NRMA ROAD TRAVEL REWARDS

Secure and connected vehicles

Stronger data, privacy and cyber rules in Australia.

August 2026

Contents

About the NRMA

We're one of Australia's largest member-owned organisations, with a 105-year history and more than 3.6 million members. We offer a world of road, travel and rewards that help members live more freely.

We're for members. We're independent.

We are a member-owned organisation, independent and non-partisan by design. We advocate for our members and their communities and engage constructively with governments, stakeholders and industry to help shape fair, practical outcomes that make life better for all Australians.

Our positions are shaped by member experience, research and consultation.

It's an approach we've taken for more than a century, guiding how we advocate for and contribute to practical change that improves safety, affordability and access. By working openly with others, we focus on outcomes that make a real difference for communities across Australia.

Our partners

Irdeto is the world leader in digital platform cybersecurity, enabling businesses to operate, scale and innovate with confidence in an increasingly connected world. With more than 50 years of security expertise, Irdeto delivers integrated solutions and services that protect revenue, safeguard platforms and combat cybercrime across video entertainment, video games and smart mobility.

Data Synergies is a data and technology consultancy led by lawyer and business advisor Peter Leonard, specialising in legal strategy, design, and governance frameworks for artificial intelligence and advanced analytics. Operating across Australia, New Zealand and ASEAN, the firm guides businesses and government agencies through complex data ecosystems by bridging the gap between privacy laws, consumer protection, intellectual property and socially responsible business practices.

enX is a specialist advisory firm focussed on the market participation and grid integration of e-mobility and consumer energy resources. Its work sits at the intersection of energy markets, regulation, customer technology and grid transformation.

The National Institute of Strategic Resilience (NISR) is an Australian independent not-for-profit applied strategy institute focused on strengthening national resilience across critical infrastructure, cybersecurity, supply chains, emerging technology and societal preparedness. NISR works with government, academia, and industry to develop practical initiatives that enhance Australia's long-term resilience and strategic readiness.

NRMA connected vehicle data statement

We support the use of connected vehicle data to improve safety, mobility and services for motorists and the broader community, where vehicle data is handled responsibly, fairly, transparently, and with appropriate safeguards and assurance controls.

Our data handling practices are designed and governed to give effect to our commitment to the responsible and fair use of vehicle data.

Use of non-identifying data

We minimise the collection and handling of vehicle data that identifies vehicles or individuals and primarily analyse and use aggregated or otherwise anonymised (non-identifying) data to inform and support evidence-based advocacy and research.

Reports and insights derived from connected vehicle data assist us in making data-driven recommendations on mobility-related matters, including road safety improvements, transport planning, infrastructure investment and congestion management, particularly in regional and local communities.

Our work in this area is undertaken in collaboration with governments and technical experts and is focused on delivering public-interest outcomes such as safer roads.

Use of identifying vehicle or personal data

Where connected vehicle data that identifies vehicles or individuals is used to support services we provide to our members, we collect, use and retain personal information in accordance with our Privacy Policy, the Privacy Act 1988 (Cth), and the Australian Privacy Principles.

This includes obtaining the prior informed consent of the relevant member, for clearly stated and limited purposes. Members remain in control of whether and how identifying vehicle data is used.

Advocacy for consumer rights

As a member-owned organisation, we also advocate for stronger consumer rights in relation to connected vehicle data collected by vehicle manufacturers, service providers and other third parties using members' vehicles.

This advocacy applies to all entities that collect vehicle data that can reasonably be linked, directly or indirectly, to vehicles or individuals, or otherwise used to influence how individuals are treated.

Our advocacy includes consumer rights of access to this data, meaningful control over its use, and clear, informed consent.

Our approach to vehicle data is grounded in trust, transparency and public benefit, and is consistent with our long-standing role as an independent, member-owned advocate.

NRMA member survey

84%

of members are concerned about cyber security risks.

70%

are unwilling or unlikely to purchase from a brand that trades in their information, including 36% who would definitely not choose that brand and 34% who would consider a different brand.

69%

with connected vehicles lack understanding of how their data is collected and used, while 26% didn't read the T&Cs when purchasing their vehicle.

54%

say data collection and retention by manufacturers would influence their brand choice, with data handling and potential on-selling having a significant impact on choice.

84%

would be somewhat or very likely to avoid a brand in the future if it suffered a major cyber security incident.

56%

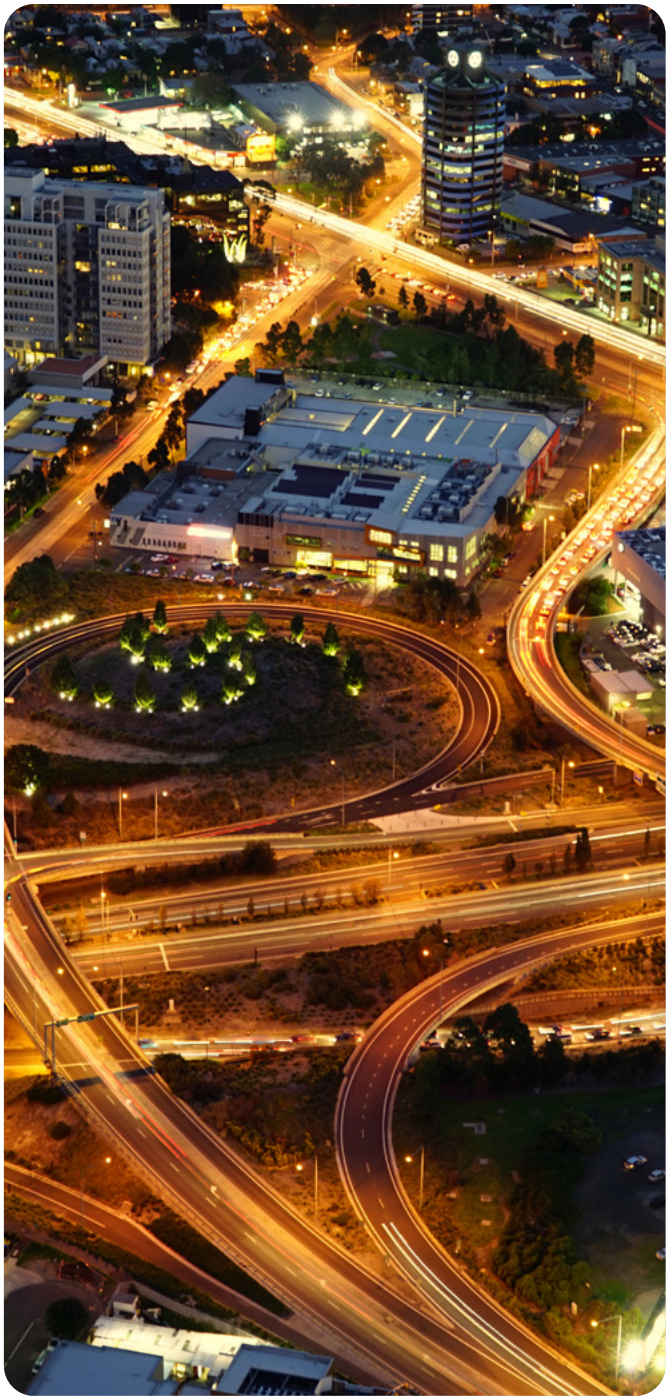
who drive, or plan to drive, an EV are concerned about cyber security risks related to EV charging.

95%

identified at least one of the following as a top concern: vehicles being remotely hacked, accessed or controlled, or data being sold or shared without consent.

Foreword

Australia's transport systems are undergoing a profound digital transformation. Connected vehicles, electric vehicles and emerging autonomous technologies offer major opportunities to improve safety, efficiency and convenience for motorists, while also contributing to achievement of national goals of sustainability and smarter infrastructure. At the same time, these technologies are reshaping the cyber security and data privacy landscape surrounding transport.



Modern vehicles are no longer simply mechanical platforms. They are increasingly connected to telecommunications networks, cloud services, mobile applications, charging infrastructure and wider digital ecosystems. As a result, cyber security, privacy and resilience are becoming fundamental components of transport policy and infrastructure assurance.

This report highlights an important reality: the benefits of connected transport technologies must be matched by appropriate safeguards for consumers, infrastructure and national resilience.

The National Institute of Strategic Resilience (NISR) particularly welcomes the report's focus on the interconnected nature of these challenges. Questions surrounding data governance, consumer transparency, trusted technology supply chains, offshore data storage, and the security of increasingly networked transport and energy systems will become more significant as adoption accelerates.

Importantly, the paper approaches these issues in a balanced and constructive manner. Building strong cyber security, privacy protections and resilience into connected transport systems should not be viewed as an obstacle to innovation, but as an essential enabler of public trust and long-term success.

NISR commends the NRMA and its partners for contributing to this timely national conversation. Australia has an opportunity to position itself as a leader in secure, trusted and resilient connected transport systems, supported by thoughtful policy development, collaboration and resilience-by-design principles.

This report is a valuable contribution to that effort.

Alison Howe
CEO, NISR

Introduction

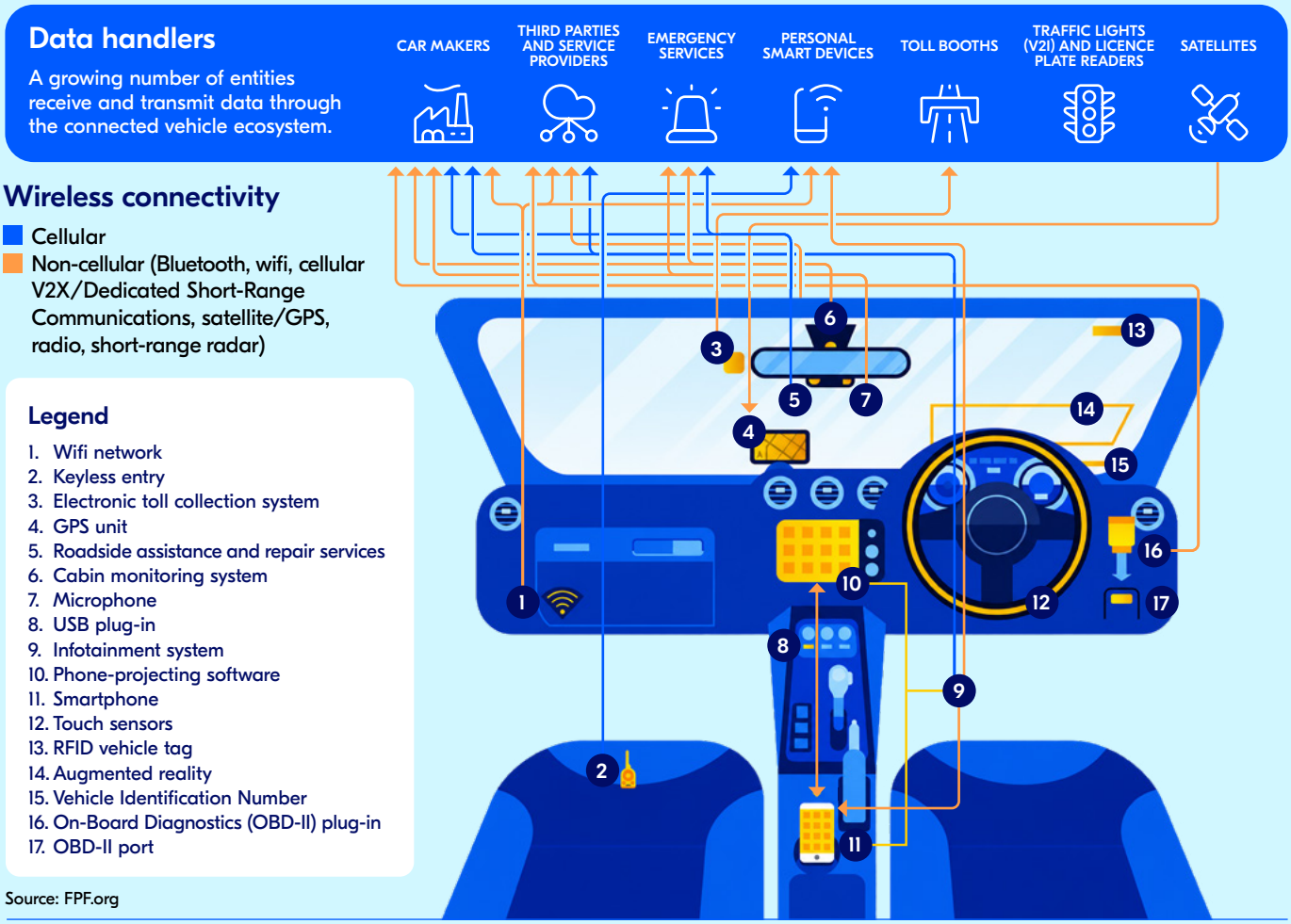
Connected vehicles (vehicles equipped with internet access and wireless connectivity that allow them to communicate with other vehicles, infrastructure, and services) are now widely adopted in Australia.[1] By 2031, more than 90% of new passenger cars sold in Australia are expected to have connected features, in line with global trends.[2]

The technology can improve safety and convenience for motorists by providing real-time hazard warnings, traffic and navigation updates, remote monitoring, and in some cases automatic emergency assistance after a crash.

