National Motor Vehicle Theft Reduction Council

Preparedness for Connected and Automated Vehicles (CAVs)

Vehicle tracking and remote vehicle functions

September 2021

PREPARED BY:
IAG Research Centre

Informing Australia on vehicle crime.

ISBN: 978-1-876704-72-8

Contents

1. Executive Summary

IAG Research has performed a scan of the major vehicle manufacturers for the Australian market to uncover what vehicle tracking capabilities they have as well as the ease and process used by criminals to disable these systems. The results of the scan are detailed in sections 3 and 4 of this report.

There are two main methods for vehicle manufacturers to implement connectivity within their vehicles.

- The first is an integrated system that connects to a cellular network which reports back to a main server. It is primarily used for the SOS emergency feature in an event of an accident or for the use of tracking stolen vehicles, for example, like General Motors' OnStar. Data sent from the vehicle includes time of accident, cause of activation, GPS coordinates and Vehicle Identification Number (VIN).

- The second method is via mobile applications which allow for remote vehicle capabilities. These apps have features that are able to be accessed anywhere and allow for remotely locking/unlocking the doors, starting or stopping the engine, setting the climate control or even sending live GPS coordinates.

There are different meanings of tracking, depending on the context. It could mean any of the following:

- A relay of real-time GPS coordinates, whereby the vehicle communicates via the in-built SIM card installed, in the exact same way your mobile phone tracks your phone's position. It is seen via a connected app and even historical data of previous trips can be viewed by the owner.

- Tracking for other services presented via the head unit or centre screen, for example, route information, live traffic updates and speed limits warnings. For areas with no reception, like tunnels, the vehicle uses a predictive algorithm to determine position until reception is restored.

- Tracking done outside of the view of the customer. It is done so through the cellular system "pinging" the vehicle GPS coordinates back to manufacturer-operated servers every few seconds. This data does contain vehicle-identifiable data and is on-sold to third parties. This data is virtually impossible to get without a formal agreement in place with the manufacturers.

There are also third-party tracking devices that are used in fleets, for vehicles that are financed, and for personal anti-theft reasons. These offer a host of additional functionalities, such as remotely cutting off the fuel lines in the event of theft, turning the vehicle into a Wi-Fi hotspot, driver safety scores, vehicle history log, and even the ability to dial the installed SIM card to hear what is being said near the tracker. Some use batteries and can be placed virtually anywhere in the vehicle via magnets, others can be wired directly into the vehicle's architecture.

The increase in technology, and specifically of vehicle tracking capabilities, has provided law enforcement with a new utility for conducting investigations. However, criminals have already understood the implications of these systems and have begun to innovate ways of turning them off once in vehicles they have either stolen or used in other crimes. Once the system has been thoroughly defeated, there is no known way for the vehicle to be tracked (other than through traditional methods, e.g. traffic cameras, CCTV, etc.).

Owners of vehicles can opt out of many of these services, but the cellular and telematics systems seem to be a crucial part of the vehicle architecture and switching them off may also affect other vehicle behaviors. The claim to much of this data is also up for debate with various stances taken by courts around the world, and often varying between states within the same country.

Comments provided by NSW Police suggest there is a significant legal process if it is at all possible to activate and access a vehicle tracker if the vehicle belongs to the suspect being investigated. The process is much simpler if the vehicle is stolen and the owner provides permission to track their vehicle. This can and does include remotely activating a tracking device that was otherwise deactivated.

2. Project Objective

The objective for this project is to perform a market scan of vehicles manufacturers to determine whether their vehicles are equipped with tracking technologies for police and investigation purposes.

The insights provided will enable law enforcement a better understanding of how to track vehicles using the manufacturer's mobile app or the vehicle's integrated systems, with the aim to assist them in their investigations. The integrated systems offered by some manufacturers also have the capability to call emergency services to the scene of an accident through the recorded GPS location from the vehicle.

Connected vehicles give consumers the ability to track and monitor their vehicles from the convenience of their mobile phones. Mobile apps offered by vehicle manufacturers can come with a host of other personal convenience features such as, but not limited to; remote entry, heating ventilation air-conditioning (HVAC) controls, fuel level, battery charge (EVs), range (EVs), destination logs and vehicle maintenance. Available features vary according to make, year and model.

3. OEM apps

The list of compatible models below highlights the breadth of model offered by the manufacturer to give an understanding of the scope of the market. The vehicles specified below have the ability for remote tracking via an integrated cellular system or a mobile app. The information collected for this research is based on Australian and overseas sources and may not be exhaustive.

3.1 BMW

App name: my BMW.

Key functions: GPS tracking, remote entry, remote climate controls, activation of headlights and ability to manage their maintenance services.

Additional information: the integrated Intelligent Emergency Call systems allows data to be sent to the Emergency Call Centre to decide what rescue measure is required. The system is automatically activated in the event of an accident or manually by pressing the SOS button located near the rear-view mirror. The data includes GPS location, number of airbags deployed and an estimation of the severity level.[1,2]

Technical information: inside the roof aerial is a GPS and a telematic antenna included (figures 1,2 of Section 4). Both are connected directly to the communication module (ATM/TCB). The communication module is then connected to the main head-unit/iDrive computer. The vehicle's GPS location is stored in the telematic communication box (TCB) module.

Compatible 2021 BMW Models: BMW 1 and 2 Series – standard on M140i, 230i and M240i, optional on other variants.

BMW 3 Series sedan and Touring – standard on 330i, 330e and 340i, optional on other variants.

BMW 3 Series Gran Turismo – standard on 330i, optional on 320d.

BMW 4 Series – all variants.

BMW 6 Series – all variants.

BMW 7 Series – all variants (with touchscreen).

BMW X3 and X4 – standard on xDrive 28i and xDrive30d, optional on other variants.

BMW X5 and X6 – all variants (with touchscreen).

3.2 Ford

App name: Ford Pass.

Key functions: remote lock and unlock, remote start, vehicle status, remote vehicle monitoring, live traffic updates, GPS locator and vehicle health alerts.

Additional information: the service is free for Ford owners and is made possible by a FordPass Connect embedded modem that pairs with the user's smartphone app.[3]

Compatible 2021 Ford models:

Ford Everest.

Ford Ranger.

Ford Transit.

3.3 Honda

App name: HondaLink

Key functions: remote engine start, lock and unlock doors, automatic collision notifications, recall notifications, service appointments, roadside assistance, emergency call, speed alerts, security alarm alerts and stolen vehicle locator.

Additional information: the "Hondalink" app is currently only available for the American market. An additional feature of the service tracks the drivers' behaviour, provides tips and rewards insurance discount to those drivers based on their driving score. The subscription service is free for the first twelve months then $89 USD for subsequent years.[4]

Compatible 2021 Honda Models:

Honda Odyssey.

Honda Accord Sedan.

Honda Civic Coupe, Hatchback, and Sedan.

Honda Civic Si Coupe and Sedan.

Honda CR-V.

Honda Fit.

Honda HR-V.

Honda Insight.

Honda Pilot.

Honda Passport.

3.4 Hyundai

App name: Auto Link.

Key functions: view driving habits, fuel efficiency, GPS location, check tyre pressures and battery status using an OBD Bluetooth dongle.

The premium offering allowed users to remotely lock or unlock doors, remotely start or shutdown the engine, remotely adjust climate controls and remote vehicle tracking.

Additional information: Auto Link services were available for Australia and New Zealand from March 2017 to July 2020, (now discontinued). It has been speculated that the end of the Auto Link app could make way for Hyundai's Blue Link app which has a larger global footprint (currently operating in Europe and the US).

The Hyundai Blue Link app offered outside of Australia provides the same features while using an integrated 4G telematics system.[5]

Compatible Hyundai Models (from 2017-2020):

Hyundai Santa Fe Highlander.

Hyundai Kona Elite.

Hyundai I30 Elite.

3.5 KIA

App name: UVO.

