadvantages to imposing these obligations on carriage service intermediaries in the connected vehicle service delivery continuum. Is there a regulatory or information gap that would justify extending the application of the network security and assistance obligations to these entities? Alternatively, is it efficient or sufficient to impose those obligations on others, like MNOs?

³⁰ *Telecommunications (Carriage Service Provider—Security Information) Determination 2022*, division 2.

³¹ Tel Act part 14.

³² Tel Act s 313.

Information gathering powers of the ACMA

Information gathering powers are necessary for the ACMA to exercise its functions and powers. CSPs are obliged to comply with a number of record keeping obligations. The following thresholds apply to those obligations:

- Telecommunications (Consumer Complaints) Record-Keeping Rules 2018 – rules only apply to providers with a minimum of 30,000 services in operation; and
- Telecommunications (Customer Service Guarantee) Record-Keeping Rules 2011 – rules only apply to providers with a minimum of 100,000 Customer Service Guarantee services.³³

We are interested in whether there are potential advantages from the ACMA information gathering powers applying to providers in the connected vehicle service delivery continuum, or whether the potential regulatory burden outweighs the benefits.

Technical obligations

There are also a number of obligations in the Tel Act of a technical nature, which are largely not relevant to connected vehicles presently. These are listed for completeness:

- Integrated Public Number Database (IPND): CSPs that supply a carriage service to an end user with a public number must provide the public number customer data to the IPND Manager.
- The Numbering Plan: Sets out all the numbers that can be used to supply carriage services to the public and outlines rules for the use of public, and some non-public, numbers.
- Technical regulation—telecommunications standards: Specified customer equipment³⁴ and cabling that comply with applicable technical standards must be labelled with a compliance label. Equipment and cabling that does not meet applicable technical standards must be labelled with a non-compliance label.³⁵
- Obligation to connect: The manager of a network or facility must permit connection of any correctly labelled customer equipment or cabling that also meets the standards required for that equipment or cabling, except where that manager might believe labels have been applied in contravention of the Tel Act, or where there could be a threat to the integrity of a telecommunications network, or to the health and safety of persons affected by the telecommunications network.³⁶

We are interested in views from stakeholders about whether these obligations ought to apply to particular providers in the connected vehicle service delivery continuum.

Questions for stakeholders

In general, connected vehicle manufacturers and after-market providers are subject to the obligations on CSPs. However, it is unclear whether, how or by whom in the supply chain these obligations should be met. The increasing prevalence of connected vehicles and the future of automated vehicles raises questions about how the regulatory framework should define these

³³ This obligation only affects CSPs using landlines and would not be an obligation faced by CAV manufacturers or aftermarket resellers.

³⁴ Tel Act s 21 defines 'customer equipment'. It is likely that the ACMA could make technical standards for CAVs if it chose to do so, or that certain aspects of connected vehicle equipment may need to be compliant with certain telecommunications standards.

³⁵ *Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015*.

³⁶ Tel Act s 413(3).

networks, which obligations should apply, and who ultimately should be responsible for fulfilling those obligations.





In particular, the Department is interested in the implications of data and communications being carried across telecommunications infrastructure in ways that would not previously have been thought of as traditional telecommunications, and whether the obligations required for CSPs easily overlay these non-traditional formats. The Department's initial views are that while this is an emerging technology that does not meet the traditional view of a carriage service, there are still important network safeguards and consumer obligations that should continue to apply to these services and certainty around those obligations and who is responsible for them are necessary to allow this sector to grow.

To that end, the Department seeks to ask the following questions:

- 1. Should companies that distribute connected vehicles (or products that can alter vehicles so they can connect to telecommunications infrastructure for the purpose of transmitting data to and from the vehicle) be categorised as CSPs under current regulations? Or should these companies be exempt from this categorisation? Is it possible for a solution to incorporate future technologies that may have a similar effect?**
- 2. If these companies are not exempted, which obligations should they comply with? Which entity in the overall supply chain should be responsible for those obligations? What would be a feasible mechanism for ensuring obligations are met?**
- 3. Can you envisage upstream and downstream competition issues that would benefit from telecommunications-specific regulation?**
- 4. Would telecommunications-specific consumer protection benefit owners of connected vehicles, or is the general consumer law sufficient?**
- 5. There is a general obligation on Carriers and CSPs to secure their networks and equipment from interference. Can all parts of the network be reasonably protected? Is there anything about connected vehicles that make them particularly vulnerable to attack?**
- 6. CSPs also have obligations requiring them to assist with law enforcement and national security agencies. Is this required assistance already provided for under existing legislation? Is there information or assistance that can be provided by companies that distribute connected vehicles (or products that can alter vehicles so they can connect to telecommunications infrastructure for the purpose of transmitting data to and from the vehicle) that cannot be provided by more 'traditional' Carriers or CSPs?**

The Department is interested in hearing from interested stakeholders on these and other related questions.

Appendix 1

 <p>Competiton</p>	 <p>Consumer</p>	 <p>National Interest</p>	 <p>Universal Services</p>
<ul style="list-style-type: none"> • Access regulation: ACCC regulated terms for services, information and facilities • Wholesale-only and functional separation requirements for residential broadband • Any-to-any connectivity • Non-discrimination • Numbering • Anti-competitive conduct prohibitions • Powers and immunities • NBN-specific requirements (wholesale, line of business, privatisation) 	<ul style="list-style-type: none"> • Codes and Standards • Consumer service guarantee • Network reliability • Spam and telemarketing • Privacy protections • Calling Line Identification • Universal service provision: broadband • Universal service provision: voice • Broadband readiness for new developments • ACMA technical regs • Operator services • Directory services • TIO membership • Do not call / Anti-spam 	<ul style="list-style-type: none"> • Reasonable assistance to government (law enforcement, security, disasters) • Technical assistance to security and law enforcement • Defence and Disaster plan compliance • Interception • Stored communications preservation • Data retention • Physical and cyber security (including submarine cables) • Integrated Public Number Database 	<ul style="list-style-type: none"> • Telecommunications Industry Levy for Universal Service Obligation, national relay service, emergency call service • Regional Broadband Scheme