Commercial fleets use connected technology to improve safety, reduce costs, and run vehicles more efficiently.

Governments and research institutions increasingly use vehicle data to support transport planning, congestion management, and policy development. Properly anonymised and aggregated data offers clear benefits for road safety analysis, infrastructure planning, and regulatory oversight.

But as vehicles become more connected and data-driven, these benefits bring new risks that existing privacy and cyber security frameworks were not designed to manage. The policy challenge is to enable beneficial uses of vehicle data while ensuring identifiable information is collected, used and shared transparently and securely, with consumers retaining meaningful control.



Source: FPF.org

[1] Australian Cyber Security Centre. Introduction to connected vehicles. Australian Government. https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-devices/introduction-to-connected-vehicles

[2] Kemp, K. Modern cars are surveillance devices on wheels with major privacy risks. UNSW Newsroom. https://www.unsw.edu.au/newsroom/news/2024/11/modern-cars-surveillance-devices-privacy-risks

PRIVACY RISKS

Concerns about connected vehicle data are no longer hypothetical. Privacy regulators in many jurisdictions, including the Australian Privacy Commissioner, have warned that connected vehicles can access vast amounts of sensitive information, including voice recordings, location data, images, driving behaviour, and data drawn from paired smartphones.[3] Overcollection of data from connected vehicles raises concerns about privacy risks, including uses that may be unfair, unreasonable, or contrary to the rights and interests of individuals in the vehicle. It also raises significant data security risks: larger and inadequately safeguarded data stores create opportunities for misuse or unauthorised access, including by malicious third parties.

These risks have direct consequences for consumers. Connected vehicle systems and linked mobile apps and services have been used to unlawfully track movements, restrict access to vehicles, and enable controlling or abusive behaviour, including in cases of domestic and family violence.[4]

Research by Australian academics and consumer organisations[5] has found that many carmakers and vehicle suppliers underestimate the risk of serious harm to individuals from privacy and data security failures.[6] Some misunderstand their obligations under the Privacy Act to prevent overcollection, overuse, oversharing, and unnecessary retention of information about identifiable individuals. Some fail to limit their collection of personal data — from both drivers and passengers — to what is genuinely necessary to deliver the connected service in question.[7]

Others rely on privacy policies that are difficult to find, complex, fragmented, or unclear. Where privacy disclosures are not sufficiently prominent, clear and understandable — in regulator terms, not sufficiently transparent — carmakers, suppliers or other third parties collecting personal information may not comply with their legal obligation to ensure that personal information is collected only by lawful and fair means.[8] An entity collecting and handling personal information about others must take reasonable steps to protect the data security of that information, protecting both against hackers and unauthorised use.[9]

Some manufacturers collect and share connected car data with third parties such as advertisers, data brokers, insurers, or analytics providers, often using broad or vague consent terms that limit meaningful consumer choice.[10]

However, not all connected vehicle data raises the same privacy risk. Properly anonymised or aggregated system-level data can be valuable for road safety, infrastructure planning, congestion management and public policy. Sharing and uses of properly anonymised or aggregated connected car data may be socially beneficial and reasonable where individuals and particular vehicles cannot reasonably be re-identified, and the data is protected and governed by demonstrably effective controls. By contrast, there are significant risks of privacy and data security harms to individuals when there is collection, use and sharing of identifiable or reasonably re-identifiable data, without clear limits and controls, inadequate transparency, and absence of meaningful consumer choice.

[3] Evidence of Commissioner Carly Kind to Legal and Constitutional Affairs Legislation Committee of the Australian Senate. Parliamentary Hansard, available at https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/estimate/29360/&sid=0006

[4] Australian Human Rights Institute. Technology facilitated abuse using connected cars: Gaps, limitations and supporting victim-survivor safety. UNSW Sydney. https://www.humanrights.unsw.edu.au/research/current-research/technology-facilitated-abuse-connected-cars

[5] Blakkarly, J. Drive one of these car brands? This is how much of your data they're tracking. CHOICE Website.

[6] The list of possible data harms is extensive. Examples include a negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit; offer of less favourable terms (for example, for insurances), or cancellation or an unfavourable change in terms; online abuse; discrimination, stigmatisation or reputational injury; inconvenience or expenditure of time; disruption and intrusion from unwanted communications or contacts; threats to personal safety arising from use of data by perpetrators to find or track an individual or otherwise monitor their movements or other activities; and other detrimental or negative consequences that affect an individual's private life or family matters. See further Peter Leonard, Privacy Harms: A research paper for the Office of the Australian Information Commissioner, available at https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/research-publications-on-the-privacy-act; Danielle Keats Citron & Daniel J. Solove, Privacy Harms, 102 Boston Uni Law Rev. 793

[7] Australian Privacy Principle 3. Personal information collected should be "relevant, minimal and not excessive": Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) AICmr 24 at [77]; see also Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, Chapter 3: Australian Privacy Principle 3 - Collection of solicited personal information, version 1.2, available at https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines

[8] Australian Privacy Principle 3.5; Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, Chapter 3, particularly at [3.87]

[9] Australian Privacy Principle 11

[10] Kemp, K. Driving Blind: The Unexamined Privacy Risks of Connected Cars, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5025836

Connected vehicle technology and data collection have outpaced Australia's current laws, which were not designed to regulate real-time transport data. Rules governing privacy and data access are being stretched to cover connected vehicles, rather than being designed specifically for them. Australia also continues to rely on voluntary industry standards, such as the FCAI Voluntary Code of Conduct for Automotive Data and Privacy Protection. Car manufacturers and their service partners control most of the data, not the drivers or owners.[11] Agreeing to extensive data collection is often a condition of using connected services, even where that data is not essential to vehicle operation.

In many cases, passengers have limited or no legal remedies. Laws restricting the use of surveillance devices generally do not apply to motor vehicles because vehicles are not classified as specialised 'surveillance devices'. Privacy notices and consent mechanisms typically apply only to the vehicle owner or primary driver, not to other occupants or even pedestrians passing by.[12]

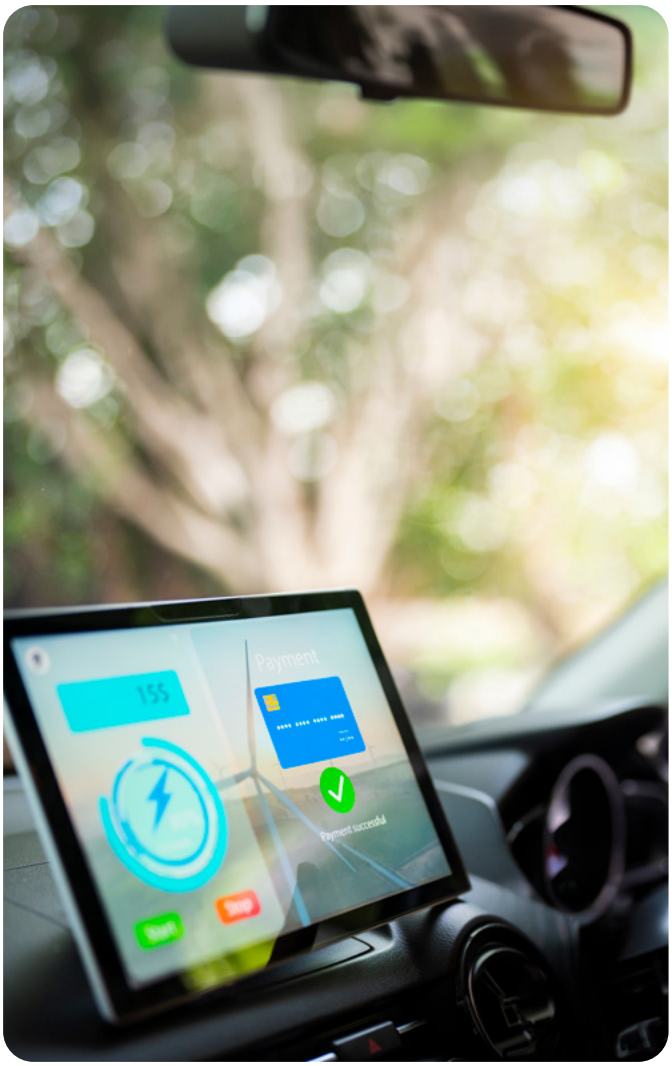
The Office of the Australian Information Commissioner (OAIC) has opened formal investigations into car manufacturers over potential breaches of privacy law linked to connected vehicles and has stated that these investigations are examining whether manufacturers are collecting more personal data than necessary and handling connected vehicle data without legally required limitations, safeguards and controls.[13]

Even with currently proposed enhancements to Australia's privacy framework, the rights of vehicle owners would be weaker than, for example, European Union countries, and California. The current position in Australia is that consent to extensive data collection, sharing, and secondary use is often a condition of accessing connected vehicle services, even when such data use is not directly related to the operation or core functionality of the vehicle.[14]

"Manufacturers are collecting more personal data than necessary."

Taken together, these concerns highlight the need for stronger, enforceable rules on what data connected vehicles can collect, how it is used, where and how long it is stored, who it is shared with, and for what purposes. Without targeted reforms to Australian privacy and data security laws, and enforcement of reformed rules, current safeguards will remain inadequate to protect owners, drivers, and passengers from connected vehicle data being used in ways that are unclear, unfair, unreasonable, or contrary to their legitimate interests.

Australian consumers should have a clear and enforceable right to refuse or withdraw consent for non-essential, opaque or excessive collection of identifiable personal data, either at the point of sale or at any time thereafter, without being denied access to core vehicle functions, safety features or warranty entitlements. This should not prevent the use of properly anonymised or aggregated data for legitimate socially beneficial purposes or prevent motorists from actively authorising trusted service providers such as repairers or roadside assistance providers to access relevant connected vehicle data for clearly stated and limited purposes.