Key functions: battery status information, remote climate control, GPS locator, remote door control, valet parking mode and vehicle status.

Additional information: Unfortunately, the suite of features including vehicle tracking is not available for the Australian market.[7,8]

Compatible Kia Models:

Kia e-Soul.

Kia Ceed MY20.

Kia Proceed MY20.

Kia X-Ceed MY20.

Kia e-Niro, Niro HEV and PHEV MY20 onwards.

Kia Sorento MY21.

Kia Sportage MY21.

Kia Rio MY21.

Kia Stonic MY21.

Kia Picanto MY21.

3.6 Mazda

App name: Mobile Start.

Key functions: remote engine start and stop, door lock and unlock, GPS location and panic alarm.

Additional information: Released in the US and Canada, Mobile Start is as complimentary one-year offering to new users with an annual renewal fee of 65 USD.

Compatible Mazda Models:

2016-2018 Mazda3: Available on all vehicle trim levels.

2016-2019 Mazda6: Available on all vehicle trim levels.

2016-2019 Mazda CX-3: Available on all vehicle trim levels.

2016-2019 Mazda CX-5: Available on all vehicle trim levels.

2016-2019 Mazda CX-9: Available on all vehicle trim levels.

3.7 Mercedes-Benz

App name: Mercedes me.

Key functions: vehicle tracker, theft notification, park damage detection, emergency call services, breakdown management, accident recovery, remote vehicle status, remote door locking and unlocking, geofencing, remote engine start and valet parking mode.

Additional information: the service is free for the first three years with plans for a subscription service at a later stage. [10]

Compatible Mercedes-Benz Models (from mid-2019 to current):

A-Class.

B-Class.

C-Class.

S-Class.

GLA-Class.

GLB-Class.

GLC-Class.

3.8 Tesla

App name: Tesla app.

Key functions: check charging progress, start/stop charging, remote climate control, remote lock/unlock, vehicle GPS tracker, remotely turn on lights and sound the horn, vent or close panoramic roof, summon vehicle out of garage or a tight parking space (for vehicles with Autopilot), and update your vehicle software from anywhere.

Additional information: Keyless driving (unlock and drive your car without your key), review service history, schedule a service appointment, check current range, valet mode (restrict access by hiding all personal data from the touchscreen, limiting maximum speed and performance and locking the front trunk and glove compartment).

Compatible 2021 Tesla Models:

Model S.

Model 3.

Model X.

3.9 Toyota

App name: Toyota Connected Services.

Key functions: Toyota Connected Services incorporates 4G technology which enhanced safety and security for its customers. The function has a button for manual activation of the SOS emergency call button or an automatic collision notification which connects to emergency services when a serious accident is detected.

Stolen vehicle tracking can assist police track a stolen vehicle with the help of their Stolen Vehicle Tracking Call Centre. This feature is dependent on vehicle battery power, 4G mobile network coverage, GPS signal strength and other factors outside of Toyota's control.[11]

Additional information: the following guide on stolen vehicle recovery has been taken from Toyota's website: [12]

> ***Report.***
>
> *In the unfortunate event of a stolen vehicle, you should first file a stolen vehicle report with the police.*
>
> ***Contact.***
>
> *Contact Toyota Stolen Vehicle Assistance and quote your police report number and VIN.*
>
> ***Trace.***
>
> *Your Toyota agent will coordinate with the police and provide them with your vehicle's location information.*
>
> *Note: Stolen Vehicle Tracking can only be authorised when the owner of the vehicle provides us with a valid police report number. Location data remains secure and protected and will only be shared with police to assist with recovery of your vehicle.*

Compatible 2021 Toyota Models:

Toyota Yaris Cross.

Toyota Camry.

Toyota Hilux.

3.10 Volkswagen

App name: Car-Net.

Key functions: remote start/stop, parking features, remote lock/unlock, diagnostics and maintenance, active crash notification, anti-theft alerts, set speed limits, geofencing and boundary alerts, valet alerts, emergency information assistance, and stolen vehicle locator.[14]

Additional information: By enrolling in the DriveView program, Car-Net users may be eligible for discounted rates from some of the top automotive insurance companies in the country. This program can also help Car-Net users monitor their driving by tracking activities like night driving, hard braking, idle time, and excess speed. [14]

VW Car-Net Hotspot allows passengers to access the internet with up to four connected devices simultaneously, including compatible tablets, smartphones, laptops, gaming devices, and more - at 4G LTE–enabled speed. [14]

Compatible VW 2014-2020 models:

VW CC.

VW EOS.

VW Beetle (Convertible and Coupe).

VW Jetta (SE with Connectivity, SEL, TDI, GLI, and Hybrid).

VW Passat (SE, SEL Premium, including TDI and VR6).

VW Tiguan (SEL, R-Line and Limited).

VW Golf/GTI/R/SportWagen, e-Golf and Golf Alltrack.

VW Arteon.

Note: currently, there does not seem to be any capability for remote engine immobilisation (REI) for any of the makes and models listed above here in Australia, at least not to the extent that this information was found by IAG Research during its investigations.

We are not seeing systems like GM's OnStar being replicated en-masse in Australia, with only a handful of manufacturers adopting similar technology, among which include Tesla, Ford and Toyota.

Some articles suggest part of the issue lies in existing infrastructure requiring upgrading to allow for reliable functionality of this feature.

4. Disabling GPS tracking systems

The Queensland Police have indicated concerns about thieves being able to turn off GPS tracking with relative ease, in some instances, it resembles the simplicity of turning off location services on a mobile phone.

This concern was also verified independently by our contact in NSW Police, that stated “a number of offenders have specific technical knowledge of the placement of various high-end motor vehicles which are fitted with factory GPS tracking devices and seek to remove the device.”

Our research has led us to various methods of disabling GPS tracking, which depends greatly on the make and model of the vehicle. Some examples of these methods are listed below, but haven’t been physically verified or tested by IAG Research.

This is not comprehensive coverage of each make and model listed in section 3, rather it serves to provide a broad overview of some of the different techniques used. It also serves to highlight how easily some of this information can be obtained via enthusiast and mechanic forums, or similar open-sources discoverable by an average user on the Internet.

BMW: Vehicles are equipped with an "internal SIM card" (telematic control unit). Through this SIM card it is possible to locate vehicles.

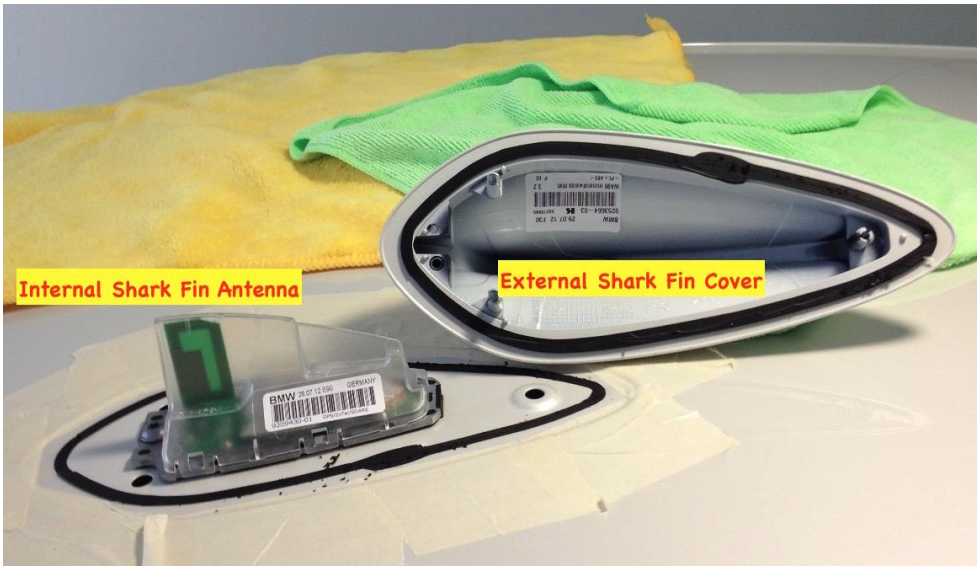
To disable the SIM card system there are two options.

