University of New South Wales Law Research Series

THE PRIVACY AND DATA PROTECTION REGULATORY FRAMEWORK FOR C-ITS AND AV SYSTEMS REPORT FOR THE NATIONAL TRANSPORT COMMISSION

DAVID VAILE, MONIKA ZALNIERIUTE AND LYRIA BENNETT MOSES

(2018) Report for the National Transport Commission, 2nd July
[2019] *UNSWLRS* 11

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

The privacy and data protection regulatory framework for C-ITS and AV systems
Report for the National Transport Commission

David Vaile, Monika Zalnieriute and Lyria Bennett Moses

2 July 2018

Contents

Contacts
Lyria Bennett Moses lyria@unsw.edu.au
David Vaile d.vaile@unsw.edu.au
Monika Zalnieriute m.zalnieriute@unsw.edu.au
c/- UNSW Faculty of Law, Sydney

1 HIGHLIGHTS AND KEY OBSERVATIONS

This Report was prepared to assist the NTC address the privacy and related regulatory and legal frameworks for information involved in C-ITS and AV systems, and develop a policy analysis of issues that may need attention. It surveys the information involved in various aspects of these systems, how the law characterises that information, and a range of regulatory approaches on particular issues. There are examples in Appendices from the text of key laws, and the body of the report summarises their effect.

Some of the observations below are extracted from conclusions and observations in the report. They note where an issue is straightforward or consistent, and also draw out some observations about gaps, inconsistencies or ambiguities, particularly in the coverage or treatment of current and anticipated C-ITS & AV system data under existing law.

Section 2 sets out the types of data and information of most interest in the C-ITS and AV context. It lists six types of data by source and discusses the information that can be derived from the data. It also introduces some of the legislation, explaining some of the patterns of coverage in privacy laws.

Section 3 goes through the key issues about the scope of terms personal information and sensitive information about a person. It discusses identification, and in 3.7 suggests the degree to which the data and information discussed in 2.2 is likely to be personal information. There is also detailed consideration of issues raised by the 'sensitive information' category.

The information involved in C-ITS and AV systems will often, but not necessarily in all circumstances, constitute 'personal information' and thus come under privacy and data protection law in Commonwealth and state and territory jurisdictions.

Whether information counts as 'personal' is contextual. The range of data and contexts in the C-ITS and AV environment is large and complex. It will rarely be feasible to attribute categories of C-ITS and AV data as PI or not PI. Processing may enable identification of personal information and sensitive information. Data collected in the cabin is particularly likely to become sensitive by context.

Most data types associated with C-ITS and AV systems should be treated as if they could be PI, unless there is good reason to the contrary. Categorising many data types as not PI could lead to complaints, distrust, and legal risk.

Section 4 surveys a number of other key laws with respect to collection powers, including road transport, telecommunications data retention, safety assurance system, law enforcement and security justifications for collection, and others.

Passenger vehicles and some light commercial vehicles are treated differently to heavy transport vehicles, with the latter subject to more stringent and comprehensive information regimes. Road traffic laws, including speeding, CCTV and ANPR already authorise certain targeted collection of data. But these schemes are quite different from C-ITS and AV systems.

Law enforcement powers to access data under using specific tools such as search warrants and authorisations are broad but pre-date the current ability to collect and analyse large data sets. With C-ITS and AV technology, there are risks that the law enforcement exception to privacy law may permit mass surveillance without a warrant.

Section 5 maps the privacy protection model on C-ITS and AV data activities, including collection, use, disclosure, storage, and deletion. It concludes by examining some of the rights of data subjects under privacy law.

A lot of the collection or use of C-ITS & AV data will be done by state and territory instrumentalities, but some of them do not have privacy statutes, including SA and WA. This creates potential inconsistency, complexity and uncertainty.

Many of the laws considered do not give extensive rights of access to one's own personal information. C-ITS and AV systems will have larger volumes of often compulsorily collected data, with greater scope for use and misuse.

Section 6 digs into the complex patchwork of surveillance device laws, considering the degree to which the prohibitions on use of one of more of the four device types are implemented in various jurisdictions, and also maps these laws onto C-ITS and AV data. A key issue is the degree to which conducting activities and using devices that may fall within the device types will contravene those prohibitions, given the strict criminal law enforcement focus of these laws, and their protection of the output of such devices with further prohibitions.

As noted by ALRC, the present device categories (listening, optical, data and tracking) are not technology neutral, and may exclude surveillance implemented by software inserted onto a general purpose device, WiFi, RFID, or data analysis and extraction.

Section 7 looks into the application of the telecommunications laws to the C-ITS infrastructure, and the question of whether any entities involved may be a regulated entity under those laws.

The status of location information is unclear. In most cases it will not be telecommunications metadata, but this may need further examination. Distinctions between 'contents' of a communication and the metadata may become less distinct.

Section 8 surveys the European data protection framework, including new GDPR and law enforcement regulations. The European definition of personal information is useful.

Section 9 explores the US legal framework, and sets out three methods for assessing whether information should be considered 'personal'. It also identifies government powers to compel access, and protections against government access to personal information. The impact of big data corporations is noted in passing.

Section 10 concludes with a series of observations about gaps and ambiguities in the current environment for C-ITS and AV data. Some of the points are noted here.

Appendices contain comprehensive information supporting the text:

Appendix A summarises the effect of and issues raised by several key court cases on the definition of personal information and the obligations of collectors to have proper basis for collection, as discussed in section 2.

Appendix B compares definitions of personal information in Table 1 and sensitive information in Table 2 in laws across the country, as discussed in section 3.

Appendix C compares privacy principles across jurisdictions in Table 1, and illustrates an anomalous set of similar principles embedded in the HVNL in Table 2, as discussed in sections 3 and 5.

Appendix D compares the key bases for exemptions from privacy laws for law enforcement purposes, as discussed in section 4.5.

Appendix E lists the four device types in Surveillance device laws in Table 1, and compares the definitions used in those laws in Table 2, as discussed in section 6.

Appendix F lists telecommunications laws in each jurisdiction, as discussed in section 7.

Appendix G includes extra material comparing aspects of the European and US frameworks, as discussed in sections 8 and 9.

Glossary explains a few legal terms

Sources include a list of many relevant pieces of legislation in Australia, as a reference, and short collections of materials from the EU and US.

2 INTRODUCTION

2.1 About this report

2.1.1 The purpose of this report

The purpose of this document is to analyse and briefly explain the impact of existing laws and regulation in relation to privacy[1] on the information[2] associated with the technology of cooperative intelligent transport systems (C-ITS) and automated vehicle (AV) systems in Australia.[3]

2.1.2 Who this report is for

The audience for this report includes those interested in understanding how existing regulatory concepts and rules in relation to privacy may apply to the information and data associated with C-ITS and AV systems in Australia. This will likely include engineers, policy-makers and policy analysts, vehicle and automated system developers, regulators, lawyers, and cyber security and data protection risk analysts.

2.1.3 The purpose of the NTC reform

The NTC is assessing whether Australia's information privacy framework[4] covering government collection and use[5] of information provides sufficient protection for privacy given the significant developments in transport technology. The NTC is focusing on the new information that may be generated by C-ITS and AV technology.

The NTC considers that privacy concerns around government collection and use may be a barrier to consumer take-up of C-ITS and AV technology in Australia. These concerns may delay or impede the deployment of technology that has the potential to significantly improve road safety.

The NTC's aim is to ensure any privacy risks of government collection and use of information generated by C-ITS and AV technology are appropriately addressed. Therefore, if Australia's information privacy framework is insufficient, the NTC may propose options for reform to the Transport and Infrastructure Council.

2.1.4 Context of this report

This report will support the development of a discussion paper the NTC is preparing for stakeholder consultation. The NTC's discussion paper will:

---

[1] The terms 'privacy' and 'data protection' are sometimes used interchangeably in regulatory discussions. In this report the term 'privacy' will generally be used to cover both concepts, unless this would unintentionally gloss over substantial distinctions. (To the extent there is a difference, privacy in some contexts covers a somewhat broader range of issues than data protection.)

[2] The term information is generally used in this Report as inclusive of related, but potentially narrower, terminology such as data, documents, records, and communications. It is also the term used in much of the legislation. The term data may be used to refer to more concrete low level outputs of sensors and the like.

[3] C-ITS means a technology platform that enables components of the transport network (vehicles, roads and infrastructure) to wirelessly communicate and share real-time information, including information on vehicle movements, traffic signs and road conditions. Automated vehicles are vehicles that include an automated driving system capable of performing the entire dynamic driving task (steering, acceleration, braking and monitoring the driving environment) on a sustained basis. The data sets for these vehicles are discussed in later sections.

[4] 'Australia's information privacy framework' refers to existing protections for privacy and related matters, and powers to collect information.

[5] 'Use' is intended to broadly cover use, disclosure, storage and destruction.

- outline potential new privacy risks associated with government collection and use of information generated by C-ITS and AV technology – in particular, it will focus on changes compared to standard vehicles in current use

- outline how Australia's information privacy framework could apply to government collection and use of information generated by C-ITS and AV technology

- seek feedback on whether Australia's information privacy framework relating to government collection and use is sufficient in light of any new privacy risks associated with information likely to be generated by C-ITS and AV technology

- seek feedback on proposed options for reform if Australia's current information privacy framework is considered to be insufficient as it relates to government collection and use of information likely to be generated by C-ITS and AV technology.

2.1.5 Entities of interest

The entities of primary interest in this report are Australian federal and state government bodies. This includes departments and agencies involved in roads and traffic operations, vehicle regulation, law enforcement and policing, and other domains.

Private entities are largely relevant only as potential suppliers of information to these government bodies. Such suppliers could include the manufacturers of C-ITS and AV systems providers of software and data for such systems, hosts of cloud data used by owners or occupants of vehicles, telecommunications carriers or telecommunications service providers ('telecommunications providers'), or infrastructure service providers..

This report does *not* attempt to address the operation of privacy regulation for private entities in their own right. In particular, it does not discuss obligations arising out of relationships private entities have with the users, owners or passengers of C-ITS and AV systems.

2.1.6 The timeframe of interest

This report is based on a comparison of current vehicle technology and anticipated future C-ITS and AV technology.

The NTC's goal is to have end-to-end regulation in place by 2020 to support the safe commercial deployment of automated vehicles at all levels of automation. This report uses 2020 as the start of the 'future' timeframe.

The further into the future the timeframe extends, the more uncertainty there is in projections about future developments in C-ITS and AV technology, information practices that may be required or possible, potential for problematic information use or disclosure, threats to information security or de-identification protections, and the personal-information-related issues that may arise. Of most interest is the next 5–10 years, which is expected to be the most intense period of development of this technology and its information practices.

2.1.7 Key features of advanced driver assistance system (ADAS), C-ITS and AV data

The categories of data from current and future vehicle technology considered in this document are based on information provided by the NTC. See 2.2 below for details.

2.1.8 Key features of the sources of law on 'personal information' in Australia

The main sources of law on 'personal information' in Australia are in privacy statutes found at both state and federal level.[6] Such statutes include definitions of 'personal information' and set out the scope of entities and information covered.

Where an item of information and the entity dealing with it are covered by such a law, the detailed rules and obligations for key activities such as collection, use, disclosure, storage and destruction will be set out in Privacy Principles for that Act. This drafting technique is borrowed from the OECD's principles-based guidelines of the 1980s.

2.1.9 The approach

We analyse attributes of the various categories of data captured to help understand in what circumstances each may comprise 'personal information' and explore implications.

The report is organised by issues, rather than by jurisdiction. Jurisdictional variations are noted where relevant to each issue.

We describe regulatory features and their interaction with particular types of information and identify the common or typical features among jurisdictions (Commonwealth and States/Territories), noting key exceptions.

Much of the detail is presented in appendices, with key points in the text.

2.2 Types of data covered in report

In this section, we outline types of low-level data that may be captured by C-ITS and AV technology. These will be the primary objects of analysis throughout the report. For each type of data, we also discuss the further information that may be derived from it after processing or data matching.

2.2.1 Image Data

2.2.1.1 Image data external to the vehicle

This data comes from dashboard cameras (dash cams) and other camera vision (external camera input units), generating still and moving images.

Derived information: Image data can reveal information about number plates of nearby vehicles, the number of individuals on the street, and the location of people and objects. Assuming image recognition and face recognition functionality applied to the video or still images,[7] this may also reveal information about the identity of pedestrians and perhaps what they are doing. It is unlikely that information about emotional, cognitive or physiological attributes will be able to be deduced from external image data.

2.2.1.2 Image data internal to the vehicle

In-cabin camera vision creates still and moving image data, mostly of the occupants of the vehicle.

[6] At the Commonwealth level, the *Privacy Act 1988* (Cth). Examples at the state level include the *Information Privacy Act 2014* (ACT), *Privacy and Personal Information Protection Act 1998* (NSW) and *Health Records and Information Privacy Act 2002* (NSW). See also Legislation heading in the Sources section at the end of this Report.

[7] This functionality is not present in dash cams or common in external cameras at present, but it is proliferating rapidly and may appear in future generations of these devices or their associated services.

Derived information: Assuming image recognition and face recognition functionality is applied to the video, information about the identity of vehicle occupants, the number of occupants, and what they are doing may be revealed. Compared to external image data, it is more likely that internal image data could reveal emotional, cognitive or physiological attributes of the occupants, especially the driver.

2.2.2 Crash data – Event Data Records (EDR)

This covers crash-related EDR data, including airbag and restraint deployment. There may be other types of data including driving mode, accelerometer and vehicle orientation.

Derived information: The data may reveal information about vehicle control, as well as about the events shortly before, during and after a crash.

Data would be continually collected and retained temporarily in a buffer to enable going back for a short period for the triggering event, but would only need to be stored longer in the event of a crash. Some systems may voluntarily retain this for longer than the minimum required to support a short wind-back.

2.2.3 Location and route data

2.2.3.1 Location and route data from Navigation Systems

Location and route data may include Global Navigation Satellite Systems (GNSS), comprising Global Positioning System (GPS) and possibly GLONASS or other satellite signal information; mobile network infrastructure location data from 3G, 4G and 5G 'phone towers'; and possibly[8] Wi-Fi access point data and compatible Bluetooth data, depending on the operating system and devices involved. The data could include geographic location at a given time, and vehicle route data.

Derived information: This data may reveal information about past actual routes and planned future routes of journeys in this vehicle, their origins and destinations, regular patterns of movement, and proximity to communications infrastructure elements like mobile phone towers at particular times**.**

It is not clear whether some of the data, such as Bluetooth data, can readily be linked back to a particular individual or car.

2.2.3.2 Location and route data from V2V and V2I communication

Vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication data may include data for the vehicle in question and for other vehicles. In particular, it provides information about vehicle location and vehicle movements as well as traffic signs and road conditions if the 5.9 GHz Dedicated Short-Range Communications (DSRC) wireless links and related C-ITS road and other infrastructure supports it.[9] A unique ID number may be broadcast by the vehicle and other devices, and received by roadside

[8] Both major mobile device operating system vendors, Google and Apple, are making significant efforts to develop C-ITS and AV technology. Both companies already maintain a global database of Wi-Fi access point data to increase precision of mobile device location analysis compared to GPS and mobile network data alone, especially in congested urban areas where those signals may be compromised. It is unclear what role such Wi-Fi systems would play in their C-ITS or AV systems. This is separate from the work on Dedicated Short-Range Communications between vehicles (DSRC for V2V), which uses a Wi-Fi-related band but is based around IEEE 802.11p rather than existing consumer WiFi. See below; and see also the US section for related issues.

[9] We do not consider other 'V2X' communications like V2P (Vehicle-to-Pedestrian) where the mechanism and content of the information to be captured is not yet clear.

equipment. Data may also include proximity to network or road infrastructure elements and any warnings, alerts or notices generated by infrastructure or vehicles.

Derived information: V2V or V2I data may reveal information on the location, direction, speed and movements of this and other vehicles. The identifier is not directly linked to information about the vehicle owner or passenger, although linking may be feasible indirectly in some instances.