[11] NRMA. What your car knows about you: How smart vehicles in Australia are collecting your data. https://www.mynrma.com.au/open-road/advice-and-how-to/driving/car-data-privacy-australia
[12] Tesla's Sentry Mode has faced regulatory scrutiny in Europe for recording passerby without consent. Pinsent Masons, 'Tesla makes camera settings more privacy-friendly following DPA investigation'. https://www.pinsentmasons.com/out-law/news/tesla-car-security-cameras-privacy-friendly-dutch-watchdog-probe
[13] Mike, F. Is your car spying on you? The privacy commissioner wants to know. The Sydney Morning Herald. https://www.smh.com.au/politics/federal/is-your-car-spying-on-you-the-privacy-commissioner-wants-to-know-20260210-p5o0xi.html
[14] NRMA. What your car knows about you: How smart vehicles in Australia are collecting your data. https://www.mynrma.com.au/open-road/advice-and-how-to/driving/car-data-privacy-australia

GROWING NATIONAL SECURITY RISK

Australia's security agencies are increasingly warning about the growing risk of cyberattacks on critical infrastructure by foreign state-backed actors. The Australian Security Intelligence Organisation has confirmed that hostile nations are actively probing Australia's transport, energy, and telecommunications systems to find weaknesses that could be exploited for future disruption. Senior officials have described Australia as now facing a high-risk environment for cyber sabotage.[15]

While these threats have to date mainly targeted major infrastructure, the rapid growth of connected vehicles (both combustion engine based and electric) and electric vehicle (EV) charging networks is creating new points of vulnerability. Vehicles now interact with electricity networks, mobile networks, and cloud services. If attackers were able to compromise these systems, the impact could go beyond data theft and lead to disruptions to transport services or even the power grid.

Australia's cyber security agencies have also warned that weaknesses in vehicle entertainment systems and connected apps could be used to steal personal information or gain unauthorised control of vehicle functions. As vehicles become more digitally connected, their security needs to be treated as part of Australia's broader infrastructure protection.

While all vehicles must meet Australian safety standards, concerns remain about data handling practices of imported vehicles. Other countries, including the United States, have proposed restrictions on data collected by vehicles manufactured by entities with links to foreign governments due to national security risks. Australia has not taken similar steps so far, but scrutiny is growing.

> **"Weaknesses in vehicle entertainment systems and connected apps could be used to steal personal information or gain unauthorised control of vehicle functions."**

This highlights the importance of clear, enforceable cyber security rules that apply to all vehicles and in-vehicle services sold in Australia, regardless of where they are made, with a focus on strong technical protections and responsible data handling.[16]

[15] Criminals could hack your EV, cyber tsar warns. The Australian Financial Review. https://www.afr.com/policy/foreign-affairs/criminals-could-hack-your-ev-cyber-tsar-warns-20251105-p5n7yg
[16] Smiths Lawyers. Cybersecurity on the Road: Hacking Threats to Connected Cars in Queensland and Impact on Driver Safety. https://www.smithslawyers.com.au/post/cybersecurity-threats-connected-cars

We are calling for:

- Stronger data rights for motorists, including transparent information about what data is collected, the ability to limit or withdraw consent at any time, and guarantees that refusing data collection will not impact core functions, safety features, or warranty coverage.
- Support for the responsible use of properly anonymised and aggregated connected vehicle data for road safety, infrastructure planning, congestion management, public policy and regulatory purposes, provided individuals cannot reasonably be re-identified.
- Clear recognition that consumers have enforceable rights to access, control and securely share their connected vehicle data with trusted third parties of their choice.
- Consistent national cyber security rules that cover connected vehicle systems, EV charging networks, software updates, and supply chain integrity, removing regulatory gaps and reducing confusion for consumers and industry.
- Clear incident response and consumer protections, including a national automotive cyber incident reporting scheme, emergency protocols, cyber security recall pathways, and guaranteed remedies for digital failures affecting safety or mobility.
- Public education and awareness campaigns to help drivers understand their privacy rights, spot cyber risks, secure their digital vehicle ecosystem, and know what to do if something goes wrong.

Cyber risks in the connected vehicle era

Connected vehicles are quickly becoming common across Australia's transport network. This connectivity allows vehicles to be part of a wider digital system, supporting new services such as vehicle health monitoring, fleet management, usage-based insurance, and improved driver assistance features that can benefit motorists. It can also support faster roadside assistance, more accurate fault diagnosis, improved safety responses and better infrastructure planning.

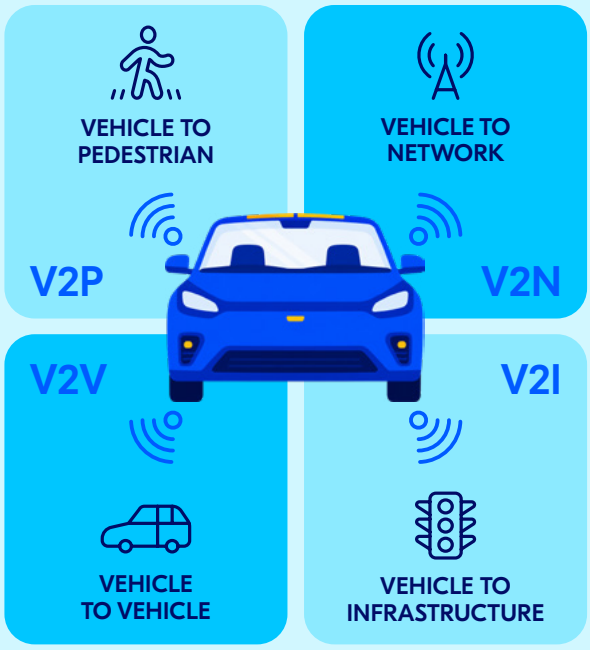
Connected vehicles collect and share large amounts of data that is not a single category of information. It may include data stored within the vehicle, data shared with manufacturers or service providers, and data broadcast between vehicles, infrastructure, mobile networks, or cloud systems. It may also combine vehicle performance data with location, route history, event data records, images, audio, in-cabin activity, external sensor inputs, and information drawn from connected devices. This matters because different data streams create different privacy, cyber security, and access risks — each requiring careful management to prevent sensitive information from being exposed and to stop malicious interference with vehicle systems — and should not be treated as though they all raise the same regulatory issues.[17]

> "Different data streams create different privacy, cyber security, and access risks."

It is important to note that connected vehicles are not limited to EVs or autonomous vehicles (AVs). Petrol and diesel-powered vehicles have incorporated internet connectivity, telematics, and remote-access features for many years, and face the same categories of cyber security and privacy risk. The sections that follow examine EVs and AVs in greater depth because their connectivity extends into additional systems, but the foundational risks described in this report apply equally to any vehicle that communicates with external networks, regardless of its powertrain.

[17] Brady, Mark. Data Privacy and Automated Vehicles: Navigating the Privacy Continuum. Monash University. https://doi.org/10.26180/11852727.v2

Types of connected data



Stored data is retained within the vehicle itself, typically in an event data recorder that captures vehicle dynamics — speed, braking, steering input, and location — in the seconds surrounding a collision.

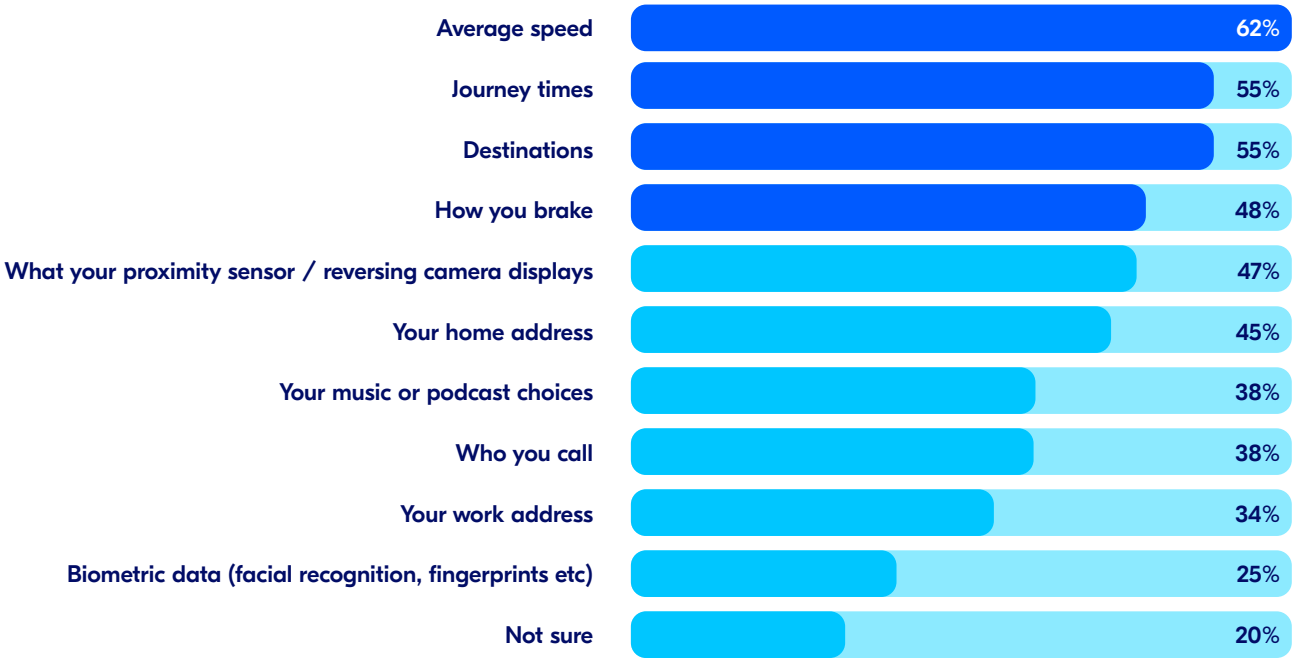
Shared data is exchanged in real time between connected vehicles and nearby infrastructure, including other vehicles and roadside systems. It includes position, proximity, and identification data.

Broadcast data is transmitted over telecommunications networks to the manufacturer's cloud systems or traffic authorities, covering the widest range of information including location, velocity, and occupancy data. At higher levels of automation this expands to include geolocation, external camera feeds, in-cabin monitoring, and biometric data.

These categories are not equivalent, and the risks they present scale with both the type of data and the level of vehicle automation. Treating them as a single regulatory problem risks either over-regulating low-risk operational data or under-protecting the most sensitive personal information.[18]

Types of data drivers believe modern cars retain

Source: NRMA survey



[18] Brady, Mark. Data Privacy and Automated Vehicles: Navigating the Privacy Continuum. Monash University. Journal contribution. https://doi.org/10.26180/11852727.v2

ELECTRIC VEHICLES

While connected EVs are not automatically more at risk than connected petrol or diesel vehicles, they raise additional concerns because they connect both the transport and energy sectors.

EVs' reliance on public and home charging infrastructure means if their back-end systems were compromised, a cyber incident could have wider impacts. A 2023 study for the Australian Energy Market Operator (AEMO) highlights cyber security and software management of EV charging systems as material risks for power system operation.[19] For example:

- Large numbers of EVs could start or stop charging at the same time, placing sudden strain on the grid.
- Disrupted communications could prevent smart charging programs from working properly, increasing costs and the risk of power outages.
- Malicious or faulty software could potentially slow or damage recovery efforts after a blackout.

Additionally, EVs' dependence on a broader digital ecosystem (online payment systems, cloud services, third-party software, and remote software updates) increases the risk of hacking, data theft, or system manipulation.

AUTONOMOUS VEHICLES

AVs use technology to understand their surroundings and carry out some or all driving tasks without constant human control, and this capability is steadily advancing. Automation ranges from basic driver assistance features, such as lane keeping or cruise control, to highly autonomous systems that can operate on their own in certain conditions.

While some autonomous features are already present in modern vehicles, capabilities requiring little to no human intervention are already available in other jurisdictions and could soon appear on Australian roads, through the potential expansion of Tesla's Full Self-Driving technology or autonomous taxi services like Waymo.

AVs build on connected vehicle technology by relying heavily on software, digital systems and artificial intelligence, including:

- Driving automation systems that use cameras, radar, mapping and software to control the vehicle.
- Communication links that allow vehicles to share information with each other and with road infrastructure to improve safety and traffic flow.
- Remote support centres that can assist vehicles when problems occur.