1) Simply disconnect the telematic control unit or pull the relevant fuse.

2) Deactivate the internal SIM from BMW directly. To do this, you must contact your local BMW dealer that can then send this request directly to BMW, who will then disable the internal SIM card of the vehicle.

In both cases, connected drive (online) services won’t work anymore, e.g. BMW assist, as it all runs through the same SIM card. The GPS system should continue to work as it uses a different antenna. Disconnecting the antenna will disable this secondary system.

In both cases, it may also result in a permanent SOS error on the screen/iDrive instrument cluster. [23, 24]



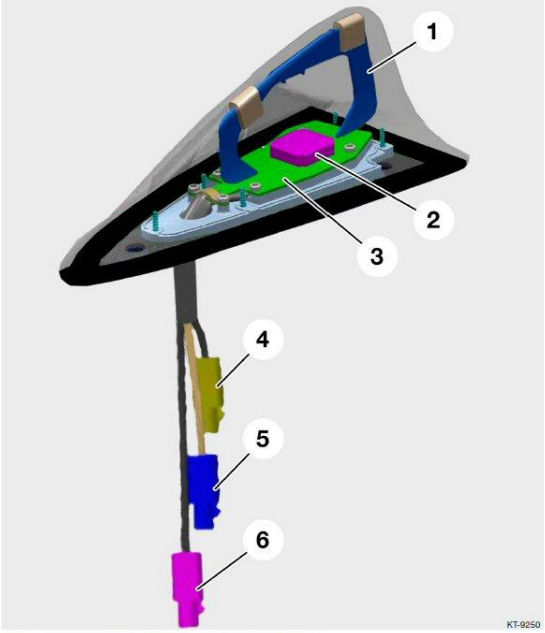
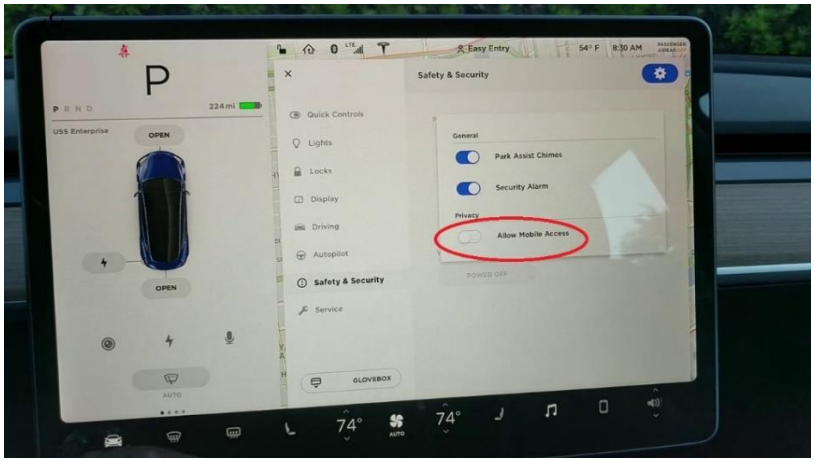


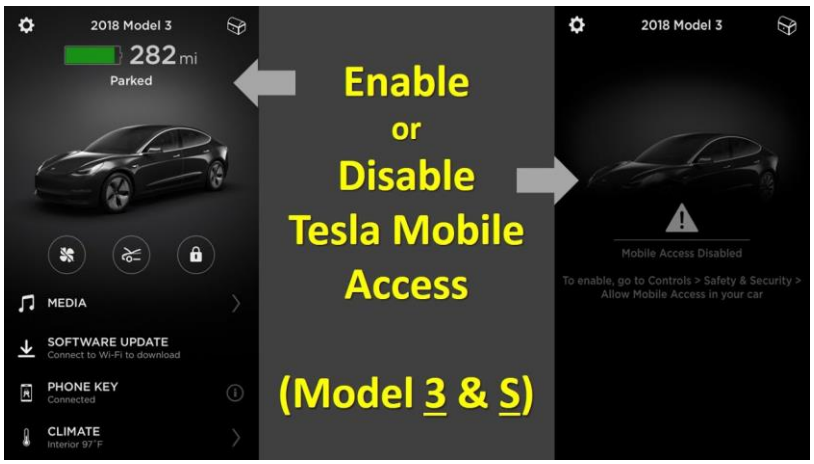
Fig. 33: Inner view of the GSM aerial (US version)

Index	Description	Index	Description
1	Group emitters of the GSM antenna	4	Connection for dual-band (US)
2	GPS aerial	5	Connection for GSM
3	Electronic evaluation unit	6	GPS connector

Figures 1, 2: Images showing telematic communication box (TCB) location inside a BMW “shark fin” antenna. [31, 32]

Tesla: Go to Controls / Settings / Safety & Security and turn off Allow Mobile Access.



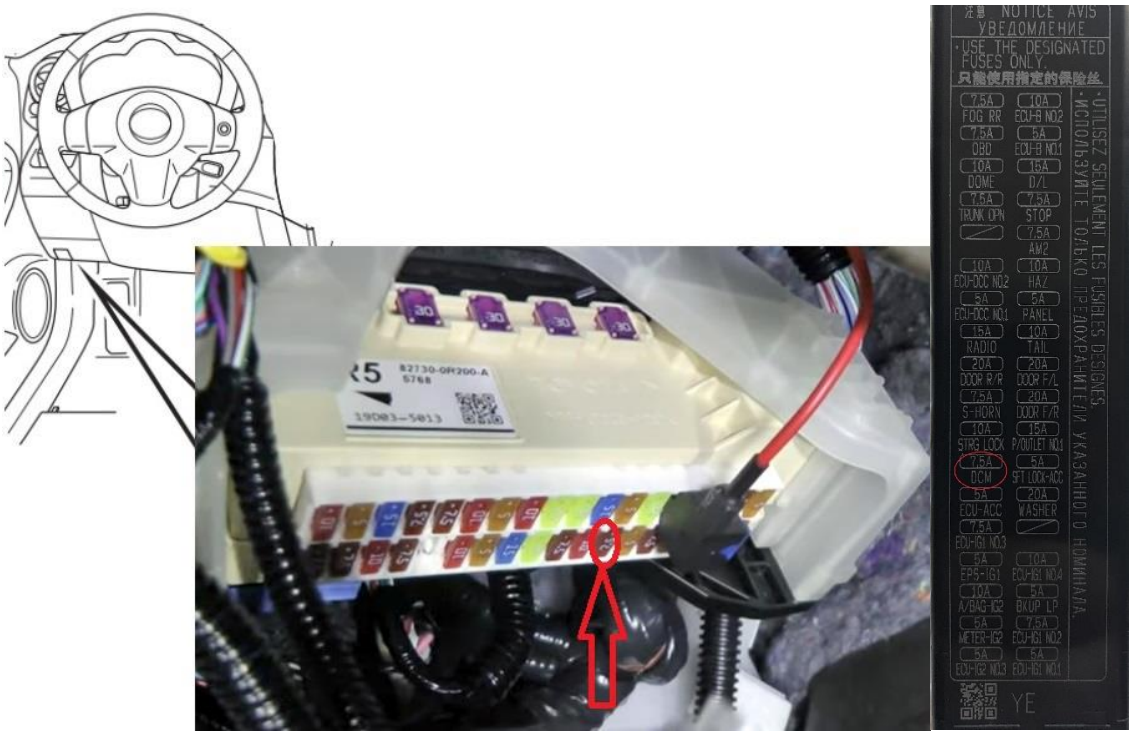


Images (from top): top figure shows how and where to switch off mobile access from the centre screen, the bottom figure shows what it looks like in the app before and after access has been disabled.