2.2.4 Data covering biometric, biological or health factors

Vehicles may include special purpose biometric, biological or health sensors for use in assessing wakefulness, attentiveness, intoxication, mental stress, physical distress or impaired reactions for a driver or other vehicle occupant. Data from such sensors can provide information about facial temperature, heart rate, breathing rate and blood glucose levels.

Derived information: In addition to these specific sensors, generic and specialist cameras and microphones may also be able to capture image or audio data that can be subjected to biometric or physiological analysis. Such analysis is not necessarily limited to identification, but can include pulse, body temperature or other circulatory information as well as behavioural biometrics like gait, eye or limb movement. Extraction of biometric or physiological information from generic sensor data may depend on increasingly sophisticated remote filtering and analysis. While this technology is improving rapidly, it may be outside the range or capacity of in-cabin specialist sensors. From there, further inferences can potentially be drawn about health, emotional, cognitive, behavioural, inebriation or physiological attributes or status of the driver or other occupants.

Some of this information, if tied to an identifiable individual, is considered 'sensitive information about an individual',[10] the highest classification of privacy related information (see section 3.8). It may itself also be identifying to the extent it captures unique or rare traits.

Biometric information can also be identifying, particularly if relying on remote access to databases of biometric data templates and to special software.

While sensor and biometric functionality is potentially applicable to individuals *outside* the vehicle, this is less likely in the near term. The limited externally capable sensors might be able to distinguish pedestrians who had particular attributes (such as age, intoxication level, disability) if those attributes became useful in predicting potential high-risk interactions with pedestrians nearby. It is less likely that the specialist sensors would contribute significantly to direct identification of people external to the vehicle, although the generalist camera data could, if coupled with sufficiently sophisticated remote recognition software and data sets, potentially identify some external people. It is unclear whether, or how soon, such capabilities will be available.

2.2.5 Audio data

2.2.5.1 Data from In-cabin microphones and entertainment systems

This includes audio signals and audio recordings.

[10] See Section3.8, below. Where information is 'sensitive information about an individual' (which may include some information that is not 'personal information'), there are additional constraints in privacy principles. These include a greater reliance on consent or special justifications for collection, and a more limited scope for permitted secondary uses not 'directly related' to the primary purpose of collection.

Derived information: In-cabin audio data may capture sounds made in the cabin by one or more occupants to the vehicle (for voice-controlled systems) or to each other, or to external parties such as those on a phone or video call.

Assuming speech recognition and speaker recognition functions are in operation, the audio may when processed also reveal the identity of some or all speakers, the number of speakers, the words spoken, the nature and content of a conversation, and perhaps tone of voice. This may also reveal emotional or physiological attributes of the speaker, or of the interaction.

See also Section 2.2.4, above.

2.2.5.2 External microphones

If a vehicle is designed to be able to hear someone outside shouting 'stop', it will need an external microphone.

Derived information: External microphone data may reveal similar information to in-cabin microphones, above, though with potentially less prospect (or intention) of identifying speakers or understanding the detail or meaning of words spoken, and more focus on understanding if there is a human or machine warning or alert in the external sound. Biometric or physiological voice attributes like alarm, threat or panic may be of most interest.

2.2.6 Data supporting operation of ADAS and automated functions

2.2.6.1 From input units

This includes sensor, radar, Lidar and similar data streams.

Derived information: This data may reveal information about locations and features nearby, their proximity and speed relative to the vehicle, generally mapping objects and people and their movement.

While it is less likely to generate information that directly identifies people, capturing features of the context and environment and distinguishing people from this background may contribute to the accuracy or viability of this identification task using other information.

2.2.6.2 *From Electronic Control Units* (ECUs)

This includes data about speed, journey distance, driving performance, and vehicle diagnostics or fault conditions.

Derived information: This data may reveal information about speed in a location, journey duration and time, and vehicle safety.

Coupled with other data, this may reveal whether the speed at a particular moment, or the duration of the journey for heavy vehicles, is over or under the legal value, where that value is provided by V2I, route or other information.

2.3 Legislation covered in this Report

The legislation covered in this Report is set out in the 'Sources' section at the end of this Report.

Sections 3, 4 and 5 of this Report focus on privacy legislation. It is worth noting at the outset that not all states have privacy legislation. There is no privacy legislation in WA,

though some related issues are covered in a Freedom of Information law, so we mention that WA FOI Act in places. In SA there is no legislation but there is an Information Privacy Principles Instruction (IPPI) published as Premier and Cabinet Circular No. 12 of June 2016. Comparisons among privacy legislation in each jurisdiction are otherwise analysed throughout.

NSW and Victoria have separate health privacy acts, and Queensland has a separate part of its general privacy act to cover health. The other jurisdictions typically cover health information as part of the general privacy act. This can explain some omissions or inclusions in what is considered 'personal information' and 'sensitive information', as set out in Appendix B, Tables 1 and 2.

In each jurisdiction, privacy legislation operates on the basis of 'privacy principles'. In this Report, principles will be referred to by the relevant abbreviations, as below.

Table – Abbreviations of privacy principles

Abbreviation	Name of principles	Jurisdiction
APPs	Australian Privacy Principles	Commonwealth
IPPs (NSW IPPs, NT IPPs etc.)	Information Privacy Principles	NSW NT QLD SA VIC
TPPs	Territory Privacy Principles	ACT
PIPPs	Personal Information Protection Principles	TAS
HPPs*	Health Privacy Principles	NSW (health specific) VIC (health specific)
NPPs*	National Privacy Principles	QLD (health specific)

* These are rarely mentioned in this report since they mostly cover medical records alone.

Terminology for each jurisdiction, and correspondence among privacy principles, is also detailed in Appendix C, Table 1. Appendix C, Table 2 gives an example of a road law, the recent *Heavy Vehicle National Law,* with provisions dealing with many of the same issues but not framed as privacy principles.

While many of the activities of interest for this report will be those of state agencies so IPPs etc. will be relevant, APPs are also often cited for several reasons: the IPPs are in many cases derived from the APPs or their precursors; APPs cover private sector organisations (with turnover over $3m) and may influence their compliance obligations in responding to government requests for information from C-ITS or AV systems, while most state and territory Principles focus on public sector agencies; and federal agencies covered by the APPs have a significant role.

Appendix B, Table 2 includes extracts from the text of privacy principles dealing with collection, use and disclosure in the context of Sensitive personal information.

Other legislation on roads, criminal, surveillance devices and telecommunications matters is considered in sections 4, 6 and 7, and Appendices E and F.

3 'PERSONAL INFORMATION' AND 'SENSITIVE INFORMATION'

Whether an item of information fits the legal category of 'personal information' (PI) is a central question for privacy regulation in Australia, and it affects legal obligations relating to C-ITS and AV information. Sections 3.1 and 3.2 discuss why the scope of this term is important, and explore and compare the definitions of the term in different jurisdictions' privacy laws. Sections 3.4–3.6 consider factors which may contribute to classification of a specific item as PI or not. Section 3.7 reviews the data categories from Section 2.2 and suggests the likely classification (PI or not) of each category. Finally, Section 3.8 considers the category of 'sensitive information' (SI) in terms of which types of information will fall into this category in different jurisdictions, and the consequences of such classification.

Many types of information from C-ITS and AV systems are likely to be PI in some or all circumstances, with only a few unlikely to be PI in most or all instances. But the degree of certainty, and the proportion of all instances of a particular type of information that may be PI will vary with the context. Some types of C-ITS and AV information will also be SI.

3.1 Why 'Personal Information' (PI) is important

Whether an item of information fits the legal category of 'personal information' (PI) is a central question for privacy regulation in Australia and thus affects legal obligations relating to information from C-ITS and AV systems. The meaning of PI is critical for both practical and legal reasons. Practically, if a data item or information element is not 'personal information', its disclosure or use will have little specific impact on a given individual. Legally, privacy law will only apply to PI.[11] Subtle nuances of the interpretation of PI can therefore make a difference to the protection and constraints that are required when dealing with a certain category of information.

Certain information may also be specifically deemed to be PI by the provisions of a particular law, and we note these where they are relevant.

3.2 Definitions of 'personal information' in statutes

Different jurisdictions in Australia have similar but slightly different definitions of 'personal information'.

3.2.1 Definition in *Privacy Act* (Cth)

The current definition of PI in the *Privacy Act 1988* (Cth) s 6 is as follows:

> ***"personal information"*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

Where we are not dealing with simple identification information like name and address which would fall into information about an 'identified individual', the critical term is

[11] There is a small set of information, including certain biometric and genetic information, that could theoretically be SI but not meet the definition of PI, and this would also be covered by relevant privacy laws along side PI. But for most realistic purposes PI is the critical concept. See section 3.8 for details of the scope of SI.

'about … an individual who is reasonably identifiable'. The key question then becomes the degree to which an individual is 'reasonably identifiable'.

There was an additional condition at the Commonwealth level that the person be 'identifiable from the information'. While this was removed in 2012, this additional condition continues to operate in some other jurisdictions – see Appendix B, and the discussion below.

3.2.2 The definitions in state and territory law compared

The definitions of PI in state and territory laws are similar, with some variations, as summarised below. Appendix B, Table 1. 'Personal information' includes the full definitions for each jurisdiction.

The practical impact of jurisdictional differences varies, with many variations of limited practical effect. One of the more significant is the exclusion, inclusion or restriction of specific sub-categories of information, such as health information or 'government information'. In some jurisdictions, there is a separate law for that category (health, as noted in section 2.3); in others the mechanism creates gaps ('government information' only in NT). Another potentially significant variation is the retention of the qualification that the individual be identifiable 'from the information', although the practical impact may be reduced for the reasons set out below.

Identity is 'reasonably ascertainable': This and related variations in wording exist in some states and territories (See Appendix B: NSW, NT, Qld, SA, Tasmania, WA) but the differences have little practical impact.

Exclusions based on separation of legislation: The ACT, NSW and Victoria do not include personal health information as this is dealt with in separate health records privacy laws, as noted above. This supports a similar but separate regime for these states' health information, with different privacy principles (see Appendix C).

Other specific exclusions: NSW and some other states and territories (see Appendix B) also have definitions with a list of specific exclusions, but these are generally not relevant to C-ITS and AV information.

Specific inclusions: The NSW definition explicitly includes biological samples, but this is unlikely to be relevant.

Identifiable 'from the information': A person must be identifiable 'from the information' in some versions but not others. This more restrictive wording is present in the definition of PI in Queensland, Victoria, NSW, but not in the ACT, NT or (after 2012) the Commonwealth. At its strongest, the additional words could mean that information does not become PI merely because there may be potential for linking with other information. However, this interpretation is unlikely. This is because there has been guidance from regulators interpreting these additional words suggesting that the effect of using with other information can still be taken into account, especially where there is any doubt as to whether it should be treated as PI. For example, when a similar restriction existed in the Commonwealth Act, there was formerly OAIC guidance that suggested that such a strict reading of 'from the information' in the former version was inappropriate.[12] There is also NSW IPC guidance[13] which says 'Identifiability is not a

[12] The former guidance, current when 'from the information' was still in the Commonwealth definition, is no longer accessible. The now-current OAIC guidance says 'Where there is uncertainty [about the meaning of 'personal information' when it is not clear and is dependent on context and circumstances], the Office of the Australian Information Commissioner (OAIC) encourages entities to err on the side of caution by treating the

black and white concept. There are many shades of grey between data from which individuals are readily identifiable, and … entirely anonymised. When in doubt, assume that data will meet the definition of personal information'. In addition, the strong interpretation would mean that identifiability was assessed out of context – but the identifiability of any information is inherently linked to what else is known. The inclusion of the nominally more restrictive wording 'from the information' is therefore likely to be of limited real practical significance.

For completeness, lawful data linking would often be unlikely to breach privacy principles as privacy principles typically do not prevent identification. Data linking could however make more information 'reasonably identifiable'. It is the capacity for data matching and linking which is interesting, not merely whether it has actually occurred: if this is easy to do, cheap and well understood but it is not being done just now, is its use 'reasonable' or not? NSW Privacy commissioner guidance mentioned in the previous note cites *Ben Grubb and Telstra* [2015] AICmr [35][14] 1 May 2015 at [52] to say that data matching can be taken into account.

There is an additional element in WA's *Freedom of Information Act* (which as noted in 2.3 is the closest to a privacy law in WA). In this law individuals can also be identifiable from 'an identification number or other identifying particular' (like a fingerprint). Use of an 'identification number or other identifying particular' implicitly separate from the information in question could have some practical impact in broadening the scope. The 'identifying particulars' exemplars are biological (similar to a specific inclusion in NSW, which adds genetic samples); this would probably cover biometrics useable for identification. It is not clear if device data identifiers reasonably linkable to a person might also be covered, since they were unlikely to have been considered when the definition was created (no later than 2004 and probably as early as the first version in 1992). However this is just one state, and not a real privacy act, so the net effect would be small.

Entities bound by legislation: Each jurisdiction has slight differences in which entities are bound by privacy law. State and territory legislation typically covers agencies and other government bodies under their jurisdiction but do not cover federal government, private sector or not for profit bodies. The partial exclusion of law enforcement and security entities is a common theme. (See Appendix D, and section 4.5 below.) The details of other exclusions can be complex.

Scope of information: In the NT, only 'government information' can be 'personal information' covered by the *Information Act*. '"Government information" means a record held by or on behalf of a public sector organisation and includes personal information.'[15] C-ITS or AV information directly collected by government as a record would be covered, and information collected by third parties which becomes a government record would probably also be covered. So there would be limited practical effect of this reduction in scope for current purposes.

---

information as personal information, and handle it in accordance with the Australian Privacy Principles (APPs).' 'What is personal information?' OAIC (online), Guidelines section, May 2017 <https://www.oaic.gov.au/resources/agencies-and-organisations/guides/what-is-personal-information.pdf>.

[13] 'Reasonably ascertainable identity', undated, <https://www.ipc.nsw.gov.au/fact-sheet-reasonably-ascertainable-identity-0>. They also cite a test by NSW tribunal of 'more than moderate steps' *AIN v Medical Council of New South Wales* [2016] NSWCATAD 5.

[14] This case was the first stage of the litigation we discuss in Appendix A and elsewhere as *PC v Telstra*; it is at the Commonwealth level, but referred to the old version of their Act which still had 'from the information' present.

[15] *Information Act* (NT) s 4. In s 4A, 'personal information' is a subset of 'government information'.

Dead persons: In most jurisdictions, the individual must be living. In Tasmania, their information is captured if they died within the previous 25 years, in NSW 30 years. In WA, all deceased are included. This will be of limited practical effect, except perhaps in the aftermath of fatalities.

3.2.3 Compare definitions of PI in state and territory road transport laws

In this section, we discuss the definitions of PI in heavy vehicle laws. One reason why more examples are not included is that many road and traffic laws do not define PI, in particular:

- many of road and traffic laws do not use or define PI, including the *Road Transport Act 2013* (NSW), *Roads Act 1993* (NSW), *Road Traffic (Authorisation to Drive) Act 2008* (WA), and most such laws in Victoria.
- in some road and traffic laws, the term PI is used but not defined, for example in *Road Transport (Driver Licensing) Act 1999* (ACT), *Road Transport (Vehicle Registration) Act* 1999 (ACT) and *Transport Operations (Road Use Management) Act 1995* (Qld).
- some road and traffic laws (such as *Road Traffic (Administration) Act 2008* (WA) s 32) have definitions of related terms like 'personal details', which are however not of direct interest, being applied to a narrower scope of activities like police investigation.

Heavy Vehicle National Law (NSW) No 42a[16] contains a definition of PI as follows:

> **'personal information**—
> (a) generally, means information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be found out, from the information or opinion; and
> (b) for the purposes of Chapter 7, has the meaning given by section 403.'
>
> In s 403, "personal information" means 'personal information that is intelligent access program information or otherwise collected for the purposes of this Chapter'.
>
> (See below for the criminal penalties created for a collection privacy principle applying to this program alone.)