While these features can improve safety and efficiency, they also increase the risk of cyberattacks or software failures affecting how vehicles operate.[20]

Overseas model shown

[19] enX, EV Technical Standards for Grid Operation. https://www.aemo.com.au/newsroom/news-updates/aemo-report-highlights-electric-vehicle-benefits-and-challenges
[20] Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., & Das, R. Attacks on self-driving cars and their countermeasures: A survey. IEEE Access, 8, 207308–207342. P. 207309 https://doi.org/10.1109/ACCESS.2020.3037705

ATTACK SURFACES AND THREATS TO VEHICLES

The potential attack surfaces described below are common to all connected vehicles, including conventional petrol and diesel models. Connectivity, not powertrain type, is the determining factor in a vehicle's exposure to cyber threats. While the scale and nature of risks may vary between vehicle types, the categories below apply wherever a vehicle communicates with external networks, apps, or infrastructure.

Potential at-risk surfaces include:

- Vehicle control systems that manage braking, steering, driver assistance features, and battery systems.
- Wireless connections such as mobile networks, wifi and Bluetooth that allow remote functions and software updates.
- Data systems that collect and transmit information on location, driving behaviour, and vehicle performance.
- Sensors such as cameras and radar that help vehicles understand their surroundings.
- In-car entertainment and user systems that store personal information and connect to smartphones.
- Charging systems for EVs, including chargers, charging controllers, payment platforms, and links to electricity networks.
- Vehicle communication systems that share safety and traffic information with other vehicles and infrastructure.
- Cloud platforms and mobile apps operated by manufacturers and service providers.
- User accounts linked to vehicle apps, digital keys and remote services, where weak authentication or poor account recovery controls can enable unauthorised access.
- Physical access points such as diagnostic ports, key systems, and external devices.

Potential cyber threats include:

- Hackers gaining remote access to vehicle systems through weak internet or wireless connections.[21]
- Attackers taking control of software update systems and pushing malicious software to many vehicles at once.[22]
- Theft of personal data or tracking of drivers through in-car systems if these are not properly protected.[23]
- Interfering with vehicle sensors or cameras so the vehicle misreads its surroundings.[24]
- Tampering with maps or navigation systems, leading drivers into unsafe situations.[25]
- Disrupting vehicle communication systems that share safety information, which could increase the risk of crashes.[26]
- Taking control of remote support or fleet management systems that oversee multiple vehicles.[27]
- Shutting down vehicle fleets through ransomware or large-scale cyberattacks, causing major service disruptions.[28]

EV CHARGING INFRASTRUCTURE

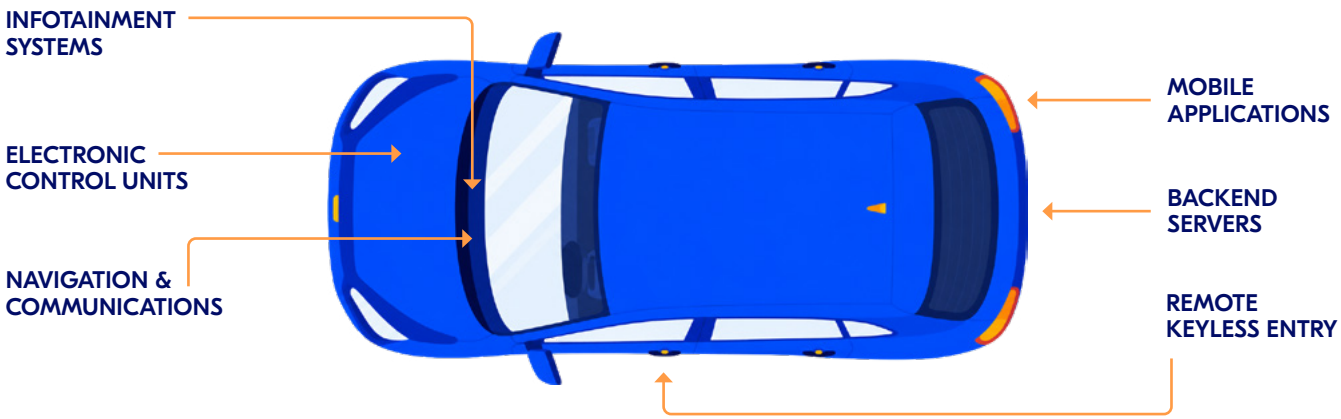
EV charging combines the flow of electricity with digital systems that manage safety, access, billing, and power levels. Chargers and vehicles communicate to coordinate charging, while back-end systems handle monitoring, updates, and smart charging functions. These systems also indirectly interact with electricity networks to help balance demand, especially for fast chargers and bidirectional technologies like vehicle-to-grid (V2G). Weak security across any part of this digital ecosystem can potentially create serious risks for consumers and the grid.

EV charging operates across three main settings:

Public charging

- Physical chargers, including slower AC chargers and fast DC chargers at public sites.
- Online systems that manage payments, user access, monitoring, software updates, and customer support.
- Third-party services such as payment providers, roaming services, and mapping apps that help drivers find and use chargers.

Threat surfaces



[21] Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. In-vehicle communication cyber security: Challenges and solutions. Electronics, 11(18), 2826. https://www.mdpi.com/1424-8220/22/17/6679
[22] Bielawski, R., Gaynier, R., Ma, D., Lauzon, S., & Weimerskirch, A. Cybersecurity of firmware updates (Report No. DOT HS 812 807). National Highway Traffic Safety Administration.
[23] Smith, M. 'Source of data': are electric cars vulnerable to cyber spies and hackers? The Guardian. https://www.theguardian.com/environment/2025/apr/29/source-of-data-are-electric-cars-vulnerable-to-cyber-spies-and-hackers
[24] Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., & Das, R. Attacks on self-driving cars and their countermeasures: A survey. IEEE Access, 8, 207308–207342. P. 207309
[25] Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., & Das, R. Attacks on self-driving cars and their countermeasures: A survey. IEEE Access, 8, 207308–207342. P. 207309
[26] Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., & Das, R. Attacks on self-driving cars and their countermeasures: A survey. IEEE Access, 8, 207308–207342. P. 207309
[27] Rosenzweig, A. Answering the inherent cyber-challenges of teleoperation. Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/inherent-cyber-challenges/
[28] DPV Transportation. Cybersecurity in autonomous vehicles: Defending cars from hackers. https://www.dpvtransportation.com/cybersecurity-autonomous-vehicles/

Home charging

- Smart home chargers connected to the internet, often linked with rooftop solar, home batteries, and energy management systems.
- Charging that can be scheduled by the driver or automatically managed by apps or service providers.
- Links to electricity network programs that help balance demand and reduce charging costs.

Bidirectional charging

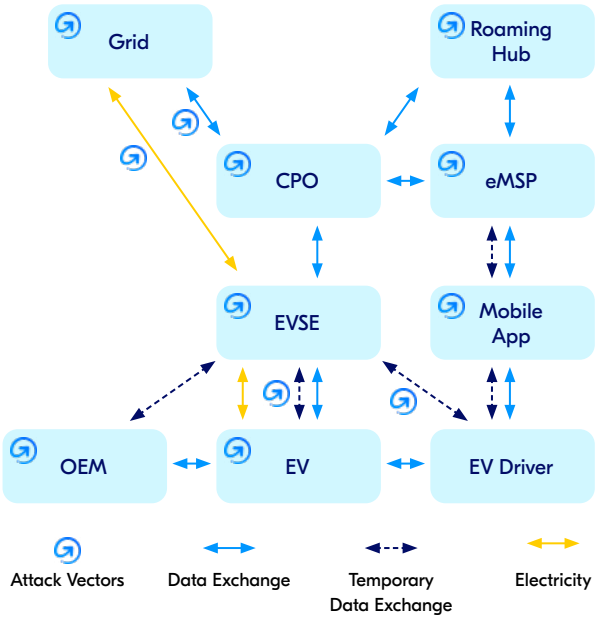
- Technology that allows EVs to send electricity back to homes, buildings or the grid, helping manage peak demand and providing backup power.
- Integration with electricity services that support grid stability and emergency power supply.

Potential cyber risks affecting EV charging systems include, but is not limited to:

- Hackers interfering with charging equipment to disable chargers or install harmful software.
- Attacks on central charging network systems that handle payments and operations, which could cause widespread outages or financial fraud, as well as physical tampering such as fake QR codes placed over legitimate ones to redirect payments to fraudsters.[29]
- Weak security around user identification or digital systems that could allow criminals to pretend to be vehicles or chargers and steal electricity or services.[30]
- Hacked home chargers being controlled in large numbers, potentially putting strain on the electricity grid.[31]
- Hacking or misuse of third-party roaming platforms or websites to conduct fraud.

Possible attack vectors in the Electric Vehicle Supply Equipment ecosystem

Source: Irdeto



Attack on charging stations

Attackers could hack charging station to harvest data or add monetary charges to user or render the charging station useless

Attack on vehicles

Can infect vehicles that interface with the charging station to attack the car's ECU

Data theft

The exchange of data between the EV, the charging station and its home network creates rich sources of data for attackers to steal

Attack on critical infrastructure

EV charging infrastructure could be used as a channel to attack the energy grid through attacks such as fake overloading or DDoS

Energy theft

If authorisation protocols are circumvented, it could be possible for attackers to steal energy from the grid

Legend

CPO: Charge Point Operator is responsible for building, owning, and maintaining the physical infrastructure of EV charging stations.
eMSP: E-Mobility Service Provider manages the EV charging experience (mobile apps and RFID cards) for drivers.
EVSE: Physical charging equipment providing power to the EV.
OEM: Company that designs, brands, and assembles the vehicle.

[29] Irdeto & Metergram. The essential guide for NEVI-funded EV projects.
[30] Panda, P. Using PKI to secure plug and charge. Intertrust Technologies. https://www.intertrust.com/blog/using-pki-to-secure-plug-and-charge/
[31] Shekari, T., Cardenas, A. A., & Beyah, R. MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 3539–3556). USENIX Association. https://www.usenix.org/conference/usenixsecurity22/presentation/shekari & enX (2023) EV Technical Standards for Grid Operation

Best practices to counter cyber threats

This section outlines best practices for facilitating secure vehicle and charging systems, drawing on international standards such as ISO/SAE 21434, UNECE WP.29 R155/156, ISO 15118, and OCPP 2.0, as well as guidance from organisations like the U.S. National Highway Traffic Safety Administration. Together, these approaches focus on protecting data and communications, managing software updates, and responding to cyber risks, while allowing new technologies to be deployed safely in Australia.

SECURE CONNECTED VEHICLES

Secure by design and lifecycle security

Modern vehicles are increasingly driven by software, which makes cyber security a core part of vehicle safety. Security needs to be built into vehicles from the outset, rather than added later, to reduce vulnerabilities and avoid constant fixes after problems emerge.

This expectation is now reflected in international standards, which require manufacturers to manage cyber risks across the full life of a vehicle.[32] That responsibility extends beyond design and production to monitoring vehicles once they are on the road and responding to cyber incidents when they occur.[33, 34]

In practical terms, this means vehicles must be securely configured at delivery, kept up to date through regular software maintenance, and properly decommissioned at the end of their life by removing stored data and access rights.[35]

Maintaining this level of security also requires continuous assurance. Systems need to be tested regularly for weaknesses, new software must be checked before release, and manufacturers must be able to quickly fix or reverse updates if issues are identified.

Secure supply chains and software

Modern vehicles use software and components from many suppliers. Best practice guidance now focuses on improving transparency about what software is used, ensuring updates come from trusted sources, and actively managing risks from third-party vendors.[36] This helps manufacturers quickly identify vulnerabilities, fix problems, and prevent unsecure components from entering vehicles in the first place.