This will disable access for all registered users of the app so they can't see or track the vehicle. Tesla will still be able to see the vehicle via GPS, so the second part to the process is removing the GPS antenna, as outlined in References [42].

Note: the last known location before the GPS antenna is disconnected will remain as the vehicle's "current location".

Toyota: Removing the 7.5 Amp Data Communication Module (DCM) fuse in the fuse box (claimed).



Figures: showing the DCM fuse and where the fuse box location [44, 45].

Removing this component may have additional unwanted effects on other functions, such as connected services, SOS service, audio issues, warning messages, etc. The detailed process can be found in References [35,36].

Disconnecting the GPS antenna under the dash is also claimed to work but will render Sat-Nav, radio, Bluetooth, weather and traffic alerts un-useable.

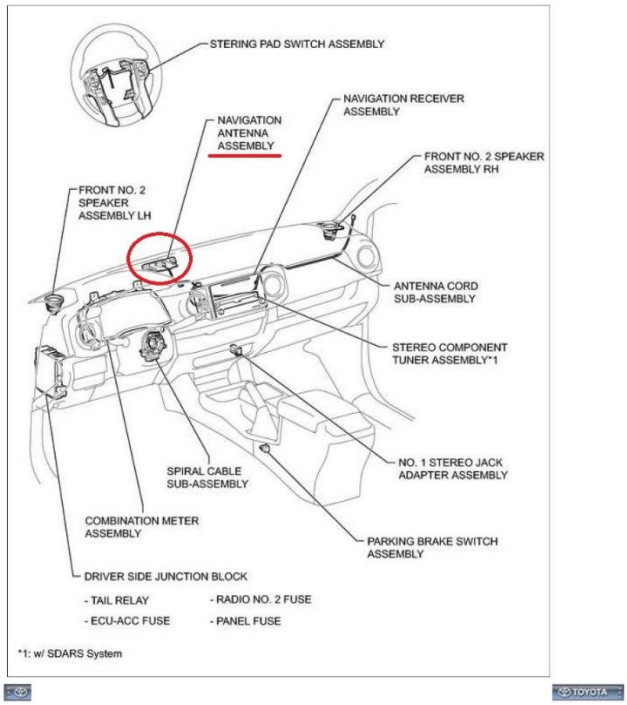


Figure: location of GPS antenna [43].

4.1 Considerations for two-factor authentication to disable tracking

Our discussions with NMVTRC and Queensland Police have uncovered a desire for manufacturers to install some sort of second form of verification when disabling tracking, for example, something like what you can elect to have when logging into Facebook.

This idea is simple enough and warranted in its approach, however, raises questions that would need answering before diving deeper into the design of what such a system may look like. Some of these questions include:

- How do you get buy-in from the manufacturers?
- Is there a standard they should adopt or model their systems on?
- How do you reset the verification system if a second or third owner purchases a vehicle?
- How does the reset system avoid being defeated by thieves? There would likely be a “restore back to factory settings” option which would be an easy way to overcome it.
- If in the case you would have to take the vehicle into a dealer, how do they verify you are the owner?
- Do multiple drivers (e.g. shared household vehicle) have different codes to disable? If so, how does the vehicle tell who is driving the vehicle and when to switch tracking on or off?
- Is there a master key? How long before it gets leaked or broken? How complex is it?

The difference here is that vehicles are used for a limited time before they are on-sold to someone else. This differs from personal things such as email or social media accounts that are tied to one person forever (essentially). That small difference complicates how the system should be designed and implemented.

We believe more research is required to take this beyond an idea and develop it into a serious consideration for implementation by manufacturers. Namely, what would be the benefit for the manufacturer to invest their time and resources into developing a new system, one that could potentially come to embarrass them if it fails or is hacked early in its lifecycle?

5. Conclusion

Features that increase convenience are being driven by consumer demand, however the technology required to implement them increases the number of available attack vectors, for example, Bluetooth and Wi-Fi.

There are two main methods for vehicle manufacturers to implement connectivity within their vehicles. The first is an integrated system that connects to a cellular network which reports back to a main server. It is primarily used for the SOS emergency feature in an event of an accident or for the use of tracking stolen vehicles. Data sent from the vehicle includes time of accident, cause of activation, GPS coordinates and Vehicle Identification Number (VIN).

The second method is via a mobile app which allows for remote vehicle capabilities. Despite security efforts from developers, there have been attacks on vehicles through the manufacturers' own (and third-party) apps. There is also a concern with the tracking of vehicles after being sold to a second or third buyer who is not made aware of any data licensing agreements, and which can lead to unauthorised access.

The global market shows there is an appetite for connected services, and it is inevitable that more services will be offered in the emerging Australian market. Whilst not all manufacturers offer mobile apps or vehicle tracking services, it is still possible they track the vehicles for individual data which can be on-sold to third-party companies.

6. Appendix I

6.1.1 Summary of results

Manufacturer	Implementation	Available in Australia	Vehicle Tracking	Vehicle model
BMW	Integrated & Mobile app	Yes	Yes	(Current Models) BMW 1 and 2 Series – standard on M140i, 230i and M240i, optional on other variants BMW 3 Series sedan and Touring – standard on 330i, 330e and 340i, optional on other variants BMW 3 Series Gran Turismo – standard on 330i, optional on 320d BMW 4 Series – all variants BMW 6 Series – all variants BMW 7 Series – all variants (with touchscreen) BMW X3 and X4 – standard on xDrive 28i and xDrive30d, optional on other variants BMW X5 and X6 – all variants (with touchscreen)
Ford	Mobile app	Yes	Yes	(Current Models) Ford Everest Ford Ranger Ford Transit
Honda	Mobile app	No	Yes	(Current Models) Honda Odyssey Honda Accord Sedan Honda Civic Coupe, Hatchback, and Sedan Honda Civic Si Coupe and Sedan Honda CR-V Honda Fit Honda HR-V Honda Insight Honda Pilot Honda Passport
Hyundai	Mobile app	No, ended 07/2020	Yes	(2017-2020) Hyundai Santa Fe Highlander Hyundai Kona Elite Hyundai I30 Elite
Kia	Mobile app	No	Yes	Kia e-Soul MY20 Kia Ceed MY20 Kia Proceed MY20 Kia X-Ceed MY20 Kia e-Niro, Niro HEV and PHEV MY20 onwards Kia Sorento MY21 Kia Sportage MY21 Kia Rio MY21 Kia Stonic MY21 Kia Picanto MY21
Mazda	Mobile app	No	Yes	2016-2018 Mazda3: Available on all vehicle trim levels 2016-2019 Mazda6: Available on all vehicle trim levels 2016-2019 Mazda CX-3: Available on all vehicle trim levels 2016-2019 Mazda CX-5: Available on all vehicle trim levels 2016-2019 Mazda CX-9: Available on all vehicle trim levels

Mercedes-Benz	Mobile app	Yes	Yes	(Current Models) A-Class B-Class C-Class S-Class GLA-Class GLB-Class GLC-Class
Toyota	Integrated & Mobile app	Yes	Yes	(Current models) Toyota Yaris Cross Toyota Camry Toyota Hilux
Volkswagen	Mobile app	No	Yes	(Selected 2014 to current) VW CC VW EOS VW Beetle (Convertible and Coupe) VW Jetta (SE with Connectivity, SEL, TDI, GLI, and Hybrid) VW Passat (SE, SEL Premium, including TDI and VR6) VW Tiguan (SEL, R-Line and Limited) VW Golf/GTI/R/SportWagen, e-Golf and Golf Alltrack VW Arteon

7. Appendix II

7.1.1 Inquiry into Vehicle Safety, Standards and Technology, including Engine Immobiliser Technology

On Wednesday 24 February 2021 the Legislative Assembly agreed to a motion that the Transport and Resources Committee inquire and report on vehicle safety, standards and technology, including engine immobiliser technology. The committee is required to report to the Legislative Assembly within six months.