The core of the definition above is closest to that in Sched 5 Queensland *Information Privacy Act* , and is also quite close to the s 3 *Privacy And Data Protection Act 2014* (Vic), though it uses the novel term 'found out' instead of 'ascertained'. This difference is unlikely to have practical effect. The HVNL includes a reference to 'database' which is absent from some other versions; again, with little effect. It also differs from Commonwealth and ACT by retaining 'from the information'; as noted in the discussion above, this is superficially significant but likely of little practical effect. It can probably be grouped with Queensland and Victorian versions for this purpose.

The *Heavy Vehicle National Laws* are also interesting in one other respect: some relevant local privacy laws do not apply to them, except to a state entity or employee exercising a function under that law: see for instance *Heavy Vehicle National Law (Tasmania) Act* 2013 (Tas) s 6. The NSW version above applies a different,

[16] S 5; see HVNL (NSW) <https://legislation.nsw.gov.au/#/view/act/2013/42a/full>.

extraterritorial approach: the NSW HVNL law says that Queensland's *Privacy Act*, and some other laws, apply in NSW for this purpose.

See also Appendix C, Table 2 for a description of the de facto privacy principle provisions embedded in Part 7.5 of the *Heavy Vehicle National Law (NSW),* and the Queensland equivalent *Heavy Vehicle National Law 2012* on which the other state laws are based.

3.3 Interpretation

There are two concepts the interpretation of which are crucial for all jurisdictions with privacy legislation – these are 'reasonableness' and 'about an individual'.

3.3.1 Reasonableness

The standard of 'reasonableness' is deliberately vague. In some circumstances, a generic standard of 'reasonable' based on what an ordinary member of the public could do unassisted may theoretically be appropriate. In other circumstances, this would be artificial because there may be a range of entities that could more easily identify a person in certain circumstances. Because identifiability depends on context, the situation of the entity would likely be treated as relevant. The importance of context in identifiability is discussed further in Section 3.4.

3.3.2 'About' an individual (or, in SA, 'relating to' an individual)

One issue in the definition of personal information is when information is 'about an individual'. This issue arose in the *PC v Telstra* case,[17] albeit in the context of earlier wording in the Commonwealth Act that referred to information being about a person' and included the phrase 'from the information'.[18] The question was whether information about how a person's call was routed in the telecommunications infrastructure was 'about' the person making the call. The court held that it was not 'about' the person making the call, at least in the particular circumstances of the case. The current relevance of this case is that assessing whether information is 'about a person' (or 'about an individual') will require an understanding of the particular information and its context. (See Appendix A, 1. *PC* v *Telstra* for more detail.)

Another case to consider is *Waters v Transport for NSW*[19] which held that travel information (location information such as tap on and tap off data generated by a card going through readers, and the journey information it creates) could be PI. The judgement considered *PC v Telstra* (distinguishing it) and examined a number of other cases at state level discussing what 'personal information' means in particular instances. It reaffirmed that this question is always context dependent. In conclusion, it stated that the factual situation in *PC v Telstra* was at the remote end of a continuum, while the location information at issue in *Waters* was much less remote from the person. (See Appendix A, 2. *Waters v Transport for NSW* for more detail.)

---

[17] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 (19 January 2017) <http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/full/2017/2017fcafc0004>

[18] It also predates the telecommunications metadata retention legislation, *Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015 (Cth); s 187LA deems this kind of retained information to be PI.

[19] [2018] NSWCATAD 40, 15 February 2018, McAteer J. <https://www.caselaw.nsw.gov.au/decision/5a8351f1e4b074a7c6e1c492>

3.3.3 Comparison

It is worth comparing the drafting and interpretation of PI in Australia with equivalent terms in the EU and US. See Sections 8.2 and 8.29.1 respectively

3.4 Factors affecting identifiability

3.4.1 Relevance of context

There is not one measure of identifiability.

The more useful related information you have, and the more effective tools, the more identifiable a given data set becomes. Whether a person is reasonably identifiable from it is not solely an intrinsic quality to the information, it is also a feature of the context, and the legal and practical resources available to those who seek to identify. The ability to identify an individual from a data set may vary:

- *over time* – a given manipulation or identifying effort often becomes easier, faster, cheaper or more feasible over time, especially with increasing adoption of machine learning tools and availability of big data sets;
- *between individual data subjects* – the task of trying to identify some individuals may attract greater willingness to expend time and effort than others. For instance, compare a targeted investigation seeking to prevent or apprehend a person making a credible threat to cause immediate serious harm with a suspicion-less survey of a whole population for a less urgent or compelling reason; and
- *between different entities trying to identify an individual* – they can vary by the closeness of their relationship to the individual or someone who can identify them already, the nature and degree of their motivation based on the purpose of the identification and thus their willingness to expend time and effort, their technical capacity, their access to other information which would help identification, the time available, and their power or ability to seek or compel assistance from others.

Who is doing the identifying matters, as the following examples may confirm.

- A person can more easily identify their neighbour from a taxi data set than a stranger because they know where that neighbour lives and works, and so can deduce which record corresponds.
- Data linked to IP addresses that would not be reasonably identifiable by an ordinary citizen may be quite easily identifiable for a telecommunications company that has a lookup table of assigned IP addresses.
- Power to compel an information host to give access to a related data set or directory increases the ability to identify an individual in a data set.

The more sources, linkage of data sets, mining, cross referencing, and access to contextual information that a particular entity can bring to bear on the task of identification, the more likely it becomes they can identify an individual associated with a nominally non-personal data point like an IP address or mobile device IMEI number (the International Mobile Equipment Identity handset or device identifier).

3.4.2 Ability to de-identify and re-identify

De-identification is a process, not an outcome. Removing obvious identifiers (such as name and address) does not mean that an individual cannot be re-identified. It is not

clear whether information can be permanently de-identified while remaining sufficiently rich for analysis. Narayan and Felten argue that machine learning techniques and access to increasing sets of big data will undermine effectiveness of any de-identification process. Cavoukian and El Emam argue that, while pseudonymous information can be re-identified, with sufficient expertise it is possible to create reliably de-identified data sets. Rizoiu et al[20] suggest the initial level of 'privacy protection' from de-identification will inevitably decline over time. This means de-identified data is more likely to become 'personal information' over time, and any protection may not be permanent.[21] The theoretical question, however, is not the relevant one – which is simply whether the person is 'reasonably' identifiable in a particular context. (See also Appendix A.)

3.4.3 Storage and retention

The more complete your information is (complete capture as opposed to fragmented capture) and the longer it is stored, the more feasible it is to re-identify individuals. A transient sample of a data stream is harder to put in context compared to a stored longitudinal sample of many data points. The location where information is stored and the period for which it is stored may thus impact the reasonable identifiability of individuals within it. This suggests differences between an un-cached stream and one which is sampled and stored; and between a small, fragmented stored sample and a full, complete capture with long-term retention.

3.5 Who can Identify?

Because, as noted in Section **Error! Reference source not found.**, the classification as PI can depend on who has access to the information and their legal powers and practical capacities, this Section focuses on relevant entities in the context of C-ITS and AV technologies.

3.5.1 The automated driving system entity (ADSE)[22]

Some ADSEs managing the big data sets and advanced AI tools needed to support C-ITS and AVs will have access to other sources of information, beyond that produced by AVs and C-ITS themselves. Large data companies such as Google and Apple may supply C-ITS and AV systems. Where ADSEs have access to large information holdings, they can combine vehicle data with these other data sets (subject to their own privacy policy and contract with users). For such companies, what is reasonably identifiable may be broader than for companies without significant data holdings.[23]

---

[20] Marian-Andrei Rizoiu et al, 'Evolution of Privacy Loss in Wikipedia,' WSDM 16, February 22–25, 2016, San Francisco. <http://dx.doi.org/10.1145/2835776.2835798>.

[21] Several 'anonymised' data sets released by Australian government agencies have been re-identified within days. See the 10% Medicare sample re-identification in 2016: Culnane et al, 'Understanding the maths is crucial for protecting privacy', *Pursuit*, University of Melbourne, 29 September 2016 <https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy>.

[22] The automated driving system entity is the legal entity responsible for the automated driving system. The automated driving system means the hardware and software that are collectively capable of performing the entire dynamic driving task on a sustained basis.

[23] There are recent reports of design efforts by some ADSEs to reduce this, by omitting end points from journey data used for map validation or restricting interaction data to encrypted on-device stores. M Panzarino , 'Apple is rebuilding Maps from the ground up', *TechCrunch*, ,29 June 2018, <https://techcrunch.com/2018/06/29/apple-is-rebuilding-maps-from-the-ground-up/>. While voluntary, these may illustrate possible regulatory options.

3.5.2 Vehicle manufacturer or other service provider

The vehicle manufacturer may not be the automated driving system entity, but they are still likely to have a keen interest in the data streams out of the vehicle. Generally speaking, most vehicle manufacturers (at least today) have narrow information holdings and would find it difficult to re-identify individuals from raw vehicle data. However, where vehicle manufacturers retain identifying information that links initial purchasers to particular vehicles, data attributed to particular vehicles will be PI.

3.5.3 Operator of road infrastructure

The operator of the road infrastructure will collect large amounts of data, and probably play a role in minimising accidents and abuse. They may also expect to be called on to assist regulation and compliance efforts. Consequently, they can be expected to have access to a wide range of information that could aid identifiability.

3.5.4 Law enforcement and intelligence agencies

While law enforcement and intelligence agencies do not have primary access to or control of vehicle data, they can use legal compulsion, including through warrants and authorisations, to require other entities make information available for their purposes. Such agencies may also have technical capacity to analyse data in ways not normally accessible to other parties. Bodies such as the Australian Criminal Intelligence Commission have even more extensive data sources and capabilities.[24] Thus, in the hands of law enforcement and intelligence agencies, more data may be classified as PI.

3.5.5 Others: Telcos, cloud operators, IT security

There are other relevant entities, particularly in telecommunications, cloud and IT security services. Many of them have to use tools like packet inspection for ordinary maintenance and troubleshooting. It may not be very difficult for them to use deep, low level network tools, extensive logging, or other information about network users to help identify the provenance of a given data stream or data set. In this case, more data will be classified as PI in their hands than it would be if in non-technical hands.

3.6 Identifiability from location Information

Location information is a special case. In some cases, it may be too remote from the individual to assist identification. In other respects, it potentially enables a deep set of inferences about a person and therefore could assist in identifying an individual. For example, daily travel between a particular home and a particular workplace would often be sufficient to identify an individual. It is useful to examine the range of contexts for location information.

3.6.1 GNSS data

GPS and similar GNSS data can be used to derive location information about the vehicle, and by extension the occupants.

[24] *Australian Crime Commission Amendment (National Policing Information) Act 2016* (Cth) carried over CrimTrac functions to ACIC, including 'systems and services relating to national policing information and nationally coordinated criminal history checks' for use by 'police, justice agencies and policymakers at all levels'.

3.6.2 Phone tower data (3G, 4G, 5G etc.)

There are several layers of data interchange between a 'phone tower' running the modern IP based network system and device handsets. This information is used by devices to estimate location.

Because most devices require explicit contracts between providers and customers, who must be identified for billing purposes, the user's identity is more likely to be 'reasonably ascertainable' in the hands of the telecommunications provider, and thus potentially PI.

Section 187LA of *Telecommunications (Interception and Access) Act 1979* (Cth)[25], which applies to some aspects of 'location information' from mobile devices and phone towers, states explicitly that the telecommunications data it covers is deemed to be 'personal information' for its purposes. This is an interesting example of a class of technical data being deemed to be 'PI' by law. It has not been judicially considered, and the language describing the data is quite opaque, but it may offer further persuasive support to the necessity to treat some of the data output of C-ITS and AVs as PI.

3.6.3 Short range wireless communication data (including DSRC and Bluetooth)

The DSRC system is for use in V2V and V2I communications. Since there are fewer personal links between occupants and the DSRC system, the chain of connections which may enable identification will likely be weaker. However, this would not be the case where identifiers for vehicles can be reasonably linked to individual vehicle owners. Thus communications using DSRC, implicitly including location information, will generally only become PI when linked with vehicle identifiers.

Bluetooth data also needs to be considered as a subset of short range location information. It is a short range general purpose consumer and IoT wireless system similar to WiFi (using the 2.4 GHz band rather than the 5.8/5.9 Ghz of DSRC), embedded in a growing range of devices. Its short range complements GNSS and WiFi data for location purposes. BT devices may be ubiquitous and disorganised and thus harder to identify than DSRC, which is customised for specific C-ITS purposes and more well-managed.

3.6.4 When does location information become PI?

While raw device location information may not on the face of it appear to be personal, it can often be related back to an individual whose home and/or work addresses are known or where an identifier is used that can be linked to an individual.

3.7 Which data may be 'personal information'?

This section sets out practical implications of the assessment of factors going to the characterisation of a data set, in a given context, as PI or not. The table below summarises the conclusions, and the discussion afterwards helps explain them.

Table – How identifiable are data types?

Data type	Identifiable or not?
Image data external to the vehicle	Possible PI, if individuals are recognisable.

[25] See *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth).

Data type	Identifiable or not?
Image data internal to the vehicle	Highly likely
Event Data Records	Possible
Location/route data from Navigation System data	Highly likely
Location/route data from V2V/V2I communication	Likely
Data covering biometric, biological or health factors	Possible
Data from in-cabin microphones and entertainment systems	Almost certain
External microphone	Unlikely, unless combined with other information
Input units	Unlikely, on their own
Electronic Control Unit data	Possible

3.7.1 Image Data

3.7.1.1 Image data external to the vehicle

This is likely to be PI, although only when linked with other information and sophisticated processing capabilities. External camera input unit data streams alone and in conjunction with current and future image, face and numberplate recognition may assist identification of vehicles nearby, and in traffic along the route, by their number plate or, less feasibly, by their external characteristics. They may also potentially assist identification of individuals on the street or nearby. There may however be a less rich local data environment from other data sources available to the vehicle with which to combine the raw data or 'pattern recognised' external image information; this may mean it is less likely that identification of those individuals in visual range of the external cameras can reasonably be done.

If the image data is made available for further processing and comparison to data sets or biometric templates held by other entities, for instance by being made accessible to remote 'hub' services, this may increase the capacity for identifying individuals, but the degree to which this occurs will likely depend on the context of each image set and the capacities of that other processing system. In the short-term, this data will not be PI but may become so in future.

3.7.1.2 Image data internal to the vehicle

Internal camera data is highly likely to contribute to identification of the driver and occupants, either through built-in recognition functions at the time, or when examined as a recording later. Thus internal image data will almost always be PI, though perhaps less so for occupants other than the driver or person in charge of the vehicle.

3.7.2 Crash data – Event Data Records

Crash data alone appears less likely to be directly usable for identification purposes. It can probably be linked with other information (assuming it is explicitly attributable to a particular vehicle at a particular time) to become PI, but its value without the linking would be low. Crash data may, depending on the EDR data set retained, reveal

information about a driver's behaviour before a crash, especially if combined with data from ECU. This could implicate the driver or occupants in a driving offence, assuming they were identifiable from other data sources, so it may be PI in this context.

3.7.3 Location and route data

It is highly likely that the data from both navigation system and V2V and V2I systems will be properly characterised as PI.

3.7.3.1 Location and route data from Navigation Systems

Sufficiently detailed trip information, especially if retained and collated over time and analysed for repeated patterns, could reveal with varying certainty attributes which assist identification (and help show a 'pattern of life'). Location and route data may become PI through association with a combination of a home address, a work address and the addresses of friends and relatives.

Route data with embedded time codes could establish the regular timetable of vehicle users, including when they are typically, or on a given day, at home or out, when they are at work, when they pick up children or relatives, and many other 'pattern of life' times and dates. It is almost certain that some or all of this information, on its own, could identify both the individual in control of the car (usually the vehicle owner and likely driver, but potentially anyone); and with less certainty, some other significant individuals in their life and networks.

3.7.3.2 Location/route data from V2V and V2I communication

The characteristics of this data and certain pseudonymising precautions reduce direct identifiability. However, PI that has been pseudonymised can still be attributed to a specific person if it is linked with other information, so will often remain PI.