Strong internal vehicle protections

Security features such as protected internal networks and restricted system access help prevent attackers from moving between different parts of a vehicle's systems.[37] For example, keeping braking and steering systems separate from entertainment or mobile phone connections reduces the risk that a hack in one area affects critical safety functions.

Safe software updates

Connected vehicles regularly receive remote software updates to fix bugs and improve performance. These updates must be securely delivered and verified to ensure only approved software is installed.[38] Strong update controls help manufacturers respond quickly to new threats while preventing attackers from pushing harmful software into vehicles.[39]

[32] ISO/SAE 21434
[33] Camacho, R. Ensure cybersecurity in the connected vehicles era with ISO/SAE 21434. EE Times Europe. https://www.eetimes.eu/ensure-cybersecurity-in-the-connected-vehicles-era-with-iso-sae-21434/ & Applus+ Laboratories. (2022, October 25). UNECE WP.29 R155/R156: New cybersecurity regulations for vehicles. https://www.appluslaboratories.com/global/en/news/publications/new-cybersecurity-regulations-vehicles-unece-wp29
[34] UNECE WP.29 R155
[35] WP.29 R156 and NHTSA Cybersecurity Best Practices.
[36] NHTSA Cybersecurity Best Practices
[37] National Highway Traffic Safety Administration. Cybersecurity best practices for the safety of modern vehicles. U.S. Department of Transportation. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-pre-final-tag_0_0.pdf
[38] United Nations Economic Commission for Europe. UN Regulation No. 156 — Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system. https://unece.org/sites/default/files/2024-03/R156e%20%282%29.pdf
[39] Brightwood, S. The importance of secure firmware updates in maintaining system integrity. ResearchGate. https://www.researchgate.net/publication/384687421

Data protection and privacy

Connected vehicles generate vast amounts of data revealing driver behaviour, passenger activity, and vehicle operation, and as automation increases, so do sensor and monitoring capabilities. The falling cost of collecting and analysing this data makes it easier for manufacturers and third parties to access large volumes of sensitive information, including detailed location and route history, biometric identifiers, and video footage.

Misuse of this data is not only a privacy issue but a physical safety risk, as individuals' movements and activities can be tracked or inferred. In some instances, too much data is being collected, used, shared, and retained without sufficient oversight, transparency, or justification, leaving vehicle owners, drivers, passengers, and regulators with limited visibility into what is happening with data that relates to their movements, behaviour, interests and activities. Data collection must be proportional; limited to what is reasonably necessary to deliver the connected service. Collecting entities should be obliged to minimise data collection — gathering only what is relevant and necessary for the provision of the connected service, and no more.[40] Data minimisation also reduces risks of breaches of information security.

Vehicle suppliers should be required to assess risks of harm, limit data collection to clear and defined purposes, and build safeguards in from the start. Effective controls must apply across the entire data supply chain, including intermediaries, with any sharing beyond stated purposes quickly detected and stopped.

Particular scrutiny is needed where connected vehicle data is used for purposes beyond the direct provision of connected services to the motorist. Under Australian privacy law, use or disclosure of personal information should generally be linked to the primary purpose of collection unless a recognised exception applies. Where personal information is disclosed overseas, entities must also take reasonable steps to ensure overseas recipients handle that information consistently with Australian privacy obligations.[41]

Reforms should focus on identifiable or reasonably re-identifiable data, targeting excessive collection, unclear secondary use, and weak consent. Properly anonymised and aggregated data should remain available for demonstrably socially beneficial uses such as road safety research, infrastructure planning, and public policy, where safeguards prevent re-identification or misuse. These reforms should align with leading international frameworks, including the EU's General Data Protection Regulation and California's Consumer Privacy Act.[42]

Secure communications

Connected vehicles exchange information with other vehicles, road infrastructure, mobile apps, and cloud services to support safety features, navigation, software updates, and fleet management.

All of these communication channels must be protected to ensure messages are genuine, cannot be altered, and remain private. Strong security controls help prevent attackers from interfering with vehicle operations or accessing sensitive information.[43, 44]

Ongoing monitoring and rapid response

For autonomous fleets such as taxis, best practice involves continuously monitoring vehicle systems and digital platforms for unusual activity or cyber threats. When problems are detected, systems should support quick investigation, clear reporting, and fast response. AVs should be able to slow down, stop safely, or hand control to a human or remote operator if something goes wrong.[45]

[40] Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, Chapter 3: Australian Privacy Principle 3 - Collection of solicited personal information, version 1.2, paragraph [3.26]
[41] Rountree, D., Fisher, J., & Lustig, M. Data driven: Navigating the legal and regulatory backroads for connected vehicles. Allens. https://www.allens.com.au/insights-news/insights/2026/02/data-driven-navigating-the-legal-and-regulatory-backroads-for-connected-vehicles/
[42] Kemp, K, Driving Blind: The Unexamined Privacy Risks of Connected Cars, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5025836; CNIL (French Data Protection Authority) & Connected vehicles: a compliance package for a responsible use of data. https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.
[43] ETSI Intelligent Transport Systems security framework and IEEE 1609.2-2022
[44] Institute of Electrical and Electronics Engineers. IEEE standard for wireless access in vehicular environments — Security services for applications and management messages (Standard No. 1609.2-2022). https://standards.ieee.org/ieee/1609.2/10258
[45] Aniculaesei, A., Aslam, I., Bamal, D., Helsch, F., Vorwald, A., Zhang, M., & Rausch, A. Connected dependability cage approach for safe automated driving (arXiv:2307.06258v1). Institute for Software and Systems Engineering, TU Clausthal. Diambil dari https://arxiv.org/abs/2307.06258

Secure communication

Cyberattacks on EV charging systems can cause service outages, enable fraud, or allow unauthorised control of chargers. To reduce these risks, charging systems now use encrypted communication and strong digital identification (Public Key Infrastructure or PKI) so that only trusted vehicles and chargers can connect. Newer systems also support automatic payment and authentication when a vehicle is plugged in, removing the need for cards or apps while keeping transactions secure (Plug & Charge).

Charging providers are improving the security of the systems that manage chargers online. This includes better control over software updates, stronger protections for digital certificates, and secure connections. At the network level, operators are adding safeguards to limit data traffic to trusted devices only, helping to block unauthorised access to equipment like communication switches. These measures are important to prevent attackers from interfering with charging or causing broader problems for the electricity grid.

Clear responsibilities and oversight are needed to ensure that both charging networks and vehicle manufacturers properly manage cyber security across their systems.[46]

What is PKI?

Public Key Infrastructure (PKI) is a framework of policies, processes, hardware, software, and standards that manages the creation, distribution, storage, and revocation of digital certificates — enabling trusted, secure communication between parties over a network.

What is Plug & Charge?

Plug & Charge is a smart system for EV chargers (based on ISO 15118 standards and relies on PKI) that automatically handles ID checks, approvals, and billing the moment you plug in at a public station — no apps, cards, or button-pushing required.

What is NEPKI?

The National Energy Public Key Infrastructure (NEPKI) is a new, not-for-profit national system being developed to securely identify and authenticate internet-connected energy devices that are seeking flexible import or export capacity from the grid. This includes equipment such as solar inverters, home batteries, and EV chargers.

Instead of each electricity network using its own separate security system, NEPKI will create a single national trust framework. This will allow devices across Australia to securely connect and communicate in a consistent way. From 2026, approved manufacturers will be able to issue secure digital certificates for their products under this national system.

For EV charging, this applies where a charger (or managed charging service) needs to securely communicate agreed capacity and operating limits with the grid. It does not apply to other EV charging functions such as payments, roaming, or Plug & Charge.

Safe software updates for chargers

EV chargers require secure software and firmware update mechanisms, as insecure update handling has been shown in research to allow remote code execution on charging equipment, and real-world cyberattacks have already shut down charging networks.[47] All charging equipment should support secure updates that ensure only approved software can be installed.

Ongoing monitoring and rapid response

Charging network operators should continuously monitor their systems to spot unusual activity or cyber threats early. Best practice includes having clear response plans for outages or cyber incidents so services can be restored quickly and damage contained.[48]

In Australia, large businesses and operators of critical infrastructure must report serious cyber incidents within set timeframes under national cyber security laws (SOCI Act and Cyber Security Act). These rules help improve preparedness, coordination, and awareness of cyber threats across the country.

However, EV charging network operations are not currently designated as critical infrastructure under the SOCI Act or the newer national cyber security framework. Governments should bring them into scope through a consultative approach that strengthens security oversight without placing unreasonable compliance or cost burdens on operators.

Protecting charging data and privacy

EV charging systems collect personal information, such as where and when people charge, how they pay, and, in some cases, information that can reveal driving patterns. To protect privacy, collection should be limited to what is reasonably necessary, secured appropriately, and handled in a transparent way in line with the Australian Privacy Principles.

When drivers pay using cards or apps, payment data must comply with appropriate industry standard requirements and Australian privacy law to reduce fraud and cyber security risks. In Australia, EV charging providers must comply with the Privacy Act 1988 and the Australian Privacy Principles, including obligations around data minimisation, security safeguards (such as encryption and access controls), and clear privacy notices.

[46] Irdeto, INCYDE, & Utimaco. A holistic approach to solving EVs toughest ecosystem challenges (Whitepaper). Utimaco. Retrieved from https://irdeto.com/hubfs/resources/white-papers/approach-to-solve-ev-ecosystem-challenges.pdf

[47] Tanyıldız, H., Şahin, C. B., Dinler, Ö. B., Migdady, H., Saleem, K., Smerat, A., Gandomi, A. H., & Abualigah, L. Detection of cyber attacks in electric vehicle charging systems using a remaining useful life generative adversarial network. Scientific Reports, 15(1), Article 10092. https://doi.org/10.1038/s41598-025-92895-9

[48] Irdeto & Metergram. The essential guide for NEVI-funded EV projects.

The Australian context

EV UPTAKE AND CHARGING INFRASTRUCTURE FOOTPRINT

By March 2026, more than half a million electric vehicles were on Australian roads.[49] The market now offers more than 150 EV models across cars, SUVs, utes, vans, trucks, and buses. This growth has been supported by the New Vehicle Efficiency Standard, introduced in January 2025, which has encouraged greater supply and increased competition, helping to improve choice and affordability for consumers.[50]

Australia's charging network has also grown quickly to support rising EV use. This included:

- Over 1,270 public fast and ultra-fast charging sites nationwide, with more than 4,190 individual charging points, representing strong year-on-year growth.
- A growing number of slower public chargers at shopping centres, tourist locations, and on streets.
- Home charging, which accounts for around 80% of all EV charging, with many households using smart chargers linked to solar panels and home batteries.

"March 2026, more than half a million electric vehicles were on Australian roads."

AUTONOMOUS VEHICLE TRIALS AND DIRECTIONS

Australia's AV sector is still in its early stages and is being driven mainly by government trials and planning rather than consumer demand. As of 2026, AVs are not approved for commercial use on public roads, but every state and territory has tested autonomous vehicles in controlled environments such as campuses and closed tracks. Some advanced driver assistance systems are also now available in consumer vehicles, allowing software updates that support supervised autonomous driving features.