The terms of reference are that the committee will inquire into and report on:

1. Options to reduce or prevent vehicles being used illegally or dangerously on Queensland roads, including vehicle engine immobilisation technology, non-technology options, operational considerations or other measures;

2. Lessons learned from other jurisdictions, particularly regarding the implementation of vehicle engine immobilisation technology to the existing vehicle fleet;

3. The Commonwealth's role in relation to vehicle standards and safety, and measures the Commonwealth could take, including requiring all new vehicles to be fitted with remote engine immobilisation technology;

4. The effectiveness of any proposed measures in improving road safety, preventing crime and assisting police in operational matters;

5. A recommended framework for legislative, policy and operational implementation of any proposed measures;

6. The benefit to and role of insurers in supporting any recommended measures;

7. Options to improve vehicle standards and safety in Queensland, including in relation to the:

    a. current Australian vehicle design rules;

    b. inspection regime for registered vehicles;

    c. pre-sale certification scheme, including measures to reduce fraud and improve consumer safety;

    d. management of written-off vehicles and 're-birthing';

    e. after-market vehicle modification framework, including achieving consistency to ensure best alignment with other Australian jurisdictions.

Report due date:

Tuesday 24 August 2021

Statement from the Record of Proceedings from the First Session of the Fifty Seventh Parliament, Wednesday 24 February 2021.

In speaking briefly to the motion, this is something for which Ian Leavers from the Queensland Police Union has been advocating for some time and I am personally a very strong supporter of it as well. This government has led the charge at ministerial council meetings of federal and state lawmakers in Canberra on this topic. We put remote vehicle immobilisers on the national agenda. This inquiry now pushes consideration of this possibility to the next level. It is part of our plan to address youth crime from every angle: better technology, more resources, tougher laws.

Question put—That the motion be agreed to.

Motion agreed to.

7.1.2 Question on Notice (22 March 2021)

Is there a legislative fix for police to be able to access GPS data of stolen vehicles for the purpose of recovery?

To access personal information such as the GPS data, police currently rely on existing authorities by either obtaining a warrant or being facilitated access to the information on a consensual basis.

Improving the timeliness of access to private information for law enforcement purposes may require strengthened arrangements to relax the current requirements for obtaining a warrant or informed consent (noting obtaining either urgently may be impractical in some circumstances). Establishing such a streamlined process with service providers, some of which may operate from other Australian or international jurisdictions, might not be a straightforward matter in Queensland law.

Legislation to authorise police access to private information without a warrant or consent would potentially engage individual rights to privacy which are protected by the Human Rights Act 2019. Altering legislation to support operational objectives around vehicle usage in certain urgent circumstances, such as ability to produce an order to a car manufacturer/dealer requiring them to provide information to police to track or depower a motor vehicle associated with a criminal purpose, would require careful consideration and consultation.

Feasibility of policy and legislative options for building in an authority into the service agreement between the customer and the service provider for the release information to the police in certain circumstances will need to be fully explored.

8. Appendix III

8.1.1 ANZPAA Remote Engine Immobilisation Reference Report Summary

This section explores the 2019 Reference Report from Australia New Zealand Policing Advisory Agency (ANZPAA).[30]

The report was commissioned in the wake of serious injury to Queensland Police Service Constable Peter McAulay who was hit by a stolen vehicle involved in a police pursuit. The premise underlying this work is that if remote engine immobiliser (REI) technology were available, the safety of the public, police officers and offenders would be enhanced. Safety, not vehicle crime is therefore the primary focus of this report.

REI technologies already exist and are in use throughout the world. However, these systems are:

- anti-theft focused and are predominantly used to prevent a vehicle from being re-started as opposed to stopping a moving vehicle.
- decentralised with system management the responsibility of car manufacturers or third-party fleet managers.
- an opt-in service which relies on vehicle owners' consent.
- in operation on a much smaller scale than envisaged for Australian policing.

There are also issues unique to the Australian context that need to be considered when analysing the feasibility of a nationwide REI system:

- Australian Design Rules (ADRs) which govern the establishment of standards under the Motor Vehicle Standards Act 1989, require evidence of a clearly defined and tested safety benefit before a standard can be implemented. This is not available for REI's because no single in-vehicle REI technology with an enabling environment currently exists anywhere in the world.
- Almost all vehicle manufacturing is currently undertaken overseas. With Australia representing 1.2% of the international vehicle market, it will be challenging to influence manufacturers to include REI technology in all vehicles across the market.
- Making allowances for current vehicle age proportions in Australia, it would take approximately 16 years from the time REI technology becomes a standard inclusion for it to become available in approximately 80% of Australia's vehicle fleet. An after-market solution is not deemed feasible for a range of reasons including technological and effectiveness.

In a perfect scenario, enabling the remote immobilisation of a vehicle would undoubtedly lead to better safety outcomes for the public, police officers and offenders. However, whether such a system is currently feasible is the more difficult question. This report examines that question with consideration given to:

Technical considerations	In vehicle technology Enabling environment
Implementation considerations	Installation Mandatory frameworks Voluntary frameworks
Stakeholder considerations	Technology Costs borne by industry Privacy and consumer rights
Future considerations	Automated vehicles Connected vehicles

Examination of the above has led to the following overall findings:

- While the technology already exists to immobilise certain vehicles, it is not yet feasible for such technology to be utilised across the entire Australian vehicle fleet.
- There has been no successful implementation of a mandated REI solution across a whole vehicle fleet anywhere in the world.
- At this time, there is no single in-vehicle technology available, nor is there the required enabling environment to support the use of REI technology. However, with continued technological development REI may be feasible in the future.
- While the technology is developing rapidly, it is likely to be superseded by connected and automated vehicles.

- Until connected vehicles have saturated the fleet, line of sight to identify the applicable vehicle would be required which may not mitigate the risk that currently exists with police pursuits.
- Until the process associated with timelines and deployment of an REI is addressed, such as vehicle verification, authorisation and connectivity, the safety impact of the technology may not be able to be realised.
- There are scenarios where there may be unintended safety consequences from deploying an REI on a moving vehicle.
- The costs of administering one interconnected REI system would be substantial, notwithstanding the costs will be borne largely by industry and passed onto consumers associated with research, development and production.
- GPS technology will also be integral to vehicle identification. This will raise issues of privacy and who owns the data that is collected.
- Fleet saturation of connected / autonomous vehicles is more likely (even probable) before fleet saturation of REIs (assuming it is possible for an ADR to standardise REI).

8.1.2 Technological Considerations

Engine immobilisers in the form of transponder-based immobilisers for anti-theft purposes have existed in Australia for some time. The term 'remote engine immobiliser' is used to describe a wide range of technologies with diverse purposes and operating systems. For the purpose of this report 'remote engine immobilisers' have been organised into the following categories:

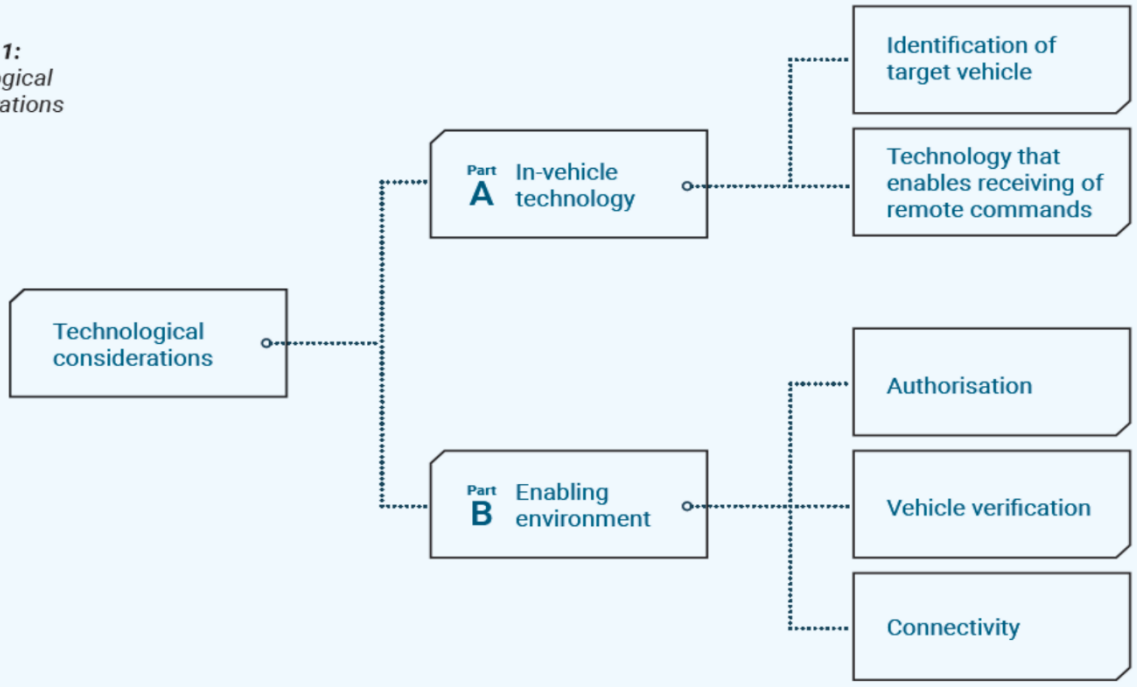
Category I Technologies and supporting systems that are installed in vehicles that can safely terminate the operation of moving or static vehicles.

Category II Technologies and supporting systems that are installed in vehicles designed to disable the operation of a vehicle after it has been stopped and turned off. These technologies are used primarily to prevent theft of vehicles.

Category III Related technologies that are not installed in vehicles but can provide a function that may support immobilisation of a vehicle.

Category I REIs are the focus of this report as these technologies and related technologies support the objective of enabling an authorised police officer to remotely, electronically and safely restrict the operation of a vehicle. The technological considerations in relation to Category I are visually presented below:

Diagram 1: *Technological Considerations*



This section of the report will examine the technological requirements and challenges associated with a Category I REI technology for use in two parts:

PART A: In-vehicle technology. This section examines the requirements of technologies installed within vehicles (referred to hereafter as the 'on-board system') to enable the remote termination of both moving and static vehicles.

PART B: Enabling environment. This section explores the infrastructure and systems architecture required to support connectivity between vehicles and operational coordination 'call' centres that send remote commands to enable the remote termination of both moving and static vehicles.

8.1.3 Part A: In-vehicle technology

Developing and installing an on-board system that would allow remote termination of an operating vehicle is challenging as these systems would be required to:

- allow for the identification of a vehicle targeted for remote immobilisation
- receive remote commands to immobilise the operation of the target vehicle.

At the time of drafting of this report, there is no on-board system that could satisfy the requirements listed in Diagram 1: Part A. This report examines each of the listed requirements, drawing on examples of related technologies that can approximate each functional requirement.

Identification of Target Vehicle

Identification of the target vehicle is fundamental to the effectiveness and utility of an REI. A remote command to immobilise a vehicle (allowing for the safe slowing down, stopping and/or immobilisation of a vehicle) must be sent to and received by the exact target vehicle. Where this technology is currently successfully utilised abroad is when the owner initiates identification process. Any identification technology will need to align to number plate technology reform because if a vehicle has false plates policing will have conflicting identifiers of the target vehicle.

The on-board system will require unique identification features and secure processes. This would ensure that any remote command would be sent to the right on-board system. Related technologies, such as Global Positioning Systems (GPS) tracking, may support such identification.

Technology that Enables Receiving of Remote Commands

On-board systems will require the capability to receive a remote command to activate slow down, stop and/or immobilise. Remote activation will require a communications network that not only enables transmission for commands to be sent to the on-board system, but also allows for the on-board system to send override commands to a number of other in-vehicle control systems.

Such vehicle systems will need to be able to:

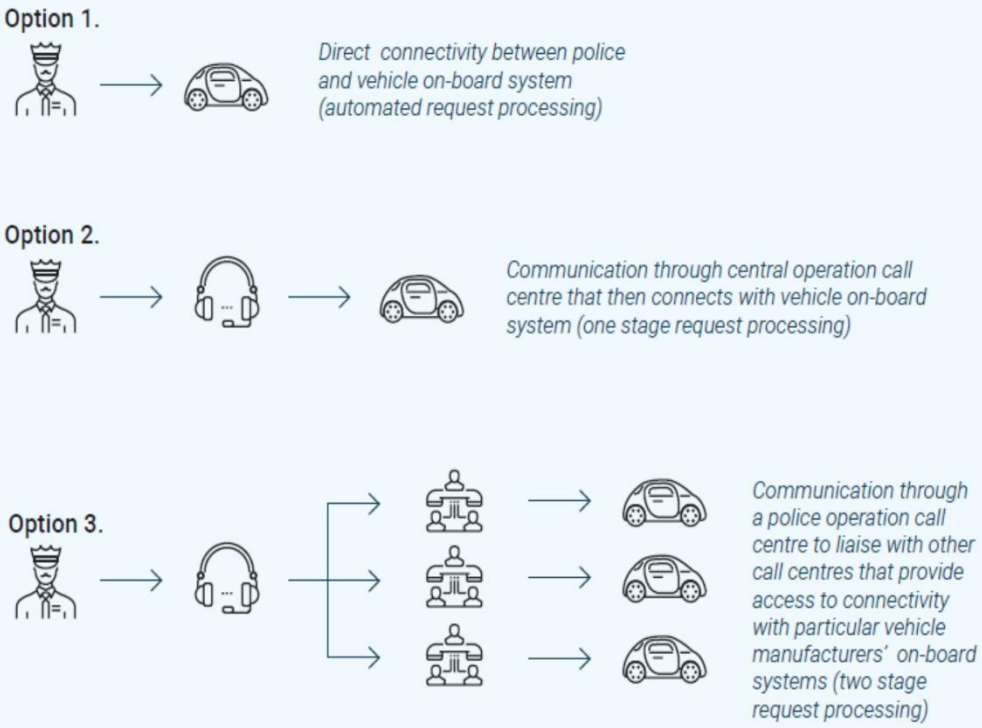
- slow down a moving vehicle to a stop, requiring control over brakes, throttle controls and transmission systems.
- immobilise vehicles by preventing them from being restarted, such as those that control the fuel pump, the ignition and/or starter motor.

8.1.4 Part B: Enabling environment

If REIs are to be implemented, an appropriate enabling environment will need to be established. This enabling environment will need to provide the systems architecture to facilitate the end-to-end process of remote termination of the target vehicle. Implementing the enabling environment will require clearly defined responsibilities as to who will establish, manage and be accountable for different parts of the systems and termination process.

Depending on consistency and design/standard for on-board systems, and responsibility for management of an REI enabling environment, termination commands may be processed in different ways (Diagram 2).

Diagram 2: *Options of different enabling environments*



This could include police officers either having the capability to directly connect to the target vehicle's on-board system, or alternately channelling requests through one or more operation coordination centres.

An ideal enabling environment would allow operational police to connect directly with a target vehicle (Option 1, Diagram 2). However, this is not feasible at this time as there is no on-board system that can operate with different OBD-II port 'language'.

Due to the number of car manufacturers within the Australian market, it would be difficult for the police officer(s) on the ground to deal directly with a General Motors or Toyota for example, whilst also maintaining line of sight of the target vehicle. Therefore, it is envisioned that operational police would need to interface with manufacturers either through a centralised coordination centre (Option 2) or through a police coordination centre that contacts individual manufacturers (Option 3).

Note on OBD-II port: Operation varies between manufacturers. These ports do not have interoperability because they are primarily a diagnostic interface that operates with numerous signal protocols. A retrofitted solution utilising OBD-II port would need to be designed against a particular car which is very manufacturer specific. If the solution is OBD-II port based it will be unlikely to reach complete fleet saturation.