The unique identification number broadcast by a C-ITS enabled vehicle using DSRC may not in itself directly identify a vehicle or user. Security certificates used to secure V2V and V2I communications are pseudonymised, offering a first layer of defence protecting personal information.[26] But these broadcast messages exchanged by vehicles with other vehicles and roadside infrastructure are more likely to be PI because the vehicle owner and likely driver can be re-identified from a series of potential links from the C-ITS identifier. This is consistent with the view of the Data Protection Working Group of the C-ITS Platform in the EU, and with the conclusion of an independent PIA for Austroads in August 2016. C-ITS technology would also produce location information, which may independently contribute to identifiability.

3.7.4 Biometric, biological or health data

Some of this data will be PI and, in addition, may contribute to re-identification of other information from the vehicle.

While special purpose biological or physiological sensor data is less likely to contribute to identifiability, general purpose sensor data (from say camera or microphone) capturing information about biometric attributes like voice, face or iris patterns may contribute to identification if it is made available to recognition systems (data template

[26] In the EU, the Data Protection Working Group (WG) of the C-ITS Platform noted that security certificates of C-ITS messages to establish trust of V2V and V2I communications are pseudonymised, and the vehicle or user is pseudonymised.

sets and pattern recognition software), either remotely in real time or from a recording later.

3.7.5 Audio data

3.7.5.1 Data from In-cabin microphones and entertainment systems

In cabin audio data could contribute to identification of occupants of the vehicle if *speaker* recognition tools are used and/or *speech* recognition tools extract identity clues. The audio parameters for speaker and speech recognition inside the cabin are favourable, since there is low noise, a good signal, and a limited known range of individuals likely to be in the cabin. They may also be directly linked to other equipment such as mobile phones that can be easily tied to an individual.

In addition, if the audio of voice is transcribed or analysed for content rather than recognition, the words said might also contribute to identifiability, and mention the names of other individuals who may be identifiable.

3.7.5.2 External microphone

As with external camera input data, data from external microphone may have some capacity to identify individuals, although with much less intrinsic capacity to combine and cross-link information compared to that available on the vehicle occupants. There is thus a much lower likelihood that a given external individual could be identified. If voice/speaker recognition (as opposed to speech recognition, which can understand words) is turned off, the prospect of external audio being a useful contributor to real-time identification of people outside the cabin may be low or negligible. In that case the data may not be, on its own, PI. If voice/speaker recognition is activated, or the data is in the form of an audio recording that can later be processed or analysed, the potential for it contributing to identification may increase – but perhaps still not very far, since trying to identify random individuals out of millions from snatches of their voice audio heard from afar in a possibly noisy street would have limited success for most current systems.

However, if the recently established national biometric identification scheme[27] develops capacity to capture and/or process voice recognition data on a mass scale and makes it available widely to law enforcement and compliance authorities, and signal processing capacity for extracting voice from noisy backgrounds continues to improve, this may change in the future. Voice recognition is probably not an early focus of that scheme, but it may be developed further in future, so this is not a near term issue.

3.7.6 Data supporting operation of ADAS and automated functions

3.7.6.1 From input units

Lidar and radar would mostly be used for mapping objects in the environment. They would improve location accuracy to a minor extent, and perhaps detect objects which were people, but on their own would be unlikely to directly contribute to identifiability of external parties. However, when coupled with external cameras in the same system,

[27] 'Biometric Identification Services', Australian Criminal Intelligence Commission, 2017, <https://www.acic.gov.au/our-services/biometric-matching/biometric-identification-services>; 'Intergovernmental Agreement On Identity Matching Services', COAG, 5 October 2017, <https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf>. See also discussions of the national biometric recognition 'hub' capability.

the potential for identification of other people and of the number plates of objects recognised as vehicles by combination with that data would be significant.

3.7.6.2 From Electronic Control Units

Data from these systems could contribute to location information and journey tracking, especially if as expected the range and data intensity of the sensors increases. However, much of the information would be about the vehicle's operation and would not in itself be likely to be personal information. In combination with other information, the driver or passenger could become identifiable. Further, in some circumstances, behaviours or dynamics of the vehicle could be used to identify a specific individual. Such capability would be useful to law enforcement in identifying a driver who disobeys road rules.

3.8 'Sensitive Information' – partly overlaps with PI

3.8.1 'Sensitive information' about an individual

Some information involved in C-ITS and AV systems will fit the definitions of 'sensitive information about an individual' (SI or 'sensitive information'). This is important because the collection, use or disclosure of sensitive information may need to meet higher standards than PI or information that is not SI.[28]

The definition of sensitive information differs among jurisdictions (see Appendix B Table 2). In some cases, sensitivity corresponds to the intrinsic sensitivity of particular data, such as biometric identification data.[29] The sensitivity (both in practice and at law) of other information or opinion may depend on context, location or content. For example, words spoken in a vehicle and captured by internal audio recorders may be subjected to speech recognition and capture statements about political opinion or sexual practices.[30]

It is sometimes assumed that 'sensitive information' about an individual is just a subset of PI, but this is not necessarily the case. Certain items (health, genetic and biometric information) can be 'sensitive information about an individual' in some jurisdictions even if they do not meet the definition of PI. Thus the 'sensitive' category is not a true subset of PI.[31] This is true for Commonwealth *Privacy Act* and most of the state and territory privacy laws that have a 'sensitive information' category. The Commonwealth definition is as follows:

"**Sensitive information**" means:

(a) information or an opinion about an individual's:
  (i) racial or ethnic origin; or
  (ii) political opinions; or
  (iii) membership of a political association; or
  (iv) religious beliefs or affiliations; or

[28] See also Appendix B Table 2 for definition and IPP provisions on collection and use in state and territory law.
[29] Only ACT and Commonwealth define sensitive information to specifically include biometric information. In other jurisdictions, this may be practically sensitive (and viewed by consumers as such) but handling of it may not need to meet the more stringent requirements associated with sensitive information.
[30] All jurisdictions with a 'sensitive information' category include political opinion and sexual practices.
[31] As can be seen from the definition below, some items in (a) are defined as also needing to meet the 'personal information' definition, while those in (b)–(e) are not. The separate treatment of the latter group in effect removes doubt as to whether they might only be 'sensitive' if they can identify the person; their 'sensitive' status does not appear to rely on meeting the conditions for 'personal information', so long as they are 'about an individual'.

(v) philosophical beliefs; or
(vi) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual orientation or practices; or
(ix) criminal record;
that is also personal information; or
(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information; or
(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
(e) biometric templates.[32]

The practical implications of some of these items are mentioned below, particularly in relation to in-cabin audio recording processed with speech and speaker recognition.

3.8.2 Variations on the definition of 'sensitive information'

There are a number of variants of the scope of 'sensitive information' in the states and territories.

- NSW, South Australia and WA do not have a 'sensitive information' category at all: it is absent from the privacy laws in NSW (PIPPA and HRIPPA) and the IPPA in SA. WA has no privacy laws.
- Victoria deals with health information in *Health Records Act 2001* (Vic) rather than *Privacy Data and Protection Act 2014* (Vic). The *Privacy Data and Protection Act 2014* (Vic) does not include biometric or genetic factors as SI. So, in Victoria, SI is a subset of PI based on the list of nine personal information types in paragraph (a) of the Commonwealth legislation.
- Only the ACT and Commonwealth definitions include biometrics and genetic information, and neither requires these two items to meet the PI definition to be considered 'sensitive'.
- The Commonwealth, NT, Queensland and Tasmania include health information as SI, whether or not it meets the definition of PI.

3.8.3 Collection of sensitive information

Sensitive information attracts different, more restrictive treatment in most Privacy Principles. The main impact of classification as SI is on collection.

Australian Privacy Principle (APP) 3.3 basically requires that collection of *sensitive* information about an individual be based on either the individual's consent and that the information is reasonably necessary for (or in the case of an agency, directly related to), one the entity's functions or activities; or the existence of one of the special grounds in APP 3.4. Those special grounds include collection required or authorized by law or court order, reasonably necessary for an enforcement body's functions, or an instance of a 'permitted general situation' or 'permitted health situation'.

[32] s 6 *Privacy Act 1988* (Cth). See Appendix B Table 2 for a comparison of provisions in other jurisdictions.

This is more stringent than the treatment collection of non-sensitive PI in APPs 3.1 and 3.2, which also allow collection without consent simply where it is reasonably necessary for (or if the collector is an 'agency', directly related to) the collector's functions.

The details of the Privacy Principle constraints on collection of sensitive information in the states and territories can be seen in the 'Collection' column of Appendix B Table 2.

- NSW, SA and WA have nothing on sensitive information collection Privacy Principles, for the reasons noted above.
- The rest of the Privacy Principles are variations on the Commonwealth APP 3.3 model. (See Appendix C Table 1.) Much of the difference is in the list of grounds that permit the collection of sensitive information without consent, the equivalent of APP 3.4.
- The ACT TPP 3 is very similar to APP 3, with fewer exceptions in TPP 3.4
- NT and Victoria have a special IPP 10 for sensitive information, rather a provision in the main collection principle for PI. These add, as grounds for collecting sensitive information without consent:
    - incapacity to give consent where this is necessary to prevent or lessen serious and imminent threat to life or health;
    - necessary for a legal claim; and
    - necessary for certain research, no practical alternative and not practical to seek consent.
- Queensland only restricts collection of sensitive information by health agencies, although the definition of SI covers the core nine non-health items too. It adds medical history collection as a ground to what is otherwise similar to the NT list.
- Tasmania has a very long list of grounds, in part because it includes more detailed coverage of health privacy and research issues in its general privacy law.

3.8.4 Use and disclosure of sensitive information

APP 6 mentions sensitive information only in the context of the grounds for using or disclosing personal information for a purpose other than the primary one for which it was collected without consent. In particular, the use of SI for a secondary purpose is only permitted where the purpose is one that the individual would reasonably expect and is '*directly* related' to the primary purpose. In contrast, if the information is *not* sensitive, a secondary purpose need only be 'related' to the primary one.

Similarly to Section 3.8.3, the Privacy Principles in different jurisdictions differ in the implications of 'sensitive information' for use and disclosure. The final column 'Use' in Appendix B, Table 2 sets this out.

- NSW, SA and WA have nothing on sensitive information Use and Disclosure Privacy Principles, for the reasons noted above.
- The ACT's TPP 6.2, NT's IPP 2.1, Tasmania's PIPP 2(1) and Victoria's IPP 2.1 closely follow APP 6.
- Queensland's NPP 2(1) is in similar terms, but its application is restricted to health agencies only.

This 'directly related' rule is the main impact on use or disclosure if information is SI. It is rather vague, but it should inhibit secondary uses that divergent significantly from the purpose of collection.

3.8.5 What information is likely to be sensitive

In some contexts, data associated with C-ITS and AVs will be sensitive. For example:

- Image data internal to the vehicle that that captures sexual practices
- Location data that suggests a person is having an affair, visiting a known brothel, attending political meetings, attending particular religious or faith venues, or visiting a particular medical specialist.[33]
- In some jurisdictions, biometric and health data.
- Internal audio recordings of voice communications might in some cases constitute 'sensitive' information, for example where people are discussing political views.

Given the context-dependence of internal image, internal audio and location data becoming sensitive, a prudent default position might be to treat all such data as sensitive.

[33] Anita Ramasastry 'Too Much Sharing in the Sharing Economy? Uber's Use of Our Passenger Data Highlights the Perils of Data Collection via Geolocation', *Verdict* (online), 10 Feb 2015, <https://verdict.justia.com/2015/02/10/much-sharing-sharing-economy>.

4 COLLECTION POWERS

Specific powers for government to collect information in the C-ITS and AV system context are quite narrow, especially in relation to road transport and vehicle related purposes.

Examples include the following:

4.1 Limited powers to collect under road transport laws

Most states and territories have provisions in their road transport laws about the information that is to be collected in the administration of the law. They are sometimes narrow and specific.

For example, s 40W of the *Road Traffic Act 1961* (SA) allows an authorised officer (including government employees when specifically authorised and police) to direct a person having a role or responsibilities associated with road transport to produce a range of information. Such information includes records required to be kept under an Australian road law and records or devices indicating the use, performance or condition of a vehicle. This could potentially capture the provision of C-ITS and AV data, but it is not clear whether it is broad enough to do so. For instance, 'keeping' is a storage type activity, rather than a collection-type activity. A similar provision is contained in s 132 of the *Road Safety Act 1986* (Vic), but only in relation to heavy vehicles.

The *Heavy Vehicle National Law* also contains a range of information-gathering powers (in Division 4 of Part 9.4). For instance s 570C requires a 'responsible person' associated with a particular heavy vehicle to provide location, route, and origin and destination of journeys. This could arguably include requiring an AV or C-ITS system provider to supply location and route information. In particular, 'responsible person' is defined to exclude, for certain speeding offences, those who pack goods or operate weighbridges, but is otherwise undefined. Appendix C discusses the de facto privacy principles embedded in the *Heavy Vehicle National Law*, including clear and robust rules about collection backed up with a $6000 penalty for a breach. The mandatory nature of the collection of information in this scheme is partly offset by strong, and potentially strongly enforced, safeguards against excess.

Passenger Transport Regulation 2007 (NSW) (repealed September 1 2017) was an example of an image collection power which could be applicable in certain transport settings. In Schedule 1 – Approved Security Camera Systems, cl 1 said that an 'authorised purpose' for the cameras includes ss 18 (a)–(d) *Workplace Surveillance Act 2005* (NSW), prosecution of an offence under *Passenger Transport Act 2014* (NSW) or *Crimes Act 1900* (NSW) in or about a bus or taxi cab, compliance with accreditation conditions of driver or operator, or passenger compliance with the subsidised travel scheme in Cl 8 Schedule1 *Transport Administration Act 1988* (NSW). This collection provision could apply to AVs working as 'bus or taxi cab', if equivalent provisions were applied to them. The newer Passenger Transport Regulation 2014 (NSW) does not have this power, but the provision is now found in Passenger Transport (General) Regulation 2017, Schedule 1, which refers to Clauses 82 (3) and 114 (4) (latter repealed).

These road transport collection powers provide modest and limited authorisation for specific types of collection, coupled with in some cases quite strong provisions to protect privacy (under the HVNL). There are many other examples of quite limited or specific powers to collect, although they could potentially cover parts of the information of interest from C-ITS and AV systems.

4.2 Access under the *Telecommunications (Interception and Access) Act 1979*

This Act includes provisions through which some agencies can access the content of telecommunications as well as data about those communications (sometimes loosely called telecommunications metadata).[34] Access to telecommunications metadata such as telephone call and 'communication' records, IP numbers, and account-holder names retained under the Act[35] is permitted without a warrant, except where the data is about a journalist. Interception of communications to access their 'contents or substance' generally requires a warrant or other authorisation. The Act allows the Australian Security Intelligence Organisation (ASIO) to authorise disclosure of intercepted communications content for national security matters, and Commonwealth and state and territory enforcement agencies to authorise disclosure for investigations into criminal offences, offences involving a pecuniary penalty, and for protection of public revenue.

The relevance of these provisions to C-ITS and AV data is unclear. The telecommunications data is held by the telecommunications service entity and would normally be related to communications from a mobile device or fixed line used by a person. In the C-ITS or AV context, the vehicle may have its own telecommunication connection, which may trigger the collection and access provisions. However, some provisions may only apply where the C-ITS is operating to provide a telecommunications service, or is declared.

Many forms of C-ITS or AV data transmitted over networks will not be covered by the legislation. Some data generated in the vehicle may only come under the legislative regime when rendered into another form, for example by speech or biometric recognition or placed into another location, such as the cloud.

There is further discussion about other aspects of telecommunications laws in section 7 below.