Australia already has strong experience with automation in other industries. In Western Australia, large numbers of autonomous trucks operate across major mining sites, and fully autonomous freight rail systems are in use in the Pilbara. In public transport, Sydney Metro launched Australia's first driverless passenger rail line in 2019.[51]

The infrastructure and rules needed to support AVs are still developing. This includes reliable mobile networks, accurate positioning systems, and digital mapping of roads. National programs are underway to support vehicle communication technologies, but mobile coverage gaps remain, particularly in regional and remote areas. While government programs aim to improve connectivity, more investment will be needed to support widespread AV deployment.[52]

Governments are also working together to plan the digital and physical upgrades needed for AVs, including road design guidance and readiness assessments. A key challenge is deciding when and how much to invest, given uncertainty about how quickly technology will evolve.[53]

Over time, AVs are expected to become more common. By 2031, limited forms of highly autonomous driving are expected to enter the market, making up a small share of new car sales. By 2050, a large share of new vehicles and a significant portion of the total vehicle fleet are forecast to operate with high levels of automation. Freight transport is likely to lead adoption, followed later by shared services such as autonomous taxis.[54]

To support this shift, new national laws are expected by late 2026 that will place safety responsibility on the companies that operate autonomous driving systems, rather than on individual drivers. These laws will sit alongside existing vehicle safety standards.

[49] Electric Vehicle Council. EV sales hit all-time high: Drivers hit the road for the Easter long weekend. https://electricvehiclecouncil.com.au/media-releases/ev-sales-hit-all-time-high-drivers-hit-the-road-for-the-easter-long-weekend-2/

[50] Electric Vehicle Council. State of EVs 2025 & Department of Climate Change, Energy, the Environment and Water. National Electric Vehicle Strategy Annual Update: 2024–25. Department of Climate Change, Energy, the Environment and Water. https://dcceew.gov.au/energy/transport/national-electric-vehicle-strategy

[51] Centre for Connected and Automated Transport. Discussion paper: The National Future Transport Summit. https://www.ccat.org.au/publications

[52] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. National road transport technology strategy. https://www.infrastructure.gov.au/sites/default/files/documents/national-road-transport-technology-strategy.pdf & Centre for Connected and Automated Transport. Discussion paper: The National Future Transport Summit. https://www.ccat.org.au/publications

[53] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. National road transport technology strategy. https://www.infrastructure.gov.au/sites/default/files/documents/national-road-transport-technology-strategy.pdf

[54] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. National road transport technology strategy. https://www.infrastructure.gov.au/sites/default/files/documents/national-road-transport-technology-strategy.pdf

REGULATORY AGENCIES

Connected vehicle policy sits across a multi-layered regulatory environment involving Commonwealth, state and territory, and local government responsibilities.

Commonwealth government agencies

- **Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA):** Responsible for national vehicle design and first supply regulation via the Australian Design Rules (ADR), AV policy, road transport technology strategy, and digital infrastructure for connected vehicles.
- **Department of Climate Change, Energy, the Environment and Water (DCCEEW):** responsible for the National Electric Vehicle Strategy (joint lead), EV—grid integration initiatives, charging infrastructure programs, and broader transport decarbonisation policy.
- **Australian Renewable Energy Agency (ARENA):** Responsible for funding EV charging infrastructure deployment and research into grid interactive vehicle technologies.
- **Department of Home Affairs (Cyber Security Portfolio):** Responsible for national cyber security policy, coordination of the 2023—2030 Cyber Security Strategy, and cyber related regulatory reforms affecting connected vehicles and charging systems.
- **Australian Signals Directorate (ASD):** Responsible for national cyber defence, cyber threat intelligence, and technical cyber security guidance relevant to connected vehicles and critical infrastructure.
- **Australian Cyber Security Centre (ACSC) within ASD:** Responsible for operational cyber security, publishing alerts and advisories, delivering threat intelligence, and receiving mandatory cyber incident reports.
- **Critical Infrastructure Security Centre (CISC):** Responsible for administering SOCI Act requirements, including cyber incident reporting and risk management obligations for critical infrastructure.
- **Australian Communications and Media Authority (ACMA):** Responsible for regulating the telecommunications elements of connected vehicles, determining carriage service provider obligations, and managing spectrum for V2X technologies.
- **Australian Competition and Consumer Commission (ACCC):** Responsible for consumer protection enforcement relating to connected vehicle products, data handling, and cyber security representations.
- **National Transport Commission (NTC):** Responsible for national reform of AV regulation, ADS safety law, and data governance for connected and autonomous vehicles.
- **Office of the Australian Information Commissioner (OAIC):** Responsible for regulating privacy and data protection obligations under the Privacy Act 1988, including oversight of how connected vehicle and charging infrastructure data is collected, stored, used, and disclosed.
- **Attorney-General's Department:** Central policy lead on Privacy Act reform and related law-and-justice issues, including cybercrime offences and surveillance law; the OAIC remains the primary privacy regulator/enforcer.
- For AVs, Commonwealth Government provides national policy leadership and coordinates the development of consistent regulatory frameworks. Key responsibilities include:
  - Developing the national AV safety law and supporting regulations.
  - Coordinating with states and territories through the Infrastructure and Transport Ministers' Meeting (ITMM).
  - Aligning Australian approaches with international standards and best practices.
  - Support research and development through Imove Australia and Austroads.

State and territory governments

State and territory governments maintain responsibilities for vehicle registration, in-service compliance, road rules, modifications and local enforcement. They also implement jurisdiction-specific EV strategies, purchase incentives, charging infrastructure programs, government fleet transition targets, and planning frameworks.

The National Electric Vehicle Action Plan Implementation Group is a joint Commonwealth, State and Territory government forum established under the National Electric Vehicle Strategy to coordinate national actions on standards, charging infrastructure, affordability, data, fleet procurement and public education. Its purpose is to accelerate Australia's transition to EVs and support cleaner air, broader uptake, and a strong domestic EV industry.

> "Connected vehicle policy sits across a multi-layered regulatory environment involving Commonwealth, state and territory, and local government responsibilities."

For AVs, state and territory governments act as road managers and service providers, with responsibilities including:

- implementing state-based AV user laws and operational regulations,
- managing AV trials and pilot programs,
- developing and deploying C-ITS infrastructure,
- planning for AV integration with public transport systems, and
- managing local road infrastructure upgrades to support AV operation.[55]

[55] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. National road transport technology strategy. https://www.infrastructure.gov.au/sites/default/files/documents/national-road-transport-technology-strategy.pdf

Local governments

Over 500 local government areas manage critical elements including development approvals, facilitating kerbside charging deployment, and public charging at community facilities.

REGULATORY FRAMEWORKS, CHALLENGES AND REFORM APPROACHES

Legal landscape

Connected vehicles sit across several legal regimes that were not designed as a single connected vehicle framework. Privacy law, consumer law, telecommunications regulation, surveillance laws, vehicle standards and emerging smart device cyber security rules can all apply, depending on the type of data collected, the service being provided and the technology used.

This creates a fragmented legal environment for manufacturers, service providers, charging operators, repairers and consumers. It also means that connected vehicle risks may be regulated indirectly through general laws, rather than through a tailored framework designed for continuous vehicle connectivity, real-time data flows and software-enabled vehicle functions.

Key legal frameworks include:

- **Privacy and data protection:** The Privacy Act 1988 (Cth) regulates the collection, use, storage and disclosure of personal information. This is highly relevant to connected vehicles because vehicle data may include location history, driving behaviour, voice data, images, linked-device information, account data and other information capable of identifying a person.
- **Surveillance device laws:** Federal, state and territory tracking device and surveillance device statutes, including the Surveillance Devices Act 2004 (Cth), may be relevant where connected vehicles use cameras, microphones, location tracking or other monitoring functions. Lack of transparency about in-vehicle recording, remote monitoring or surveillance capability may create legal risk, particularly where people are recorded or tracked without adequate knowledge or consent.
- **Consumer protection:** The Australian Consumer Law applies to vehicles and connected services, including consumer guarantees, misleading or deceptive conduct, unfair contract terms and product representations. This is relevant where connected services are offered through separate terms and conditions, where data practices are not clearly explained, or where consumers may lose access to vehicle functions, warranties or services if they refuse data collection.
- **Telecommunications and spectrum regulation:** The Telecommunications Act 1997 (Cth) and Radiocommunications Act 1992 (Cth) may apply to connectivity services, vehicle communications systems, sensors and spectrum-dependent technologies. This is relevant where connected vehicles or service providers transmit data through mobile networks, vehicle-to-everything systems, connected infrastructure or other communications systems.
- **Motor vehicle regulation:** The Road Vehicle Standards Act 2018 (Cth) establishes standards for road vehicles supplied in Australia. As vehicles become more software-dependent, questions arise about how cyber security, software updates, remote access and connected features should be treated within vehicle safety and compliance frameworks.
- **Service and repair information:** The motor vehicle service and repair information sharing scheme in Part IVE of the Competition and Consumer Act 2010 (Cth) requires access to technical repair information for independent repairers. This becomes increasingly important for connected vehicles, where faults may be software-based, data-driven or linked to cyber security controls rather than purely mechanical issues.
- **IoT and smart device cyber security:** The Cyber Security Act 2024 (Cth) introduces minimum cyber security standards for smart devices. While road vehicle components are excluded, the framework may become relevant to connected components, apps, devices or charging-related technologies that are not adequately covered by vehicle standards.[56]

> **"A fragmented legal environment for manufacturers, service providers, charging operators, repairers and consumers."**

Privacy data protection and information governance

A 2024 investigation by consumer group CHOICE found that seven of Australia's ten most popular car brands collect and share driving data with outside companies. Some brands go further than location and driving data, collecting voice recognition data through in-car systems and sharing it with overseas technology companies. Voice recognition data is treated as sensitive personal information under Australian Privacy Law, meaning it should attract a higher level of consumer protection before it can be collected and shared. Despite this, brands including Kia and Hyundai were found to share voice data with a US-based artificial intelligence company, and Tesla collects short video clips from cameras fitted inside and outside the vehicle. Some manufacturers have claimed this data is shared in a way that cannot be traced back to individual drivers.

While most major brands with connected features say drivers can opt out of data collection, they are typically signed up automatically when they buy the car or download the vehicle's app. In at least one case, a motorist who attempted to physically remove the device that transmits their vehicle's data risked voiding their warranty. Opting out is therefore neither simple nor without consequences for consumers.[57]

[56] Rountree, D., Fisher, J., & Lustig, M. Data driven: Navigating the legal and regulatory backroads for connected vehicles. Allens. https://www.allens.com.au/insights-news/insights/2026/02/data-driven-navigating-the-legal-and-regulatory-backroads-for-connected-vehicles/

[57] Blakkarly, J. Drive one of these car brands? This is how much of your data they're tracking. CHOICE Website.

The privacy terms that govern what data is collected are often long, technical, and difficult for most people to understand. This problem is made worse where key privacy disclosures are provided through in-vehicle dashboards, apps or registration screens that are poorly suited to explaining complex data practices. Connected vehicles can involve many separate data activities, including collection through sensors, cameras, microphones, smartphones, vehicle diagnostics and cloud services. Disclosures should therefore be accessible and not buried in standard terms and conditions.[58]

Privacy-by-design should be a baseline requirement for connected vehicle services. Because many connected services collect data automatically, manufacturers and service providers should avoid bundling non-essential data collection with access to core services. Motorists should be able to distinguish between data collection that is necessary for safety, security or vehicle operation, and data collection used for secondary or optional purposes. Where users cannot make that distinction, consent is unlikely to be meaningful. Broad consent clauses in standard form terms may also raise consumer law concerns, particularly where they give manufacturers or service providers wide discretion to collect, use or disclose vehicle data in ways that consumers would not reasonably expect.[59] Privacy and consumer protection reforms should therefore be considered together, rather than treated as separate issues.

In practice, connected vehicle data in Australia is controlled and managed by manufacturers and their service providers under contractual and privacy terms, not by vehicle owners. Even when an owner gives prior, express, and fully informed consent for their vehicle data to be shared with a nominated third party — such as a roadside assistance provider — there is currently no legal mechanism that compels the data controller to act on that instruction.