Regardless of which enabling environment option is utilised, the process would still require:

- Authorisation: police officers request authorisation for the operation of the target vehicle to be remotely terminated through slowing down, stopping and/or immobilisation.
- Vehicle verification: verifying the target vehicle would require pairing the unique identifier of the on-board system with other vehicle identifiers.
- Connectivity: linking remote commands sent through a communication network with a target vehicle's onboard system for actioning.

Authorisation

Authorisation for the REI to be deployed would be provided by the operational police maintaining line of sight of the target vehicle. Line of sight would be critical to ensure the target vehicle was slowed and stopped safely. The national coordination centre would receive the termination request and action accordingly. This type of request processing is used in existing services such as StarChase™ and General Motor's OnStar™.

Vehicle Verification

The identity of the target vehicle will need to be verified through a combination of pairing unique identifiers of the on-board system and physical vehicle identifiers such as number plate, make, model, colour and location. This will require both GPS monitoring and line of sight to be maintained throughout the verification process to ensure the termination of the correct target vehicle.

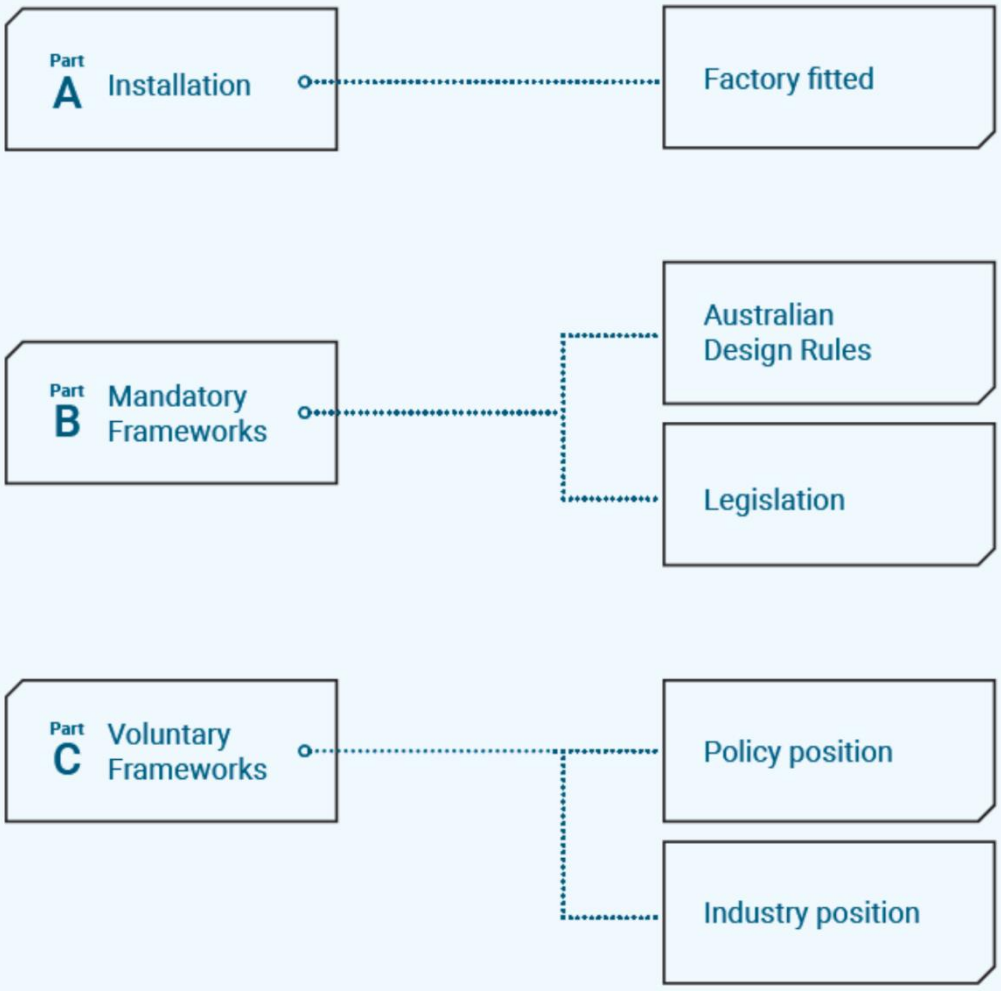
Connectivity

Telecommunications infrastructure is essential when receiving remote requests for termination and remotely actioning termination commands. The effectiveness of the entire enabling environment will rest on the capability and capacity of the network to provide reliable connectivity. Current communications infrastructure uses either short-range (peer-to-peer or one device connecting directly with another device) or long-range (peer-to-network or one device connecting through network infrastructure to other devices) capability. It is anticipated, partially through the rollout of 5G communication technology, that the use of 'mesh' networks could be more readily available allowing for the use of both long-range and short-range capability.

8.1.5 Implementation Considerations

If a technological solution is available, the implementation of the technology and its enabling environment will be required. Implementation considerations are addressed as follows:

Diagram 3:
Implementation Considerations



Note: The full ANZPAA report goes into further detail for each of the above parts, which won't be detailed in this report. The depth of the report overview in the Appendices is deemed sufficient to allow for commentary. In any case, further details can be found via the link to the full version in the References section. [30]

8.1.6 Future Considerations

Technological innovation continues to evolve enabling ever greater connectivity between people and devices through the Internet. Some emerging technologies of note include the Internet of Things (IoT) and automation, often make it easier to innovate, creating substantial disruption to existing industries.

There are two areas of technological development in the automotive industry that, over time, may impact the need for REI technology:

- Connected vehicles
- Automated vehicles

Connected Vehicles

The introduction of internet connected sensors into transport infrastructure, also known as Cooperative Intelligent Transport Systems (C-ITS), enables vehicles to wirelessly communicate with other vehicles, infrastructure and other parts of the road network. Examples include collision avoidance systems through Vehicle-to-Vehicle connectivity or Vehicle-to-Infrastructure connectivity.

There are opportunities for policing to leverage from C-ITS to allow them to identify particular vehicles that may have had number plates switched. Opportunities to deploy C-ITS are also likely to expand following the introduction of a reliable and geographically widespread 5G telecommunications network.

A combination of 5G and other dedicated short-range communication technologies may be sufficient to enable more widespread vehicle-to-vehicle and vehicle-to-infrastructure communication.

It is possible that in the future, C-ITS could be leveraged to assist in or execute vehicle immobilisation, however given the early development phase of this technology, it is difficult to ascertain at present the process by which this might occur.

Automated Vehicles

Vehicles requiring decreasing degrees of human operation are expected to be available in commercial markets over the coming years. Estimates of their future market availability vary depending on the degree of automation. The NTC estimates that automated vehicles (AV) that do not require a human driver for some or part of the journey will become available after 2020. Volvo expect that fully driverless vehicles are achievable in Australia but are likely to be 'some decades away'.

A notable recent event demonstrated that police are able to exploit safety control systems of semi-automated vehicles to slow and stop a target vehicle. A Tesla Model 3, travelling at speeds exceeding 110kmph, was safely stopped while the driver slept. However, this example does not account for potentially deliberately erratic or unexpected manoeuvring by an offender once becoming aware of police in pursuit.

Many concerns raised in this report regarding REI technology (such as surveillance and privacy) also apply to AVs. There have already been indications that consumers may have data concerns, particularly in terms of the privacy of personal information and the vulnerability of data to cybersecurity threats. AVs' reliance on complex internetconnected software and advanced communication networks may also render them vulnerable to cyberattacks, this would be similar to REI technology.

Public perception of data privacy and cybersecurity vulnerabilities are seen as barriers for adoption of AVs. There would be similar concerns regarding REI technology.