4.3 Access to information with a warrant under road and traffic laws

Road transport laws generally authorise searches or access to information with a warrant in some circumstances. By way of example:

- Section 41B of the *Road Traffic Act 1961* (SA) allows an authorised officer to apply to a magistrate for a warrant to enter and search premises if the authorised officer believes, on reasonable grounds, that there may be records, devices or other things at the premises that may provide evidence of an Australian road law offence.
- Section 128 of the *Road Safety Act 1986* (Vic) similarly allows an authorised officer or police officer to apply for a search warrant in relation to premises if there are reasonable grounds that the premises contain evidence of a contravention of a road or transport law.
- Warrant provisions are contained in section 729B of the *Heavy Vehicle National Law*, though these relate to electronic work diary protected information.

[34] The term 'metadata' does not itself appear in the legislation itself. Section 187A(1) refers to 'information of a kind specified in … section 187AA … relating to any communication carried by means of the service.' The service can be that of a telecommunications carrier, internet service provider or an entity declared by the Minister..
[35] Section 187AA TIAA lists 6 'items of information to be kept'.

It is unclear whether such warrants would provide for the collection of C-ITS and AV data or the information derived from it.

4.4 Potential or proposed requirements under the safety assurance system for AVs

The NTC is developing safety criteria against which automated driving system entities will be required to submit a Statement of Compliance. The current draft is contained in the consultation Regulation Impact Statement[36] and includes a criterion relating to data recording and sharing.[37] The criterion proposes placing requirements on automated driving system entities to record and provide certain data to relevant parties. This could include crash data, information on who is in control of a vehicle, and information relevant to liability disputes. The proposed data recording and sharing criterion also requires automated driving system entities to provide information to certain government agencies, including law enforcement. At this stage, a legislative power attached to specific enforcement responsibilities to provide access to the information has been considered but has not been specifically agreed.

It is unclear whether requiring automated driving system entities to provide certain information to enforcement and other government agencies would, in the absence of legislative powers to access the information, be sufficient. However, as noted above, the NTC understands that there may be circumstances where information is provided to government in the absence of specific legislative collection powers.

4.5 Other features of the law enforcement and security collection regime

4.5.1 Exemptions from privacy law

Under the APPs in the *Privacy Act 1988* (Cth), APP entities including private sector organisations may only disclose personal information (including to government) for the particular purpose for which it is collected unless the person consents (APP 6.1(a)) or one of the secondary purpose exceptions applies (APP 6.1(b), referring to 6.2 or 6.3). There are similar provisions in state and territory law such as Queensland IPP 11(1)(b) and (c)-(f); NT IPP 2 (c) and (ca)–(i); and NSW s 18, though in somewhat different terms.

One common secondary purpose exception is where the organisation reasonably believes that the use or disclosure of the information is reasonably necessary for one or more 'enforcement related activities' conducted by, or on behalf of, an 'enforcement body'[38] – see for example APP 6.2(e), Qld IPP 11(1)(e), NT IPP 2(1)(g); NSW s 23. This sort of exception could allow automated driving system entities to provide personal information to police for AV-related enforcement purposes (for example, to determine who was in control of an AV at the time of a breach a road traffic law). However, it would also allow personal information to be provided to police for a range of other law enforcement purposes.

[36] See <http://www.ntc.gov.au/Media/Reports/(C07CE648-0FE8-5EA2-56DF-11520D103320).pdf>.

[37] Note that terms originating from interpersonal relations such as 'sharing' are not usually found in privacy and data protection or law enforcement legislation, which use terms like disclosure, publication, or access for provision of personal information to other parties so as to specify the nature of the transaction or arrangement and avoid implicit characterization in emotive terms.

[38] See Appendix D Table 1 for comparisons of some of the key provisions, such as 'enforcement body'.

4.5.2 Special features of the law enforcement regime

4.5.2.1 Generic law enforcement powers and specific provisions – State laws

Law enforcement entities seeking data generated by C-ITS and AV technology may be able to rely on both general statutory authorisation for law enforcement purposes and specific laws or court authorisation to create exemptions from normal privacy rules in a particular case.

State laws provide generic law enforcement powers to state law enforcement entities. By doing so, they help define the scope of 'enforcement related activities' for the purposes of federal and state law. It is useful to distinguish between general police powers (eg, to enforce road traffic laws) and specific powers to compel information for certain purposes (which are typically not in the generic police legislation).[39] For example, the *Police Act 1990* (NSW) and the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) (LEPARA) do create certain general powers for police,[40] but explicitly separate them from the range of other special NSW statutes which they may be called on to enforce. Below is a subset of those these laws referred to in LEPARA which may have some relevance to the C-ITS and AV system context:

- *Crimes Act 1900*
- *Crimes (Administration of Sentences) Act 1999*
- *Crimes (Forensic Procedures) Act 2000*
- *Criminal Procedure Act 1986*
- *Drug Misuse and Trafficking Act 1985*
- *Essential Services Act 1988*
- *Heavy Vehicle (Adoption of National Law) Act 2013*
- *Heavy Vehicle National Law (NSW)*
- *Law Enforcement and National Security (Assumed Identities) Act 2010*
- *Law Enforcement (Controlled Operations) Act 1997*
- *Police Powers (Vehicles) Act 1998*
- *Road Obstructions (Special Provisions) Act 1979*
- *Road Transport Act 2013*
- *State Emergency and Rescue Management Act 1989*
- *State Emergency Service Act 1989*
- *Surveillance Devices Act 2007*
- *Telecommunications (Interception) (New South Wales) Act 1987*

Here is a subset of the search warrants in other NSW acts supported in s 59(1) LEPARA:

- *Motor Accident Injuries Act 2017* , section 10.29
- *Motor Dealers and Repairers Act 2013* , section 154
- *Passenger Transport Act 1990* , section 46V
- *Point to Point Transport (Taxis and Hire Vehicles) Act 2016* , section 125
- *Road Transport Act 2013* , section 255
- *Roads Act 1993* , section 174
- *Tow Truck Industry Act 1998* , section 83

[39] Both general and specific laws with criminal law enforcement features may contain some powers to compel certain information, although these may be couched in more limited terms in the general law. The more specific laws may have more clearly and narrowly defined powers which go beyond the former.

[40] For instance, s 36(3)(b) of the latter creates a general power to stop and search a vehicle and seize and detain any 'thing' which 'may provide evidence of the commission of a relevant offence'. There may be doubt whether 'thing' includes intangible information, as such powers are often read narrowly.

Some of the laws above are discussed separately in this Report.

As well as the laws covering specific aspects of criminal and other laws, as above, particular bodies may also have specific extra powers to request or receive normally protected information, including those in anti-corruption roles and those operating information surveillance or interchange services for other government bodies. Examples include corruption bodies Independent Commission Against Corruption (ICAC) and Independent Broad-based Anti-corruption Commission (IBAC).

4.5.3 Differing 'uses' – unrelated to basic vehicle operation

Many law enforcement uses of information may be unrelated to the original purpose of collection. To the extent that the 'required by law' and law enforcement purpose exemptions[41] operate to create exceptions to the usual expectations of notification and restriction based on the actual primary purpose of collection, this may comply with privacy law. However, it may create privacy risks and raise consumer concerns, especially if implemented on a mass scale. See the discussion on mass surveillance, below.

4.5.4 Mass surveillance: creation of suspicion v. targeted investigation of suspicious activity

The criminal law prosecution process in Australia depends on investigators obtaining evidence properly, on the basis of 'reasonable suspicion' or 'probable cause', to justify the issue of search warrants or interception orders.[42] Information from blanket mass surveillance, or untargeted bulk investigation, is generally at risk of exclusion as inadmissible in criminal proceedings, although some such information can be used under intelligence gathering and national security operations, typically for the most serious kinds of threat. This is a reflection of the strong traditional legal protections against the practice of 'general warrants' and mass surveillance, which use investigations to generate suspicion where there was none.[43] However, the line between having a standing right to access a bulk data set and targeted access for particular investigations is sometimes unclear. The metadata retention regime in Australia is a modern instance that highlights this tension. The process known as Privacy Impact Assessment (PIA) may assist in understanding the potential implications of the new functionality, both in terms of formal compliance with existing provisions and also of identifying significant areas of concern at the fringes of clear cut legal compliance issues.

A significant unresolved issue is whether the data generated by C-ITS and AV technology could facilitate mass surveillance, since it will be produced in large quantities and some components will be potentially quite revealing. It may thus be seen

[41] For instance, APP 6.2(b) and (e).

[42] This is the process of police investigation of a crime that has been committed in order to provide prosecutors with admissible evidence strong enough for them to be confident they can prove beyond reasonable doubt that a particular person committed all the elements of a particular offence at a particular time and place, so they can then charge the person, prosecute them in court, and succeed in getting a conviction for that offence. Preliminary investigation can make use of potentially inadmissible and unproven allegations in order to create leads and identify suspects, but without stronger grounds these may be insufficient to persuade a court to issue a search warrant or order.

[43] This is paralleled by the traditional reluctance of courts to order open-ended 'fishing expeditions' by litigants seeking to take advantage a court's powers to authorise 'discovery' of information for trial (over-ruling normal expectations of confidentiality, secrecy, privilege or privacy) unless there is already a clear description of what part of the case and to whom the target information refers.

as an opportunity by law enforcement agencies. There is a potential risk that this would allow a greater level of surveillance. To the extent that this develops, it is likely that citizen concerns about this potential will be expressed (as some have already been)[44] and some consumers will avoid these technologies.

4.6 Other bases for collection

There may be other powers relevant to the collection of transport information by government. These include access powers attached to specific enforcement responsibilities, such as the enforcement of road traffic laws. For example, s 25 *Heavy Vehicle (Adoption of National Law) Act 2013* (NSW) authorizes RMS to breach confidences, and creates other legal obligations to disclose and to authorize the disclosure of information.[45]

Other government agencies (such as the Australian Taxation Office) may have powers to compel the provision of information, including personal information. These organisations would not need transport information for transport related purposes, but rather for investigatory purposes (for example, tax evasion investigations). We do not cover the detail around these types of collection powers.

There may be circumstances where compulsory government collection powers do not exist, but third parties still provide the information to government, in effect on a voluntary basis. Examples of such circumstances may include:

- under the telecommunications metadata retention scheme in the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIAA), there are limited categories of data and limited periods of retention, but recent research suggests that telecommunications providers may have new reasons for retaining more data and for longer periods than required. They may also provide it to federal law enforcement and security agencies, even when not required to do so. The data is likely to contain location data.
- under s 313 of the *Telecommunications Act 1997* (Cth), which creates an obligation, discussed further in section 7.2, that leaves open the possibility that a telecommunications entity may see providing certain information is 'doing their best' to prevent the commission of an offence using the network.
- when witnesses, whistle-blowers or infrastructure providers are not obliged to report or provide information to a person who is authorised to collect it, but choose to do so, such as in respect of traffic incidents. To the extent that AVs are involved in such incidents this may become common.

[44] See for instance the recent discussion of global developments in Neil McBride, 'Driverless cars offer new forms of control – no wonder governments are keen', *The Conversation*, 21 June 2018 <https://theconversation.com/driverless-cars-offer-new-forms-of-control-no-wonder-governments-are-keen-98585>. 'There's a reason why governments are so keen on driverless cars – and it's not just because of the potential economic benefits. They offer the chance for even greater tracking and even control of citizens' every move. Far from setting us free, driverless cars threaten to help enable new forms of surveillance and oppression. … In reflecting on the ethics of driverless cars we need to move beyond the constraints of trolleys and levers to a wider agenda that addresses the concepts of autonomy, community, transparency, identity, value and empathy.'

[45] See *Heavy Vehicle National Law (NSW)* No 42a, which the above law implements.

5 MAPPING PRIVACY PROTECTIONS ONTO C-ITS AND AV DATA ACTIVITIES

A number of stakeholders refer to who 'owns' the data.[46] Ownership is however not necessarily a helpful term to use in the context of C-ITS and AV data. You can own a hard disk, but this will not give you untrammelled rights to use PI or copyrighted material in its files. Instead, it is more helpful to use privacy law concepts and ask which entity collects, uses, accesses, holds, or discloses certain information. This section explores those terms.

5.1 'Collection'

5.1.1 What does 'collection' cover?

The concept of collection covers direct collection from the individual, whether by soliciting or not, and indirect collection of information 'about the individual' from third parties. Collection of C-ITS and AV data by government may be done indirectly via the automated driving system entity or telecommunications provider or it may be done directly through roadside devices such as C-ITS receivers.

Privacy principles focus on collection as a key point of control and treat the purpose of collection and whether it is necessary for the collecting entity's functions or activities as critical factors. There are variations of how closely connected the purpose has to be to the function. The purpose of collection is also relevant to what uses and disclosures are permissible.

APP 3 distinguishes between the information for collection being 'directly related' and being merely 'related' to the functions or activities. It requires that 'organisations' only collect if it is reasonably necessary for the functions or activities, while 'agencies' can in addition base the justification on necessity for other purposes 'directly related' to the functions or activities, not just the functions themselves:

> **APP 3 – collection of solicited personal information**
>
> **Personal information other than sensitive information**
>
> 3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.
>
> 3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

5.1.2 Primary and secondary collection by a government agency

An agency is the primary collector of information where it collects it itself. For example, government-owned infrastructure may collect data direct from vehicles. In the context

[46] This idea of 'owning' personal information has been popularised by commercial exploitation of such information in jurisdictions like the US, which have limited data privacy rights for individuals and an emphasis on exploitation of personal data as an 'asset'. Ownership is not the appropriate way of understanding relationships of entities with information, since information does not behave like other forms of property. In particular, privacy law emphasizes not 'ownership' but primary human interests of the data subject protected by international treaties (such as the 1966 International Covenant on Civil and Political Rights) and human rights and civil liberties law. It relies on a range of explicit and implicit concepts, including dignity, autonomy, control, consent, necessity and authorisation, that cannot be understood using the language of 'ownership'.

of C-ITS messages, collection by government owned roadside devices may constitute direct collection from the individual where that individual is in effective control of the vehicle and aware that collection was occurring.

Primary collection is typically broader than secondary collection – such as later collection of information already collected from an entity or agency by law enforcement. In some circumstances, law enforcement agencies will conduct primary collection, for example from roadside speed cameras or licence plate detectors. The purpose of collection needs to be clearly stated.

Where an agency collects data itself, it will need to comply with rules around collection in the relevant privacy law. If proposed collection is to be secondary, from another party who already has the information, there may be non-compliance with APP 3.6, which creates a presumption in favour of collecting directly from the individual.[47]

> 3.6 An APP entity must collect personal information about an individual only from the individual unless:
>
> (a) if the entity is an agency:
>
> (i) the individual consents to the collection of the information from someone other than the individual; or
>
> (ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or
>
> (b) it is unreasonable or impracticable to do so.

The 'unreasonable or impracticable' exception appears broad, although the recent case of *Waters v TFNSW* rejected a claimed justification for a collection process that was supposed to be reasonably necessary for a purpose of the entity. This may have increased the level of sceptical scrutiny one could expect about claims of 'unreasonable or impractical' but 'necessary to collect'. Where C-ITS and particularly AV data is collected by the ADSE and not the individual, the individual will not themselves have access to the data. This may be considered 'unreasonable or impractical', since the individual cannot in practice provide it. If collecting the data is indeed necessary, secondary collection with thus most likely not conflict with the obligation in APP 3.6 or state and territory equivalents.

5.1.3 Notification of the purpose of collection; change of purpose

A key element of the Privacy Principles model is the obligation of a collecting entity who is covered by obligations, such as an agency (Qld), public sector agency (NSW) or

[47] This assumes the collector is a federal agency, or a substantial business. Much roadside infrastructure will be state and territory owned, so reader should also refer to the equivalent IPP, such as TPP 3 in the ACT, s 9 of the NSW act and IPP 3 from Qld. See Appendix C. Table 1 to see the variation between jurisdictions. For example APP 3.6 says 'an APP entity must collect personal information about an individual only from the individual unless:
(a) if the entity is an agency:
(i) the individual consents to the collection of the information from someone other than the individual; or
(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or (b) it is unreasonable or impracticable to do so.'
NSW IPPs s 9 has the basic consent alternative but omits APP 3(a)(ii) (by law) and (b) (unreasonable), and adds to the generic consent provision another one applying to consent from the parents or guardians of a minor. Qld IPP 3 merely requires the agency to take account of (3) 'the extent to which personal information is collected from the individual the subject of it, and the way personal information is collected, are not an unreasonable intrusion into the personal affairs of the individual.'

organisation (NT), or an APP entity,[48] to notify individuals affected of 'the purposes for which the entity collects, holds, uses and discloses personal information', or to make them aware of these purposes.[49] This original purpose is important as it will influence obligations in relation to later use and disclosure. This notification is done via the IPP or APP Privacy Policy that affected entities must provide, for APP 1.4(c), and often more directly for APP 5.2(d).