Existing privacy frameworks, such as the Privacy Act, primarily focus on the vehicle owner or primary driver, leaving passengers with little or no protection despite the collection of their personal information. As vehicles become more automated and sensor-rich, they may collect information about passengers, pedestrians, cyclists, nearby vehicles and other road users. These people may have no direct relationship with the vehicle manufacturer or service provider and may never see, understand or accept the relevant privacy terms. This strengthens the case for privacy-by-design, data minimisation and clear limits on secondary use.

The Australian Privacy Commissioner's current stated regulatory priorities include upholding privacy and information access rights when dealing with new and emerging technologies with high impact, including new surveillance technologies such as location data tracking in apps, cars and other devices.[60] As noted previously, formal investigations by the OAIC are underway into vehicle suppliers concerning possible breaches of the Privacy Act. These investigations are examining whether vehicle suppliers are collecting more personal information than necessary and whether that data is being used or shared without fully informed and voluntary consent.

The powers of the privacy regulator, and the range of enforcement options available to the regulator, were expanded in December 2024. The Australian Attorney-General is considering further reforms to the Privacy Act that would increase incentives for companies that collect and use personal data, including vehicle suppliers, to ensure that connected vehicle data is used fairly, reasonably, and with greater transparency for affected individuals.

Australia's current regulatory and data access frameworks were not specifically designed for continuous, real-time consumer vehicle data and remain incomplete for AVs. Compliance is currently being 'fitted into' general privacy and consumer law, rather than managed under a tailored real-time vehicle data regime. Robust privacy reforms alone will not guarantee meaningful consumer control of real-time vehicle data. Targeted data access and data governance reforms are needed to empower owners to access and use data about their connected vehicles.

"Connected vehicle data in Australia is controlled and managed by manufacturers and their service providers under contractual and privacy terms, not by vehicle owners."

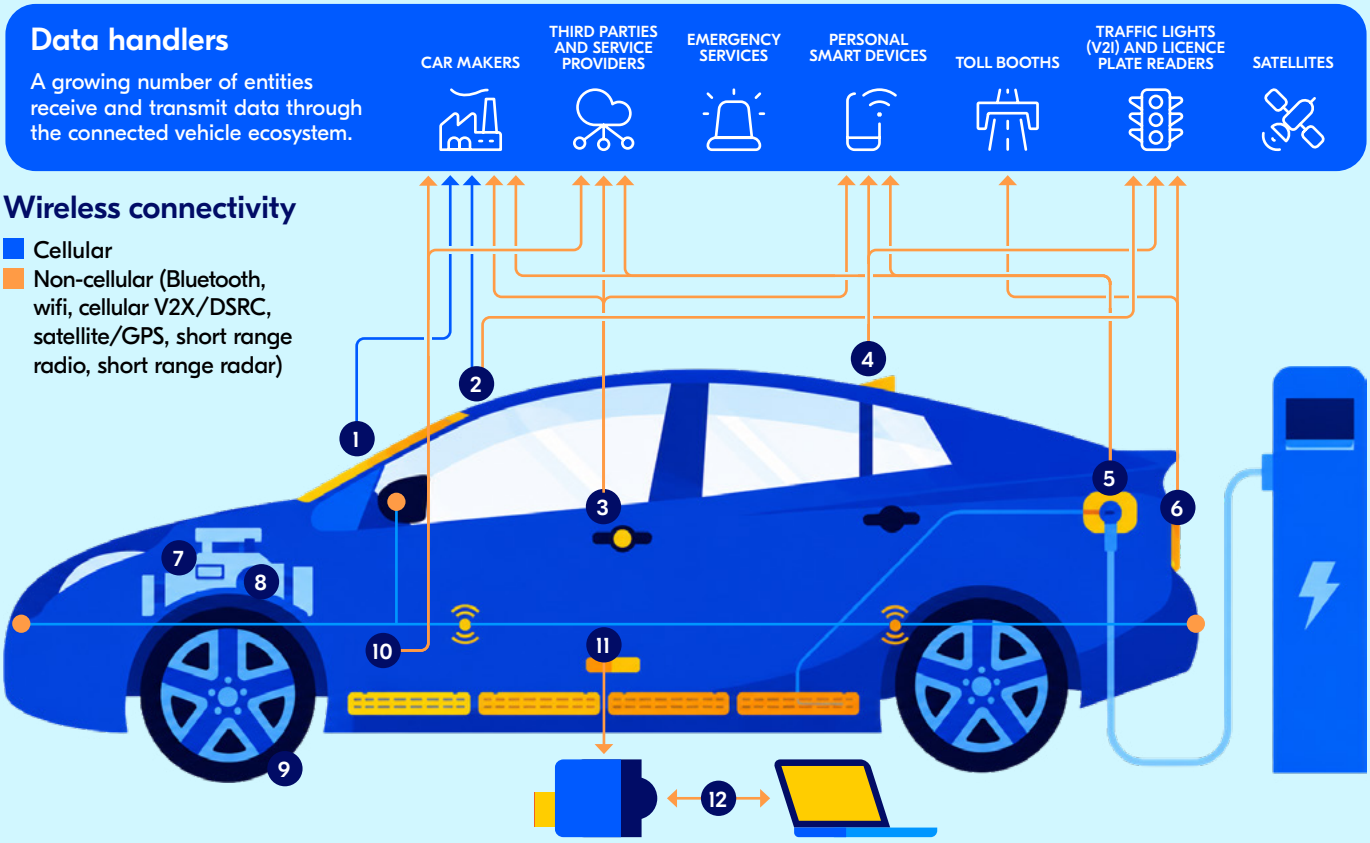
Central to these reforms must be an unequivocal right for car buyers to withdraw or restrict consent for non-essential, opaque or excessive collection of identifiable personal data at the point of sale or subsequently, without penalty, and without loss of core vehicle functionality or degradation of safety-critical features. This right should sit alongside a clear ability for motorists to actively authorise trusted third parties, such as emergency and roadside assistance providers, to access relevant data for clear, limited and beneficial purposes.

The motor vehicle service and repair information sharing scheme is also relevant as vehicles become more software-dependent. Independent repairers and roadside assistance providers may increasingly need access to diagnostic, software related repair information to identify and resolve faults safely.[61] Any future connected vehicle data framework should ensure that protections do not unintentionally prevent legitimate repair, diagnostics and roadside assistance.

[58] Rountree, D., Fisher, J., & Lustig, M. Data driven: Navigating the legal and regulatory backroads for connected vehicles. Allens. https://www.allens.com.au/insights-news/insights/2026/02/data-driven-navigating-the-legal-and-regulatory-backroads-for-connected-vehicles/
[59] Rountree, D., Fisher, J., & Lustig, M. Data driven: Navigating the legal and regulatory backroads for connected vehicles. Allens. https://www.allens.com.au/insights-news/insights/2026/02/data-driven-navigating-the-legal-and-regulatory-backroads-for-connected-vehicles/
[60] Office of the Australian Information Commissioner. OAIC regulatory priorities. https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/oaic-regulatory-priorities
[61] Rountree, D., Fisher, J., & Lustig, M. Data driven: Navigating the legal and regulatory backroads for connected vehicles. Allens. https://www.allens.com.au/insights-news/insights/2026/02/data-driven-navigating-the-legal-and-regulatory-backroads-for-connected-vehicles/

A principles-based approach to connected vehicle data

Connected vehicle data should be regulated on a risk-based, principles-led basis rather than as a single data class.[62] Data that is identifiable or reasonably re-identifiable can create privacy and consumer harms, particularly when it reveals location, driving behaviour, in-cabin activity, linked-device information, or other sensitive details.[63] At the same time, appropriately de-identified and aggregated data can support road safety analysis, infrastructure planning, congestion management, regulatory oversight, and transport policy.[64] A pro-consumer framework should therefore protect identifiable vehicle data, enable responsible public-interest uses of aggregated data, and allow motorists to authorise trusted service providers to access relevant data for limited and beneficial purposes.



Legend

1. Front, rear, and windshield sensors
2. External vehicle imaging and scanning
3. Biometric access
4. Dedicated Short-Range Communications (DSRC) radio
5. Charging device
6. Number plate
7. Telematics control unit (TCU) and electronic control unit (ECU)
8. Vehicle communications network
9. Tyre pressure sensors
10. Third-party monitoring device
11. Event data recorder
12. Crash data retrieval unit

Source: FPF.org

Vehicle design and safety standards

The DITRDCA leads national policy for connected and autonomous vehicles, manages vehicle safety standards, and tracks international developments to guide future regulation. The NTC is leading reforms for managing vehicle generated data and AV safety, including new laws that will set ongoing safety responsibilities and monitoring requirements for companies that operate autonomous driving systems. Austroads supports this work by assessing practical issues around connected vehicle technology, such as secure communications and infrastructure readiness across states and territories.

The Road Vehicle Standards Act allows the federal government to set mandatory safety and design rules for vehicles sold in Australia. While current vehicle standards do not yet include specific cyber security requirements, they allow manufacturers to meet recognised international cyber security and software update standards instead. This provides a pathway for stronger cyber protections to be applied in the Australian market.

[62] Brady, M.. Data privacy and automated vehicles: Navigating the privacy continuum. Monash University Law Review, 45(3), 589–625. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839250

[63] Falk, A. UNSW privacy and security regulation for connected cars workshop [Speech transcript]. Office of the Australian Information Commissioner. https://www.oaic.gov.au/news/speeches/unsw-privacy-and-security-regulation-for-connected-cars-workshop & Allens. Data-driven: Navigating the legal and regulatory backroads for connected vehicles. https://www.allens.com.au/insights-news/insights/2026/02/data-driven-navigating-the-legal-and-regulatory-backroads-for-connected-vehicles/

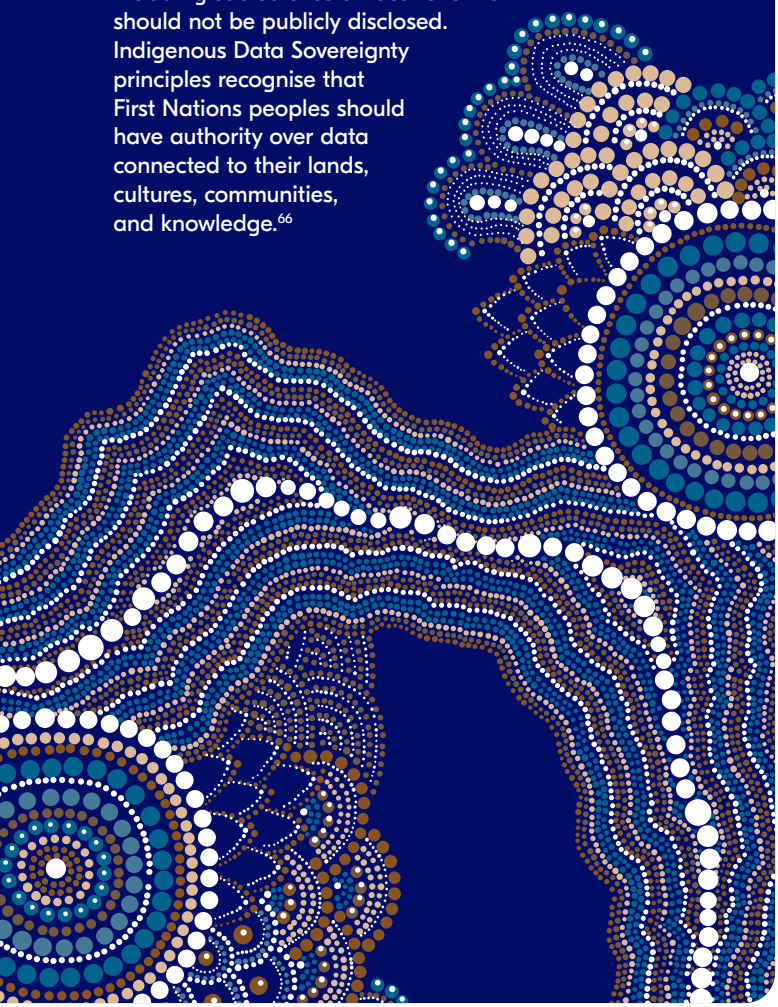
[64] Khanal, M., & Edelmann, N. Application of connected vehicle data to assess safety on roadways. Eng, 4(1), 259–275. https://doi.org/10.3390/eng4010015 & Michigan State University Innovation Center & Ford Mobility. Connected vehicle data validation: How do cv events relate to collision trends? https://innovationcenter.msu.edu/wp-content/uploads/2022/03/SafetyInsights_w4.pdf

Connected vehicle data, vulnerable people and sacred spaces

Connected vehicle data can reveal more than how a vehicle is used. It can show where people live, where they work, where they regularly travel, and which places they visit. This creates risks not only for vehicle owners, but also for passengers, vulnerable people, communities, and custodians of culturally sensitive locations.