8.1.7 Findings

After careful consideration, the report presents the following overall findings:

- While the technology already exists to immobilise certain vehicles, it is not yet feasible for such technology to be utilised across the entire Australian vehicle fleet.
- There has been no successful implementation of a mandated REI solution across a whole vehicle fleet anywhere in the world.
- At this time, there is no single in-vehicle technology available, nor is there the required enabling environment to support the use of REI technology. However, with continued technological development REI may be feasible in the future.
- While the technology is developing rapidly, it is likely to be superseded by connected and automated vehicles.
- Until connected vehicles have saturated the fleet, line of sight to identify the applicable vehicle would be required which may not mitigate the risk that currently exists with police pursuits.
- Until the process associated with timelines and deployment of an REI is addressed, such as vehicle verification, authorisation and connectivity, the safety impact of the technology may not be able to be realised.
- There are scenarios where there may be unintended safety consequences from deploying an REI on a moving vehicle.
- The costs of administering one interconnected REI system would be substantial, notwithstanding the costs borne largely by industry and passed onto consumers associated with research, development and production.
- GPS technology will also be integral to vehicle identification. This will raise issues of privacy and who owns the data that is collected.
- Fleet saturation of connected / autonomous vehicles is more likely (even probable) before fleet saturation of REIs (assuming it is possible for an ADR to standardise REI)

8.1.8 Related technologies

The following section highlights some related anti-theft technologies.

Radio Frequency (RF) Pulse Immobiliser

This technology disables all electronic systems using high frequency RF pulses to disrupt electronic components, slowing down and/or stopping vehicles. For example, RF Safe-Stop is a 350kg emitter that can be integrated into SUV sized vehicles that can disable small vehicle electronics from up to 50 meters away.

Pursuit Management System (STARCHASE™)

A pursuit management system which involves the shooting of a tracking device from a pursuing police vehicle. The device attaches to the target vehicle allowing police to track its location. Once the vehicle has slowed down or stopped police can safely intercept it. StarChase™ data demonstrates that once the pursuing vehicle has been tagged and the pursuit ceased, the driver will generally slow down within two minutes, driving to a normal speed. Police will then rely on the GPS mapping to monitor the vehicle and apprehend once it is safe to do so. This has led to an 80% apprehension rate.

Geofencing

This technology refers to the implementation of a geographically demarcated virtual zone where the entry, speed and fuel supply of vehicles can be controlled digitally. It limits vehicle operation in geographical zones and would not apply to vehicles travelling outside that zone. The technology has been trialled in Stockholm Sweden, funded by Swedish Government departments and manufacturers including Veoneer, Scania, Volvo Cars and the Volvo Group.

References

1. https://www.bmw.com/en-au/offers-and-services/bmw-apps/my-bmw-app-overview.html My BMW overview
2. https://www.caradvice.com.au/507079/bmw-connected-australian-rollout-confirmed-timing-to-be-announced/ BMW connect My BMW rollout confirmed
3. FordPass Connect Arrives in Australia With Ford Ranger Everest And Transit Leading Connectivity Push FordPass App Now In App Stores FordPass app overview
4. HondaLink: Connectivity for Smart Phones and Honda Vehicles HondaLink app overview
5. Hyundai Auto Link App | Owner Benefits | You Drive. We Donate | Hyundai Australia Hyundai Autolink overview
6. https://www.hyundai.co.nz/autolink-premium-frequently-asked-questions Hyundai Autolink FAQs
7. UVO CONNECT by Kia. Tap into the future. Kia UVO app overview
8. 2021 Kia Stonic facelift unveiled, on sale in Australia late 2020 | CarAdvice Kia Stonic
9. https://www.mazdamobilestart.com/index.jsp Mazda mobile-start
10. Mercedes me connect: Mercedes-Benz Mercedes-Benz Sydney Alexandria (mbsydney.com.au) Mercedes me
11. Safety & Security | Connected Services | Toyota AU Toyota security features overview
12. https://www.toyota.com.au/connected/services/stolen-vehicle-tracking Toyota stolen vehicle tracking
13. Volkswagen adds Siri integration to Car-Net app | CarAdvice Siri integration into VW car-net
14. car-net (vw.com) VW car-net overview
15. The interoperable EU-wide eCall | Mobility and Transport (europa.eu) EU-wide eCall overview
16. https://www.wired.com/story/mycar-remote-start-vulnerabilities/ Remote-start app exposes cars to hackers
17. https://www.securityweek.com/researchers-hijack-tesla-car-hacking-mobile-app Tesla app hacked
18. https://www.parliament.qld.gov.au/work-of-committees/committees/TRC/inquiries/current-inquiries/VehSafetyStdTech Link to Queensland Parliament Inquiry
19. https://www.kia.com/content/dam/kia2/in/en/uvo/QRG.pdf Kia UVO
20. https://www.customgeophev.com/faq/ Ford custom Geo-fence
21. https://www.audi.com.au/au/web/en/owners/audi-track.html Audi track GPS device
22. https://www.reddit.com/r/rav4club/comments/ejxiog/toyota_data_tracking_how_to_turn_off/ Toyota forum disable tracking
23. https://www.justanswer.com/bmw/cikku-disable-gps-bmw-connect-2018-x5.html BMW forum disabling GPS
24. https://www.justanswer.com/bmw/2hmrx-someone-tracked-car-gps-and-or-bmw-assist.html BMW forum
25. https://www.justanswer.com/bmw/d2gy5-know-disconnect-tracker-off.html BMW forum disabling GPS
26. https://www.youtube.com/watch?v=Bbp7S-0m0h8 BMW tracker and fuse box location
27. https://www.youtube.com/watch?v=CKd4E0Lege0 Tesla disable mobile tracking.
28. qon-29Mar21_QPS.pdf (parliament.qld.gov.au) Questions on Notice
29. TRCVehicleSafetyStandTechInq.pdf (parliament.qld.gov.au) Brochure about the Inquiry
30. REMOTE ENGINE IMMOBILISER (parliament.qld.gov.au) ANZPAA Reference Report 2019
31. https://g05.bimmerpost.com/forums/showthread.php?t=1645493&page=7 BMW Shark Fin image (Fig 1)
32. https://www.quora.com/What-is-the-tail-like-object-at-the-top-of-modern-BMWs BMW shark fin image (Fig 2)
33. https://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/?sh=315daffc2ef8 Car conversations being recorded by Police
34. https://www.documentcloud.org/documents/3295671-Complaint-About-Legality-of-OnStar-GM-Order.html Louisiana Court hearing regarding OnStar
35. https://www.rav4world.com/threads/2019-rav4-dcm-deactivate-procedure.304339/ Toyota RAV4 disable tracking
36. https://www.youtube.com/watch?v=cYsIb4CWCcA YouTube video of Toyota fuses
37. https://i.ytimg.com/vi/CKd4E0Lege0/maxresdefault.jpg Image of Tesla privacy mode
38. https://i.ytimg.com/vi/QyfkRIaKrts/maxresdefault.jpg Image of Tesla mobile access disabled
39. https://www.youtube.com/watch?v=CKd4E0Lege0 YouTube video of disabling mobile access in a Tesla
40. https://www.youtube.com/watch?v=i5xfqqxMOFE YouTube video of live vehicle tracking for a Tesla
41. https://teslaownersonline.com/threads/any-one-how-can-you-disable-location-in-navigation.17982/ Tesla forum on how to disable location
42. http://www.fixyourtesla.com/3/ANTENNA-GPS-REMOVE-AND-REPLACE.html Tesla technical procedure to remove GPS antenna

43. https://www.tacomaworld.com/threads/how-can-i-permanently-disable-toyota-gps-tracking.708749/ Image of how to disable vehicle tracking via navigation antenna
44. https://www.rav4world.com/cdn-cgi/image/format=auto,onerror=redirect,width=1920,height=1920,fit=scale-down/https://www.rav4world.com/attachments/1583166906461-jpeg.150259/ Image of Toyota fuse cover
45. https://fuseandrelay.com/wp-content/uploads/2021/06/location-3.jpg Image of Toyota fuse box location
46. https://www.tesla.com/en_AU/support/tesla-app Tesla app information