Issue about collection, and notification about the purpose of collection, that may be relevant for a changing environment like CITS and AV systems include:

- What happens if and when the use to be made of the data, in effect the purpose for collection, changes?
- How does an APP entity notify data subjects about 'secondary uses'?
- If collection is indirect, is there an obligation to ensure the collecting entity notifies the subject of the secondary collection?

For government collecting C-ITS information by government-owned roadside devices, the proper channel for notification may need some thought. Notification at each collection point may be impractical, although responsive data system could hold the information for queries by vehicles using them. An alternative may be provision of notification information during a registration or licencing process, although this is remote from the actual context and time of collection.

5.1.4 Which data items?

Collection covers all the items in section 2.2 above.

See also the discussion in section 3.8 of the further constraints on collection of information if it falls into the categories under 'sensitive information about an individual' in a particular jurisdiction.[50]

5.1.5 When collected? Where?

Information collected directly via devices will typically be captured in real time, though it may not be accessed or used until later, having being 'held' or stored in a device for batch transmission.

Information collection indirectly from third parties may occur in real time, if there is some feed through arrangement, or later.

5.2 'Use' by government

The concept of use of personal information (and sensitive information[51]) is central to the Privacy Principles model.

[48] See sections 6, 6C and 6F of the *Privacy Act 1988* (Cth). For our purposes government related APP entities include 'agencies' and 'organisations', covering most federal bodies and their contractors, and those state and territory authorities and instrumentalities that have been prescribed at the request of the relevant jurisdiction.
[49] Australian Privacy Principle (APP) 1.4(c) and APP 5.2(d) Notification of the collection of personal information, in *Privacy Act 1988* (Cth) Schedule 1. See also the various IPPs in state and territory laws, which may be more relevant for collection by state agencies than the APPs would. For instance s 10 of the NSW IPPs requires notification too, as does the ACT TPP 5, IPP 1.3 in NT, Qld IPP 2(3), SA IPP(2), Tas PIPP 1(3), and Vic IPP 1.3. The notification provisions are broadly similar, though they require less detail about secondary recipients.
[50] Appendix B Table 2 provides further details.

5.2.1 What does 'use' cover

Use covers several categories, the first two of which may be readily permissible, with some constraints, while the third may be often impermissible:

- direct or primary use, namely the one which was notified to the subject as the purpose for which the information was collected
- secondary use, which is not the primary use but is related to it (the degree of relationship can be ambiguous)
- uses quite unrelated to the original purpose of collection

With C-ITS and AV data, the primary use will often be merely to enable the effective and safe operation of the vehicle.

There may also be some types of data which are not collected for this purpose but for other related purposes, including ensuring compliance with regulatory or other requirements secondary to the basic operation of the vehicle. This is more likely to include roadside and in-cabin contexts than the core control of the vehicle. Compliance with sleeping periods and speed limits in the heavy vehicle context may be examples. More specific collection for cognitive monitoring for alertness, consciousness, drug consumption or other factors that could influence the capacity of a driver to take control of an AV may be considered. Alternatively, in car microphones may be primarily used for making voice calls, but there could be interest in using the data for other purposes.

Some jurisdictions[52] treat disclosure to another party as a use, or in very similar terms, while others keep a clear distinction so that a disclosure of PI is not a 'use' of it.[53]

In jurisdictions where disclosure is a use, non-specific use rules may inadvertently also permit broad disclosures to third parties inconsistent with the spirit of privacy law, which is to treat disclosure as a significant point where control needs to be exercised. For instance, Qld IPP 10(1) allows use where '(e) the other purpose is directly related to the purpose for which the information was obtained' while IPP 11 has no such 'directly related' exception for disclosure. By contrast NT's IPP 2(1)(a) and (b) accept a 'directly related' exception for disclosure.

5.2.2 Methods for authorising use

If a state or territory public sector agency or a federal agency has collected information under the IPPs (Information Privacy Principles) or APPs, it may only use or disclose it (NSW, Qld and SA IPPs refer to 'use' not 'use or disclose'),[54] for the purpose for which it was collected. Its use or disclosure for secondary purposes is restricted, though in practice the restrictions have exceptions substantial enough to permit a wide range of such uses. Exceptions to the restriction vary across the states and territories, but all include (with the exception of WA):

- with the [informed] consent of the individual;

---

[51] See Section 3.8 and Appendix B Table 2. As noted there, the main effect of being 'sensitive information' is that be default permissible secondary uses are those which are 'directly related', not merely 'related' to the primary purpose of the collection.

[52] For instance, NT IPP2 'Use and disclosure'.

[53] For instance. Queensland IPP 10, Limits on Use and IPP 11, limits on disclosure.

[54] See for instance Queensland IPP 10. 'Limits on Use of Personal information'.

- to prevent or lessen a serious threat to the life, health, safety or welfare of an individual or the public;
- as authorised under another law [or court or tribunal order];
- for law enforcement purposes.

This would for instance likely allow

- in-cabin video recordings collected by police for AV-related enforcement purposes to be used for secondary law enforcement purposes.
- location information collected by government (including any location information revealed from messages broadcast through C-ITS or related services) to be disclosed for law enforcement purposes.

5.2.3 Which parties 'use' the data, for what purpose? Change of use

The entity that collects the data is typically the first entity to use it. When it is disclosed to another party, privacy law requires consideration of the relationship between its proposed use and the purpose for which it was collected. Where the recipient third party, who may be government, 'uses' it for a purpose other than that for which it was collected or a related secondary purpose, it may be necessary to examine the basis by which this other use was authorised.

Where the use to which the data will be put changes after collection, there is a question about whether the data subject needs to be notified of this change (if they were never put on notice of this originally). This will depend on the relationship between the new use and those originally disclosed.

This has recently become controversial in a recent case where PI about an individual was disclosed by a ministerial office. In that case, it was justified on the basis that the data subject should have 'reasonably expected' a use apparently unrelated the original statutory purpose when they chose to publicly critique the operations of the relevant government program.[55] A similar controversy could arise in the context of C-ITS and AV systems, there is potential for similar controversies. If 'reasonably expected' is used frequently as a basis for claiming changed use (especially if it is contrary to the interests of the subject), then what might be expected by individuals will continue to expand. Privacy is thus reduced through a 'ratchet effect' – lax practice becomes the new legal standard. Even if such a ratchet effect is permissible in law, controversy surrounding reliance on this principle may lead to consumer distrust.

[55] APP 6.2(a) applies 'in relation to the use or disclosure of personal information about an individual if: (a) the individual *would reasonably expect* the APP entity to use or *disclose* the information for the secondary purpose and the secondary purpose is: (i) if the information is sensitive information -- *directly* related to the primary purpose; or (ii) if the information is not sensitive information -- related to the primary purpose'. (emphasis added). See Acting Privacy Commissioner Angelene Falk, 'Concluding statement — Centrelink release of personal information,' OAIC, 29 May 2018 <https://www.oaic.gov.au/media-and-speeches/statements/centrelink-debt-recovery-system - concluding-statement-centrelink-release-of-personal-information>; reported in F. Duxfield and S. Smiley, 'Privacy decision sets worrying precedent for what the Government can reveal about us,' ABC online, 31 May 2018 <http://www.abc.net.au/news/2018-05-31/privacy-precedent-what-can-the-government-reveal-about-us/9816700>.

5.3 'Disclosure'

5.3.1 What does 'disclosure' cover?

Disclosure is the act of an entity that holds personal information providing it in some way to another party. This may be by:

- providing access to it directly
- transferring the master copy or diverting the data feed
- making a copy and transferring it or duplicating the data feed
- enabling remote querying of the data so that a third party can use it for some purposes, in whole or in part, without a human intermediary

5.3.2 Disclosure to whom/which parties

For our purposes, the most relevant disclosures in the C-ITS and AV system environment include:

- disclosure by government to another government agency (e.g. road agency to police)
- disclosure by a third party commercial entity to government
- disclosure by government to a commercial entity (e.g. to an ADSE for a necessary purpose)
- disclosure by government to a foreign entity, including a contractor or service provider

5.3.3 Methods for authorising disclosure

Disclosure of personal information by the private sector or government can be done legally using a number of methods. Under the Privacy Principles model, such as in APP 6.1 and 6.2 or Queensland IPP 11, these justifications include where such a disclosure is:

- necessary to achieve for the primary purpose of collection of PI or for a related purpose
- necessary to achieve the primary purpose of collection of SI or for a directly related purpose (in those jurisdictions where this category is used)[56]
- 'required or authorised by law' (including under laws of interest here such as transport, telecommunications and criminal laws)
- necessary for certain protective actions, such as in relation to serious imminent threats to life or health
- subject to 'informed consent' by the subject[57]
- based on a claim that the data subject would have 'reasonably expected' the disclosure, as noted above[58]

[56] This exception may not apply if disclosure is a disclosure, not a form of use.
[57] While often legal, relying on consent can be controversial where consent is bundled with other services.
[58] Falk, ibid..

There are potential concerns and practical implications if a private sector entity acting as ADSE is not covered by the APPs (i.e. because it is an exempt 'small business' due to turnover under a $3 million threshold).[59]

5.3.4 Disclosure from one jurisdiction to another country

This process includes disclosure by foreign third parties to government (i.e. by a foreign-based AV entity), by government to a foreign government (perhaps for intelligence or security purposes), or by government to a foreign third party (eg for processing or other services). It is also known as 'trans-border data flow' and may be subject to special controls. Provisions of the other country's law, our relevant local law, and any rules about cross border data transfer itself may be triggered. The European GDPR, discussed may thus be directly applicable to some Australian government and corporate uses of information, as discussed in Section 8.1.1.

5.3.5 Collection, use and disclosure in road transport laws

Most (but not all) states and territories have provisions in their road transport laws about the confidentiality of information gathered in the administration of the law. These provisions typically govern the use and disclosure of this information to other government agencies and third parties. This information is primarily vehicle registration and driver licensing information.[60] In some cases confidentiality might also extend to certain driver diaries and monitoring.

Many states and territories make unauthorised use or disclosure of information gathered in the administration of the road transport laws an offence.[61]

The provisions are unlikely to cover C-ITS and AV data, unless this data is used for one of the monitoring purposes (such as those in HVNL, or other safety schemes), not the core registration and licensing purpose.

5.4 Holding, storage, retention

This activity, keeping an item of information for a period of time, is described in various regulatory settings using terms such as store, record, hold, keep, retain, or archive. Generally speaking, these terms have a similar meaning.

'Retention' is typically used in the telecommunications sector to cover keeping traffic data or metadata much longer than it might otherwise be held for operational purposes. The alternative to a requirement to retain is a discretion for an agency or entity to choose voluntarily to retain. Relying on voluntary compliance raises similar privacy risks to enactment as a requirement. Indeed, it could result in data being retained for longer than the minimum requirements specified in legislation.

Archives legislation[62] requires government departments and agencies to retain information in certain sorts of records for defined periods and, often, to destroy them if not needed after that period. The degree to which C-ITS or AV system data held by government will be subject to archiving obligations is outside scope for this report.

---

[59] S 6D *Privacy Act 1988* (Cth).

[60] See, for example, *Road Safety Act 1986* (Vic) s 90J(1).

[61] *Road Transport Act 2013* (NSW) s 101; *Transport Operations (Road Use Management) Act 1995* (Qld) s 143; *Motor Vehicles Act 1959* (SA) s 139D, *Road Safety Act 1986* (Vic) s 90Q, *Road Traffic (Administration) Act 2008* (WA) s 143A.

[62] Such as *Archives Act 1983* (Cth), *Territory Records Act 2002* (ACT), *State Records Act 1998* (NSW), *Public Records Act 2002* (Qld), *State Records Act 1997* (SA), *Archives Act 1983* (Tas). *Public Records Act 1973* (Vic)

Government departments may need to comply with archiving laws in the same way as they do for other data sets they hold.

5.5 'Deletion' or de-identification of personal data

There may be requirements to delete or destroy information after a period of time, either under a privacy law or under another law. There can be requirements to de-identify, either in addition to or as an alternative to a requirement to delete or destroy. These are linked in some jurisdictions i.e. requirement to 'destroy *or* de-identify'.[63] There are different methods to do this, from simply omitting a reference in a table of contents, through time-consuming multiple over-writing of storage locations, to physically destroying storage media on which data was held. The effectiveness of particular methods is not always clear. There may be other ways of authorising or requiring de-identification, including the rules for use of data in research and experiments. In some circumstances, data cannot be disclosed or published unless it is de-identified.

Deletion and de-identification obligations apply to those holding the data, or those proposing to use it for eg, research, or for publication. There are other circumstances where de-identification is required, including where information is used for research purposes, where it is selectively released under FOI, and where it is proposed for release as 'open data'.[64] There are also similar requirements in archives legislation.

'No further use': There are provisions in archiving laws which require deletion when there is 'no further use' for data.

Informal obligations or promises: Some data holders make assurances that data can be deleted on request. These may be hard to enforce or require.

Spent convictions: There are provisions which allow or require certain minor convictions not to be revealed. While many of these may refer to traffic offences, it seems unlikely there is direct relevance to C-ITS and AV data sources.[65]

5.6 Rights or entitlements of data subjects

5.6.1 Notification of purpose of collection

As noted above in section 5.1.3, data subjects have the right to be notified about the purpose of collection of their PI. This can be in a privacy policy, in a more specific notification, or provided as the basis for 'informed consent'. The framing of the notice or information may need to address the following issues:

- The fact of collection and the purpose of collection, use or disclosure[66]
- Uses will typically be required to be notified.
- Depending on whether a 'disclosure' is a 'use' or an activity of its own, disclosures may need to be separately notified.

[63] Eg APP 11.2, which is similar to the ACT. Victoria, Tasmania and NT include 'deletion' as part of correction in IPP 6, and as destroy or permanently de-identify in a separate principle in IPP 4.2 about data security. NSW has an obligation to no longer retained and disposed of securely after necessary, in s 12. Queensland does not seem have a provision of this type in the main IPPs, but in NPP de-identification fills the role of destruction in other security principles.

[64] See for instance the Open Data Charter, <https://blog.data.gov.au/news-media/blog/australia-adopts-international-open-data-charter>.

[65] For instance, *Crimes Act 1914* (Cth) s 85ZM.

[66] Eg, *Privacy Act 1988* (Cth) APP 5.

- Few provisions are specific about rights in relation to changes in purpose or planned use of the information. This creates potential ambiguity about the degree to which a subject will be notified of such changes.[67]
- It is less common to be notified about deletion arrangements.

5.6.2 Informed Consent

5.6.2.1 Nature of information/disclosure required to be given

There is considerable ambiguity about the level of specificity, extent and clarity of information required to establish that a consent is 'informed'. Where vague and general information is offered, particularly in relation to the identity of third parties who may get access to the information, consent may not be properly 'informed'. However, in Australia, many privacy policies remain vague.

Consent may also be sought for a wide range of collections, uses or disclosures which are not essential to the provision of a particular service. In some circumstances, the subject may have little practical choice but to consent. For instance, the operators of various systems in the C-ITS or AV environment may insist on consent for a wide range of data uses as a condition for access to a vehicle's software. There may come to be limited alternatives, particularly for users who are unable to use alternative travel services, for example as a result of poverty of disability.

5.6.2.2 Role of consent

Where a particular use or disclosure is otherwise not permitted due to operation of the relevant privacy law, specific consent may be sought in order to facilitate that use.