In domestic and family violence situations, connected vehicle apps and location data can be misused by controlling or abusive individuals to monitor, stalk, restrict, or control another person's movements, often without knowledge of the person under surveillance. It may reveal how many people are travelling in a vehicle and facilitate monitoring of what they say or do. Location data may reveal where someone has been, where they are likely to go, or whether they have left a particular area. In some cases, connected services may also allow remote access to vehicle functions, creating another pathway for coercive control.[65]

Connected vehicle data can also create risks for Aboriginal and Torres Strait Islander communities if movement data exposes culturally sensitive places, including sacred sites or locations that should not be publicly disclosed. Indigenous Data Sovereignty principles recognise that First Nations peoples should have authority over data connected to their lands, cultures, communities, and knowledge.[66]



Telecommunications regulatory consideration

If a vehicle manufacturer provides internet or communication services as part of a connected vehicle, it may fall under existing telecommunications consumer protection rules, including complaint handling and service standards. The Department of Communications has consulted on whether Australia's current telecommunications regulations are suitable for connected vehicles, but final decisions have not yet been made.

Cyber security regulation and oversight

The Cyber Security Act 2024 introduced mandatory cyber security requirements for certain consumer smart devices (does not apply to road vehicles or vehicle components). Manufacturers and suppliers must meet minimum security standards, such as using secure default settings, fixing known vulnerabilities, providing timely software updates, and clearly informing consumers about security features and support periods. Regulators can enforce these rules through audits, penalties, and ongoing compliance checks. A dedicated regulatory instrument, designed specifically for vehicles, would be a more appropriate way to mandate cyber security standards for the automotive sector rather than expanding the existing smart device regime.

In the energy sector, governments are also working to strengthen cyber security rules for EVs and charging infrastructure through the Consumer Energy Resources Roadmap. This process is expected to introduce nationally consistent standards for device security, system interoperability, secure authentication, and ongoing maintenance.[67] For now, Australia's minimum standards for public EV charging focus mainly on design, payments, reliability, and customer service, and do not yet include specific cyber security requirements, leaving an important gap in protections.

AV frameworks

Australian governments are working together to establish a comprehensive regulatory framework for the safe commercial deployment of AVs. This end-to-end framework will include:

- **National AV Safety Law (AVSL):** New legislation to govern the safety of autonomous driving systems, expected to be in place in the coming years. This will provide the legal foundation for AVs to operate on public roads.
- **AV in-service safety regulator:** A dedicated body responsible for ongoing oversight of AV safety once vehicles enter service.
- **Vehicle standards for AVs:** Technical requirements aligned with international standards, particularly those developed by the United Nations World Forum for Harmonisation of Vehicle Regulations.
- **State and territory laws:** Regulation of AV users, registration, and operational requirements will remain under state and territory jurisdiction, though national consistency is a key objective.

The regulatory framework for AVs is being developed with security as a baseline consideration, including requirements to guard against third-party interference and cyber-attacks. However, specific cyber security standards and assurance mechanisms for AVs are still evolving.[68]

[65] Australian Human Rights Institute. Technology facilitated abuse using connected cars: Gaps, limitations and supporting victim-survivor safety. UNSW Sydney. https://www.humanrights.unsw.edu.au/research/current-research/technology-facilitated-abuse-connected-cars

[66] Aboriginal Areas Protection Authority. About sacred sites. Northern Territory Government. https://www.aapant.org.au/sacred-sites/about-sacred-sites & Janke, T., McKenzie, C., & Carter, N. Indigenous Data Sovereignty: The legal and cultural considerations. Terri Janke and Company. https://www.terrijanke.com.au/post/indigenous-data-sovereignty-the-legal-and-cultural-considerations

[67] Department of Climate Change, Energy, the Environment and Water. National consumer energy resources roadmap. https://www.energy.gov.au/sites/default/files/2024-07/national-consumer-energy-resources-roadmap.pdf

[68] Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. National road transport technology strategy. https://www.infrastructure.gov.au/department/media/publications/national-road-transport-technology-strategy

Critical infrastructure provisions

Australia's cyber security laws impose mandatory obligations on operators of designated critical infrastructure assets under the national Security of Critical Infrastructure (SOCI) framework, while most other businesses are guided mainly by voluntary standards. In the transport sector, critical infrastructure includes assets such as major ports, freight network infrastructure, public transport systems, and major airports. Outside of vehicle safety standards and general obligations under privacy and consumer law, most cyber security measures in the transport and EV charging sectors remain voluntary, supported by government guidance and best practice frameworks rather than mandatory rules.

EV charging networks are not currently classified as critical infrastructure in Australia. This differs from the European Union, where charging point operators are treated as either 'essential' or 'important' entities and must meet mandatory cyber security obligations, with both categories subject to mandatory cyber security risk management and incident reporting obligations under EU NIS2.[69] This direction may influence future reforms in Australia.

Interoperability standards for EV charging

Australia is starting to adopt minimum technical requirements for EV charging equipment, particularly where chargers interact with the electricity system (e.g. smart and bidirectional charging). These developments are occurring through national energy policy and standards processes, overseen by Energy Ministers and implemented via market bodies and standards organisations.

Current initiatives focus on:

- Interoperability and communications (e.g. Most optimal versions of OCPP).
- Grid security and stability, especially where chargers provide flexible load or export services (e.g. recent changes to Australia's grid connection code AS/NZS 4777.2).

[69] NIS2 stands for the Network and Information Security Directive 2 (Directive (EU) 2022/2555). It is the European Union's updated cyber security law that replaced the original 2016 NIS Directive.

Bidirectional charging

Recent updates to Australian grid connection standards allow EVs to send power back to homes and the electricity grid. This has opened the door for wider use of technologies such as vehicle-to-home and vehicle-to-grid charging. However, these standards focus mainly on electrical safety and do not yet include clear cyber security or compatibility requirements. As a result, security is largely left to voluntary industry practices rather than firm rules.

The National Roadmap for Bidirectional EV Charging sets out a long-term vision for expanding these technologies and highlights their potential benefits for consumers and the electricity system. However, it does not set minimum standards for secure communication or data protection.[70]

While Australia is making it easier for bidirectional charging to grow, the security and interoperability foundations needed for safe and reliable operation are still developing. Stronger policy direction and consistent standards will be needed to support long-term success. This work is being supported by a new government-funded industry collaboration called Vehicle-Grid Network.

> **"Stronger policy direction and consistent standards will be needed to support long-term success."**

[70] Australian Renewable Energy Agency. National roadmap for bidirectional EV charging in Australia. https://arena.gov.au/knowledge-bank/national-roadmap-for-bidirectional-ev-charging-in-australia/

Recommendations

RECOMMENDATION 1

Strengthen privacy protections for vehicle telematics and in-car data

A pro-consumer connected vehicle data framework must ensure motorists can access their vehicle data and direct it to trusted third parties of their choice for clear and limited purposes. Motorists deserve clear, honest information about how their data is collected and used, and connected vehicles must handle that data in ways that respect their rights rather than exploit their reliance on modern mobility technology. Today, identifiable connected vehicle data is too often collected, used, shared, and retained without transparency, clear justification, or meaningful consumer control, which is particularly concerning where data can reveal location, driving behaviour, passenger activity, or other sensitive details.

A stronger consumer framework should not prevent beneficial data use. Properly anonymised and aggregated data should remain available for public-interest purposes such as road safety, infrastructure planning, and regulatory oversight, and motorists should be able to actively authorise trusted providers to access their data for specific services including roadside assistance and fault diagnosis.

Better protections also require stronger incentives for vehicle suppliers to assess data-related risks and reduce them. This means designing privacy-protective processes from the outset, with built-in safeguards ensuring data is collected and used only when necessary and for a clearly stated purpose. These controls must also reliably detect and stop any use or sharing beyond that purpose, by both the vehicle supplier and any third parties handling the data. The goal is a shift in data governance that makes privacy, safety, and security the default rather than the exception.

The NRMA calls for:

- Transparent and meaningful consent, including privacy notices across all brands with limits on data collection and retention, amendments to the Privacy Act to ensure connected vehicle data is only collected and used fairly and reasonably, stronger consumer law safeguards against unfair standard form terms that obtain broad or open-ended consent, and separate consent pathways for essential, optional and secondary data uses — with an unequivocal right for consumers to refuse or withdraw consent for non-essential, opaque or excessive collection at the point of sale or at any subsequent time, without loss of access to core vehicle functions, safety features or manufacturer warranty entitlements,
- Privacy-by-design requirements for connected vehicle services, including clear data classification rules distinguishing between stored vehicle data, shared service data, broadcast communications data, identifiable personal data, and properly anonymised and aggregated system-level data,
- Fair and transparent access to essential vehicle data, with the owner's active authorisation, to support emergency assistance, roadside assistance, and vehicle repair,
- Support for properly anonymised and aggregated connected vehicle data for road safety, infrastructure planning, congestion management and regulatory purposes, where individuals cannot reasonably be re-identified,
- Enforceable and standardised rules governing the sharing of telematics data with insurers, advertisers and third-party apps, and
- Enforceable regulatory backing for all of the above, rather than reliance on voluntary industry codes.

RECOMMENDATION 2

Set nationally consistent cyber security and interoperability standards

Australians should be protected from cyber security and data protection risks introduced through connected vehicles, EV chargers and their supporting software ecosystems. Fragmented requirements across states and territories create costs for industry that inevitably get passed through to motorists, but they also create uneven security settings. A consistent national motoring digital security framework would reduce cyber risk, improve community confidence and support safer integration with the electricity grid.

The NRMA calls for nationally aligned:

- vehicle data-governance rules that distinguish between identifiable personal data, properly anonymised and aggregated system-level data, and consumer-authorised sharing with trusted third parties,
- mandatory standards for connected vehicle cyber security and data protection,
- optimal cyber security and interoperability requirements for public and home charging infrastructure,
- supply chain assurance measures including software transparency, verified sources, secure-by-design practices and third-party risk management across vehicles, chargers, telematics systems, apps and payment platforms.

RECOMMENDATION 3

Strengthen incident reporting, consumer protections and recall mechanisms

When cyber incidents affect vehicle safety, charging access or personal data, motorists need rapid and transparent notification. Australia should establish clearly defined:

- national automotive cyber incident reporting scheme,
- emergency response protocols for automotive cyber incidents,
- recall mechanisms for cyber security defects, and
- guaranteed consumer remedies when digital failures affect safety or mobility.

RECOMMENDATION 4

Educate and inform consumers on staying safe in a connected motoring environment

The NRMA supports proactive and targeted public education campaigns that help motorists understand:

- how to protect their data,
- how to identify cyber security risks,
- how digital keys and apps should be secured, and
- what rights they have when something goes wrong.