5.6.3 Information quality and data integrity

Some privacy laws require data integrity or quality of personal information to be protected. For instance, APP 10 says:

> 10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is **accurate, up-to-date and complete**.
>
> 10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, **having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant**. (emphasis added)

In C-ITS and AV systems, information may either be extremely current in a stream or potentially quite dated if retained as a snapshot. Data may also not be 'complete' in that it is not a full data set from all sensors. It is unclear how these requirements would be interpreted in the context, for example, of a system that only stores data in response to particular stimuli (such as a crash or incident). On the other hand, if *all* data is collected and retained, the relevance test may not be satisfied, since there may be excessive noise resulting in a loss of utility.

5.6.4 Complaint pathways and remedies

Complaint to regulator: Unless the activity or the entity is exempt, the subject may complain to the regulator about the activities of data host entities.

[67] See also section 5.2.3 above.

Complaint to law enforcement: There may be law enforcement oversight bodies to which a subject is entitled to complain where data is accessed or used by law enforcement. This assumes, of course, that the individual concerned is aware of the relevant access or use.

Legal action: In Australia, there is no established basis for a legal action for a breach of privacy, although there may be other, more marginal types of legal action that could be commenced. Arguably, the absence of a self-help litigation option puts a higher ethical obligation on system designers to protect the interests of data subjects.

Correction: There may also some be FOI style correction or annotation rights, such as seen in APP 13. Health record privacy principles include detailed correction provisions, but biological data collected in the C-ITS and AV context is unlikely to count as such a record.

6 SURVEILLANCE DEVICES

The relevance of surveillance device laws is their role in the collection of information.

Surveillance device laws, found in all Australian jurisdictions, provide criminal offences for the unauthorised use of up to four categories of device:

1. listening devices (some laws only cover this)
2. optical surveillance devices
3. tracking devices
4. data surveillance devices[68]

The laws prohibit installation or operation of surveillance devices except in certain circumstances, generally if there is authorisation in the form of a warrant or consent for the purposes of law enforcement or criminal investigation.[69] They also prohibit communicating or publishing certain information, including information derived from the surveillance device, and also information about the use of the device which may reveal confidential operations and methods of law enforcement and security services using such devices.

Surveillance device laws protect privacy by creating offences for these unauthorised acts, and a strict environment of authorisation, warrants, documentation and oversight. They are designed to inhibit and suppress both installation and use of the devices as well as the use or disclosure of the information they generate unless it is done within the limited criminal law enforcement context in which they are designed to be used. They create a strong impediment to using relevant or using information derived from them outside a criminal law enforcement context. Unlike general privacy laws, surveillance device laws do not permit many secondary uses without consent or allow collection for purposes that are not expressly permitted.

There is some inconsistency between the laws in the different jurisdictions with respect to the types of devices regulated, and the scope of the offences, defences and exceptions. This inconsistency may result in increased uncertainty and compliance burdens for organisations operating at a national level as well as lack of clarity in the protection afforded individuals.[70] These inconsistencies are discussed in more detail in section 6.1.

There are strict controls on use and disclosure of the data collected from a surveillance device and information about each operation.

The applicability of surveillance devices laws is discussed further in section 6.2.

6.1 Diverse state-based laws – comparison

There is commonality in covering one or more of the four device types, although some older laws only cover listening devices, and only the newer ones cover data surveillance devices. See the extensive table in Appendix E for details. The definitions of the devices are generally very similar, and quite broad. Typical definitions, and how they apply, are shown in the Table below.

[68] Appendix E Table 2 has text of each legislation's definitions, and extensive examples. See also 'Legal Guide to Surveillance Legislation' in each jurisdiction on SmartSafe.org.au for readable summaries of their general effect.
[69] *Surveillance Devices Act 2004* (Cth); *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act* (NT); *Invasion of Privacy Act 1971* (Qld); *Surveillance Devices Act 2016* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA).
[70] See *Serious Invasions of Privacy in the Digital Era* (DP 80), ALRC 2014, '13. Surveillance Devices', [13.3]

Table – The four surveillance device types, and where they appear

Device	Jurisdiction
"***listening device***" means any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing […].	All
"*optical surveillance device*" means any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight […].	Not in ACT,** Qld or Tasmania
"***tracking device***" means any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object.	Not in ACT,** Qld or Tasmania
"***data surveillance device***" means any device or program* capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device.	Not in ACT,** Qld, Tasmania or WA

***** 'Program' is omitted in NT data surveillance device definition.
** Only listening devices are covered in the *Listening devices Act 1992* (ACT). All devices are covered in *Crimes (Surveillance Devices) Act* 2010 (ACT), but as in *Surveillance Devices Act* (Cth), unauthorised use is not prohibited.

This group of laws generally create offences prohibiting the installation or use of surveillance devices without authority, and contemplate authorised use only by law enforcement with a warrant or specific authorisation by senior officers in the jurisdiction unless certain conditions are met.[71]

There are also special purpose laws, including the NSW *Workplace Surveillance Act 2005*, which covers the workplace and treats devices slightly differently.

NSW, the NT, SA and Victoria have laws specifically relevant to vehicles, namely a prohibition on tracking devices. It is not permitted to install, use or maintain these devices without authorisation. There are minor variations in the elements of the offence for each type of device: s 6 listening, s 7 optical, s 8 tracking, and s 9 data (Victorian provisions). For example:

> **S 8 Regulation of Installation, use and maintenance of tracking devices**
>
> (1) Subject to subsection (2), a person must not knowingly install, use or maintain a tracking device to determine the geographical location of a person or an object—
>
> (a) in the case of a device to determine the location of a person, without the express or implied consent of that person; or

[71] *Surveillance Devices Act* (Cth) addresses only authorisation of use of surveillance devices by law enforcement officers. It does not contain offences prohibiting unauthorised use generally. Unauthorised use of a device is presumably thus only covered by the state or territory law which applies where the activity occurs, for whatever devices it covers. The Commonwealth law however, in common with other jurisdictions, does prohibit unauthorised use, communication or publication of 'protected information' from or about use of a surveillance device by law enforcement. *Crimes (Surveillance Devices) Act* 2010 (ACT) covers all four devices but also prohibits only these dealings with 'protected content', not unauthorised use of devices. *Listening devices Act 1992* (ACT) does prohibit unauthorised use of devices, but only for listening devices.

(b) in the case of a device to determine the location of an object, without the express or implied consent of a person in lawful possession or having lawful control of that object.

(2) Subsection (1) does not apply to—

(a) the installation, use or maintenance of a tracking device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or

(aa) the installation, use or maintenance of a tracking device in accordance with a detention order or supervision order or an interim order under the *Serious Sex Offenders (Detention and Supervision) Act 2009*; or

(ab) the installation, use or maintenance of a tracking device in accordance with a parole order under the *Corrections Act 1986*; or

(ac) the installation, use or maintenance of an electronic monitoring device in accordance with a community correction order under the *Sentencing Act 1991*; or

(ad) the installation, use or maintenance of a tracking device in accordance with an order of the Governor of a prison under section 30 of the *Corrections Act 1986* ; or

(b) the installation, use or maintenance of a tracking device in accordance with a law of the Commonwealth.

In the absence of consent, a warrant, an authorisation, an order, or a statutory power, the collection and installation of a device of this nature will be an offence in those jurisdictions.

Referencing the Victorian provisions, there are also other offences for:

- use of optical or listening devices by employer: s 9B.[72]
- unauthorised use, communication or publication of 'protected information', or information permitted to be observed, or information from the surveillance: ss 9C, 11, 30D.
- exposure of 'technologies and methods', s 30I.

There are exceptions to the prohibition on unauthorised use in relation to content for material already in the public domain, prevention of serious harm to persons or property, activities prejudicial to national security, and assistance to a foreign law enforcement.

This model is replicated for each device in most of the variations of these laws.

6.2 Devices affected

C-ITS and AV devices could potentially be optical surveillance devices, listening devices, data surveillance devices or tracking devices. For example:

- devices such as in-cabin cameras, microphones or biological or health sensors could potentially be optical surveillance devices, listening devices, or data surveillance devices depending on their data profile
- sensors generating other C-ITS and AV system data, such as external audio and image sensors and some of the operational sensors [Lidar and other ADAS sensors, location and route detectors, and perhaps EDR] could potentially be

[72] This is an example of a workplace-specific provision. In NSW there is a separate act for this, as noted above.

caught as tracking devices, listening devices, data surveillance devices or optical surveillance devices.

The vehicle system operator or ADSE would often be the entity doing the surveillance and they may be asked to provide the data to government. If they were carrying out unauthorised surveillance, the legality of the original collection may be in doubt. This would firstly open the operator to further offences of communicating or publishing information from the device. Secondly, government collection of this information might contravene privacy principles concerning fair or lawful collection.

Government roadside devices could potentially be surveillance devices that fall within these laws. For example:

- Bluetooth receivers could potentially be a data surveillance device or tracking device.
- ANPR is likely to constitute an optical surveillance device or tracking device.
- Messages broadcast through C-ITS could be captured by roadside beacons or infrastructure (such as traffic lights). Such beacons or infrastructure could perhaps be 'tracking devices' or 'data surveillance devices', although as mentioned in the note below, ALRC saw many gaps in coverage of wireless devices which could be used for surveillance.

Enforcement agencies contemplated in the legislation may be able to access, use or communicate the information derived from certain 'surveillance devices' lawfully with a warrant or specific authorisation, but other agencies may be prevented from doing so. Access to such 'protected information' from surveillance devices is heavily restricted, as its loosely controlled circulation is considered potentially dangerous.

6.3 The obligations – to whom do they apply

The operator of the surveillance device would be the party primarily covered by the prohibition on installation and use. This could be private parties or, less frequently, government agencies who operate C-ITS or AV infrastructure.

The prohibition on using, communicating or publishing data without authorisation would, if triggered, prevent the (usually private) collector from lawfully making the data available to others, such as government.

In most cases, unlike with telecommunications interception and data retention laws, the surveillance device powers do not impose obligations on or require the sort of cooperation of other parties that would apply to say carriers or ISPs who do the primary collection while operating telecommunications infrastructure. The surveillance device laws are framed to empower direct use of discrete information collection devices by police or law enforcement under the authority of an 'appropriate authorising officer'[73] or court warrant.[74] Others who are not the law enforcement officers contemplated, or who do not have the necessary authorisation or warrant, risk contravention of prohibitions on using the devices or dealing with the information.

[73] Typically chief, deputy chief, or superintendent or SES level senior officer – eg, s 6A(6) of the NSW act.
[74] A warrant is more likely to be needed if trespass, entry of premises without permission or 'interference without permission of a vehicle or thing' are necessary for installation or retrieval.

6.4 Relevant omissions

One issue with the legislation is its focus on 'device'. *R v Gittany (No 5)* [2014] NSWSC 49, discussed in Appendix A, is an example of use of software to convert general purpose hardware (in that case a person's smartphone) so another entity can use it to conduct surveillance, but this may fall outside some current surveillance device laws.[75] A less technology-specific formulation (not tied to a 'device' designed for surveillance) has been proposed as a law reform objective to reduce this problem.[76] This drafting is relevant to C-ITS and AVs because whether a particular C-ITS or AV system data feature is covered by surveillance device laws may depend on how it is implemented, not its functionality. For instance, tracking carried out without installing what would be a 'tracking device', using data manipulation from sources not initially installed to do tracking or data surveillance, may also not be covered. Similarly, it is uncertain how capture of video from devices not installed as surveillance devices would be treated.

6.5 Implications

What are the implications for government collection and use of C-ITS and AV data if C-ITS and AV technology generally, and government roadside devices collecting information from passing vehicles, come under this regime?

The first question is whether a given device or sensor system fits the existing categories in particular surveillance laws. Many C-ITS and AV devices may not fit the definitions, or only marginally. Some devices are more likely to fit, including those collecting data equivalent to listening devices, tracking devices or optical surveillance devices. See Appendix E Table 2.

While the focus here is on the device, not the data, the data's intended use and purpose may influence how the device is characterised. If a device is not installed for a surveillance purpose (for a tracking device, the relevant purpose is to determine geographical location of a person or thing; for a listening device, to listen to a private conversation; for an optical device, to observe a person, place or activity including in a vehicle; for a data device, to record or monitor input or output of a computer), but rather to monitor safety or to assist with network efficiency, this may sometimes affect its characterisation as a surveillance device. However, the ultimate motive or intent for doing one of the prohibited surveillance device acts is not an element of the offence, so 'good intentions' (network efficiency or safety) may not have major role in whether to characterise the use of a device as contravening the prohibition. As with any criminal offence, close attention to the precise elements of each specific offence in a particular jurisdiction is essential. Acontextual generalisations are of limited use.

If a given device fits within the existing categories in terms of its functional purpose (to determine the location of a person or thing, to observe an activity in a vehicle or premises, to hear a private conversation, to monitor data to or from a computer), the

[75] Some jurisdictions have a 'data surveillance device' category with a definition that includes 'program' as well as 'device'. This excludes NT (which does not include 'program') and ACT, Queensland, Tasmania and WA (which do not have a 'data' device category). In the other jurisdictions, functionality of a general purpose device caused by a surreptitious software 'program' may be covered by 'data surveillance device', but query if this extends beyond causing it to monitor 'information being put on or retrieved from a computer'.

[76] ALRC discusses the software issue above, other inconsistencies such as potential omission of WiFi and RFID interception from either surveillance devices or telecommunications law, and technological neutrality generally, in ALRC, *Serious Invasions of Privacy in the Digital Era* (DP 80), 2014, Ch 13 'Surveillance Devices', [13.13]–[13.29]. For a summary of their recommendations see *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123), 2014, Ch 14 'Surveillance Devices'. These include enacting a Commonwealth Act to replace the existing state and territory laws, and making the scope of devices covered more technologically neutral.

operators of certain such devices could potentially contravene surveillance device laws unless they are law enforcement officers who have the necessary warrants for criminal investigation purposes, they have consent from the subjects of surveillance, or they have the benefit of an exemption.[77]

The question of informed consent would need close attention, because the consent might effectively be for a law enforcement purpose of the collection. The extent to which the 'surveillance device' use is disclosed to all subjects would need to be sufficient to put each data subject, including occupants other than the person in control of the vehicle, on notice about what the device does and what the implications are.

Where certain warrants or consent are in place, with arrangements monitored and reported to senior police, the activities will not be an offence, but there may be many C-ITS or AV system data practices which will not be carried out under a warrant. The schemes do not seem to contemplate bulk exemptions for mass surveillance or non-targeted surveillance, or for the operation of the various devices by persons other than law enforcement.

The inconsistency between the different jurisdictions is probably less than with some of the other types of legislation we cover in this report. The main variant of interest is that in some states, certain devices are not covered – see Table in Section 6.1 above.

[77] See for instance, s 37 *Surveillance Devices Act 2004* (Cth) permits federal and state law enforcement to use optical surveillance devices without a warrant if it does not involve (a) entry onto premises without permission; or (b) interference without permission with any vehicle or thing.

7 TELECOMMUNICATIONS

7.1 Role of entities in relation to the carriage service system

C-ITS and AV systems will need to be closely integrated into telecommunications systems. In some cases, communications services to either road infrastructure or vehicle operators will be delivered by independent telecommunications entities. In others, the infrastructure or vehicle operators may themselves act as a telecommunications entity. In particular, ADSEs or C-ITS manufacturers may themselves be relevant entities under telecommunications legislation in the future.

The relevant entities under telecommunications legislation are carriers, carriage service providers (CSPs) and carriage service intermediaries. The carriers are the infrastructure providers. The carriage service providers (who may also be carriers) package access to this as a service (like a wholesaler). Carriers and carriage service providers are often dealt with together. The intermediaries (often called re-sellers, like retailers) are dealt with separately, with less protection for consumers and less influence over the network.

7.2 Telecommunications legislation

7.2.1 Telecommunications Act 1997 (Cth) ('TA') [FLR]

Under Part 14 of the *Telecommunications Act 1997*, relevant entities (carriers, CSPs and carriage service intermediaries) are under an obligation, to:

(A) 'do their best' to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or of the states and territories, s 313(1) and (2) (abbreviated to 's 313(1)' below); and

(B) give officers and authorities of the Commonwealth, states and territories such help as is reasonably necessary for the enforcement of the criminal law and laws imposing pecuniary penalties, assisting enforcement of foreign criminal laws, safeguarding national security and the protection of the public revenue, s 313(3) and (4) (abbreviated to 's 313(3)' below).

Additional obligations are imposed on carriers or carriage service providers under the *Telecommunications (Interception and Access) Act 1979* (Cth) covering:

(C) data retention, interception capability and delivery capability, Chapter 5 Parts 5-1A, 5-3 or 5-5 TIAA.

(D) provisions for various interception warrants and other requirements to collect, retain and deliver the contents of communications.

There are also obligations about collection, retention, preservation and delivery of information that is *not* the contents of communications, commonly called telecommunications data or 'metadata' (though the term 'metadata' is not used in the TIAA itself), typically without a warrant or court order.

7.2.1.1 Different approaches to retention of metadata and contents of communications

Some telecommunications information, both telecommunications metadata (information other than content) and the content of communications, may be legally required to be collected, retained and possibly disclosed ('delivered') to authorities.

Telecommunications metadata is collected routinely on a mass scale, with retention now required under the new retention scheme in Part 5-1A of the TIAA.

The content of communications is still collected on a very small, highly targeted and specifically authorised scale.

7.2.1.2 Retention of location information

Because only quite limited data is required to be retained (typically just data about the start and end moments of a communication, not data from within the three periods before, during or after these points), it is unclear the degree to which metadata retention obligations described above extend to cover further telecommunications data that could identify location and movements of a device or vehicle (location data), including cell tower information and related data.

'Service providers' covered by the metadata retention obligation are carriers and Internet service providers (ISPs).[78] They may wish to voluntarily collect, retain and deliver further telecommunications metadata outside the scope of a mandatory data retention obligation, specific request or warrant (for instance from before, during and after the start and finish points of a communication) and/or to retain the data beyond the mandated retention period. Such 'voluntary' extensions of collection, retention and delivery may in effect be neither required nor prohibited under law, at least as long as they do not involve 'interception' of communications content, which requires a warrant.

It may be useful to specify in legislation how far such a telecommunications provider is legally permitted to do additional voluntary collection and retention of telecommunications information from AV and C-ITS systems, whether for future law enforcement access or for their own purposes.

7.2.1.3 The ambiguous obligation for Telcos to do their best to prevent networks being used for offences

The obligations in section 313(1) and (2) for relevant telecommunications entities to 'do their best' for preventive purposes, (A) above, is ambiguous and has been the subject of scrutiny.[79] The discretion as to what preventive action is required appears to be left open by statute for the telecommunications entity, including to:

- identify which offences to seek to prevent,
- specify what methods to use in aid of prevention,
- state how much effort or funds to apply to the task, perhaps weighing up proportionality factors, and thus
- decide what in a given instance constitutes 'their best'.

If C-ITS or AV operators participate in telecommunications services themselves, they may be especially likely to receive such suggestions, given the richness of their network's data. They may also be new participants in the carriage service industry, as C-

[78] ISPs are as defined under the *Broadcasting Services Act 1992* (Cth). TIAA s 187A defines 'service provider'.
[79] Inquiry into the use of subsection 313(3) of the Telecommunications Act 1997 by government agencies to disrupt the operation of illegal online services, *Report*: *Balancing Freedom and Protection*, Standing Committee on Infrastructure and Communications, Parliament o f Australia, 1 June 2015 <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Infrastructure_and_Communications/Inquiry_into_the_use_of_section_313_of_the_Telecommunications_Act_to_disrupt_the_operation_of_illegal_online_services>. See submissions and Report.

ITS or AV operators would probably be, if they decided to run part of their communications internally.

7.3 Relevance of the type of C-ITS platform used

C-ITS could utilise the DSRC 5.9GHz platform or the cellular network (likely 5G). The type of platform used potentially affects the applicability of telecommunications legislation. However, both of the above may be covered by at least some of the telecommunications law.

Where C-ITS messages are sent over DSRC, they would not be sent over a carrier's 'carriage service' but in an adjacent band (via a similar mechanism to WiFi).[80] These messages would therefore not be covered by the major parts of the telecommunications legislation covering carriers, CSPs and carriage service intermediaries.

While the *Telecommunications Act* is largely focused on this carrier/carriage service context, the TIAA s 5 has a somewhat wider definition of 'telecommunications network', not confined to a telecommunications system operated by a carrier. A non-carrier system solely relying on 'radiocomunications' would be outside of the ambit of that Act, but if there was a terrestrial or non-radiocomunications aspect and no integration with a carrier – for instance, if a part wired part wireless system used a private network not a public carriage network to link things together – this could be covered. Some C-ITS platforms may operate in this way.

Where C-ITS messages are sent over the cellular network, they would be sent over a carrier's 'carriage service' and therefore would also be covered by the telecommunications legislation discussed above.

The applicability of telecommunications legislation is discussed above in Section 7. Applicability depends on the nature of the messaging methods, the data types, and what counts as 'telecommunications metadata' or the 'contents of a communication'. In the scenario above, the private backbone for C-ITS, not connected to the carrier system but operating independently as self-contained road infrastructure, would probably be outside of the carrier/carriage service parts of the TA, but within the scope of a 'telecommunications network' and thus subject to parts of the TIAA.

It would not be a service provider for the purposes of the metadata retention scheme if it was neither carrier nor ISP under s 187A of the TIAA, but it would be brought under it if it were subject to a declaration, which can apply to those other than carriers and ISPs. Further inquiry into the network architecture and the detailed profile against the various criteria in the TA and TIAA would be necessary to determine whether a particular instance was covered by some or all of the TIAA obligations.

[80] Under the *Telecommunications Act 1997* (Cth), 'carriage service' means a service for carrying communications by means of guided and/or unguided electromagnetic energy.

8 THE EUROPEAN DATA PROTECTION FRAMEWORK – OVERVIEW

8.1 The EU Framework

The relevant legal framework for the processing of personal data in relation to C-ITS and AVs is composed of two main parts, firstly the new *General Data Protection Regulation* ('GDPR')[81] – which came into force on 25 May 2018 and replaced the *Data Protection Directive*[82] – and secondly the new Directive on the protection of personal data processed for law enforcement purposes (*Law Enforcement Directive*), which was to be implemented by Member States by the 5th May 2018.[83] Government access and processing of personal information in the context of C-ITS and AVs might be governed by either the GDPR or the *Law Enforcement Directive*, or none of them (in case of national security, as explained below), depending on the purpose for which such data is accessed and processed by government agencies.

8.1.1 Scope and Applicability of EU Data Protection Framework

The GDPR applies to both public and private sector activities. In the context of C-ITS and AVs, this means that the GDPR regulates data collection and processing by C-ITS and AV manufacturers or their service providers, as well as any further processing of the data by government agencies (subject to exceptions). However, because the GDPR explicitly allows for exceptions to its provisions when they are necessary for 'the prevention, investigation, detection or prosecution of criminal offences ...',[84] any further processing of such data by the law enforcement agencies for criminal purposes is addressed separately in the *Law Enforcement Directive*.[85] A general framework regulating governments' (and private sector's) handling of personal information thus is covered by the GDPR, except in the criminal law enforcement context, where the *Law Enforcement Directive* applies. The *Law Enforcement Directive* is a standalone piece of legislation applicable whenever personal data is collected, accessed and/or processed by competent authorities for criminal law enforcement purposes.

---

81 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88.

82 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ 1995, L 281/31.

83 *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA,* OJ 2016, L.119/89. Member States are also offered a derogation allowing legacy processing systems to remain in place until 6th May 2023, with the option of a three-year extension to 2026, where there is a 'disproportionate effort' required to bring them into compliance. Additionally, a new *ePrivacy Regulation* proposed in 2017 (not yet adopted) will cover machine to machine communications, and thus may become relevant in the future, see European Commission, 'Proposal for a Regulation of The European Parliament and of The Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (known as the 'e-Privacy Directive'),' COM/2017/010 final - 2017/03 (COD). *Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* is currently being revised by the Commission.

84 Article 23, GDPR.

85 *Directive (EU) 2016/680*, above.

Another exception is that the GDPR and *Law Enforcement Directive* do not apply to data processing by the institutions, bodies, offices and agencies of the European Union (as an organization), whose data processing is governed by a separate EU legal framework under Regulation 45/2001.[86] And processing of personal data by special EU law enforcement agencies – e.g., Europol and Eurojust – are governed by yet more tailor-made data protection regimes.[87] Similarly, the EU data protection framework does not apply to data processing outside the scope of European Union law in which Member States retain full competence and may adopt national legislation without regard to EU law. The most notable example is that of national security.[88] This exception has been employed, for example, by the UK national security police to process data about car movements in London tracked as part of the city's congestion charging scheme.[89]

The GDPR is perceived as 'transnational law'[90] because it entails aspects of extraterritorial application that are relevant to Australia. Some Australian businesses, including C-ITS or AV manufacturers or their service providers, could be subject to the GDPR if they have an establishment in the EU (irrespective of whether they process personal data in the EU);[91] if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU, where that behaviour takes place in the EU.[92] The GDPR thus might be applicable to some Australian companies working with C-ITS and AVs that would need to comply with the GDPR requirements. It does not however generally extend to processing of EU citizens' personal data in Australia, or processing of [their] personal data by law enforcement and other government agencies in Australia.[93]

---

[86] Article 2 (3) of the *Law Enforcement Directive*. EU agencies are governed by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[87] Europol's mandate is defined in the Europol Council Decision (1) (ECD) of 2009. According to Art. 4 (1) ECD, its competence covers terrorism and organised crime as well as other forms of serious crime as listed in the Annex to the ECD, such as trafficking in human beings, Euro counterfeiting or drug related crimes. Article 5 of ECD stipulates that one of the core tasks of Europol is to 'Obtain, collate and analyse information, and intelligence Facilitate the exchange of information between Member States'. Data processing by Eurojust is governed by the Rules of Procedure on The Processing and Protection of Personal Data at Eurojust (Text adopted unanimously by the college of Eurojust during the meeting of 21 October 2004 and approved by the Council on 24 February 2005) (2005/C 68/01). A full list of EU agencies in the area of law enforcement is found at EU Home Affairs website, at <https://ec.europa.eu/home-affairs/what-we-do/agencies#6>, visited [date here? Or omit 'visited]

[88] Despite general applicability of EU data protection framework to both public and private sectors, national security issues remain outside the EU competence. Therefore, EU data protection law (or any other EU law) does not apply to any national security matters governed by domestic law, as these provisions are only relevant to 'Member States when carrying out activities that fall within the scope of EU law.' Article 4(2) of the Treaty of the EU (TEU) states that EU law shall 'respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.'

[89] Section 28 Data Protection Act 1998 Certificate of the Secretary of State, DPA/s.28/MPS/2007/CC1, 4 July 2007, <https://privacyinternational.org/sites/default/files/2018-02/12.%20Security%20Service%20.%20Section%2028%20Data%20Protection%20Act%201998%20Certificate.PDF>, visited 01/06/2018. For more about UK national security police powers in the UK see Ian Brown, 'Government access to private-sector data in the United Kingdom,' *International Data Privacy Law* 2.4 (2012): 230–238.

[90] Rubinstein, Ira, and Bilyana Petkova. 'The International Impact of the General Data Protection Regulation.' (2018); Mitrou, Lilian. 'The General Data Protection Regulation: A Law for the Digital Age?' *EU Internet Law* (Springer, Cham, 2017) 19–57.

[91] Article 3, and Recital 23 of the GDPR.

[92] Article 3 of the GDPR.

[93] See OAIC, *Does the EU General Data Protection Regulation (GDPR) apply to Australian government agencies?*, <https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/government-agencies/does-the-eu-general-data-protection-regulation-gdpr-apply-to-australian-government-agencies>.

8.2 Definition of 'Personal Data'

Under EU law, data related to C-ITS and AVs qualifies as 'personal data' for any party that may be able to link such data to a specific individual with reasonable and legal means available to them. It is irrelevant whether such data is technical, generated by the technology or provided by the data subject. Similarly, the question of anonymisation depends on whether the controller can employ reasonable means to re-establish such a reference to the individual.

8.2.1 Definition: Basics

The GDPR only applies to 'personal data', which it defines as any information relating to an identified or identifiable natural person ('data subject').[94] Personal details such as a driver's (or a C-ITS or AV user/passenger's) name, address and contact details, as well as a driver's (or other passengers') biometric and biological data (see also section 2.2), will be uncontroversially classified as personal data, and EU data protection laws will apply to the use of such data.

8.2.2 Geo-location Data is also Personal Data

Beyond personal details, biometric and biological data, geo-location data collected by C-ITS and AVs will be considered personal data under EU law where such data alone or in conjunction with other information identifies an individual (driver, passenger or user of a C-ITS or AVs) through their patterns of movement.[95] The GDPR has also explicitly clarified the status of geo-location data by expressly stating that an individual can be identified directly or indirectly by reference to 'location data.'[96]

8.2.3 Data Generated by C-ITS and AV sensors is also Personal Data under EU Law

Contrary to European automotive industry association arguments,[97] various data generated by C-ITS or AV sensors such as information about speed, acceleration and use of brakes, which could be either supporting the operation of automated functions, C-ITS communications or collected by Event Data Recorders (EDR), *could* constitute personal data in the opinion of EU Court of Justice,[98] the EU Commission,[99] EU data protection authorities and the Article 29 Working Party,[100] as well as majority of legal scholars.

---

94 Article 2 of the GDPR. See also Appendix G for further information.

95 See Article 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices,* <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp185_en.pdf>22, which states location data collected by smartphones is considered personal data because individuals can be directly or indirectly identified through their patterns of movement.

96 Article 4(1) GDPR

97 German Association of the Automotive Industry/Verband der Automobilindustrie (VDA), *Data Protection Principles for Connected Vehicles*, 3 November 2014, <http://www.vda.de/en/topics/innovation-and-technology/network/data-protection-principles-for-connected-vehicles.html>; VDA, in *Access to vehicle and vehicle generated data*, Position paper, 19 September 2016, p. 1, <http://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html>. See also European Automobile Manufacturers Association (ACEA), *ACEA Principles of Data Protection in Relation to Connected Vehicles and Services*, September 2015, p. 4, <http://www.acea.be/publications/article/acea-principles-of-data-protection-in-relation-to-connected-vehicles-and-se>; ACEA, *ACEA Strategy Paper on Connectivity*, April 2016, p.4, <http://www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf>. British Society of Motor Manufacturers and Traders (SMMT), *Connected and Autonomous Vehicles*, Position Paper, February 2017, p.6 et seq., <http://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf>.

98 European Court of Justice, Judgment of 19 October 2016, *Patrick Breyer* v. *Bundesrepublik Deutschland* – C-582/14. The Court further states, that for a qualification of data as personal it is not required 'that all the information enabling the identification of the data subject must be in the hands of one person'.

99 EU Commission, *A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, COM(2016) 766 final, 30 November 2016, p. 8,

8.2.4 Can 'Anonymised Data' be 'Personal Data' under EU Law?

Under EU law, data is no longer regarded as personal data if it is '*rendered anonymous in such a way that the data subject is no longer identifiable*'.[101] However, as defined by the CJEU in *Breyer* case, *identifiability* of data subject depends on the knowledge of the data controller (an entity which determines the purposes, condition and means of processing personal data)102 and the reasonable means they are able to deploy to re-establish the identity of data subject. Therefore, anonymity of data is relative: as long as C-ITS and AV manufacturers or government agencies may link a data item to a unique identifier that can be associated with a person, the data qualifies as personal data in relation to that specific manufacturer or government agency.

8.3 Government Powers to Compel / Access Third Party C-ITS and AV Data

The EU data protection framework provides a legal basis for third party access to personal data held by private bodies (e.g., C-ITS and/or AV manufacturers) and restrictions on the scope of the obligations and rights provided under the GDPR, where a legitimate interest is pursued by third parties such as police, national security enforcement agencies.[103] However, because the GDPR does *not* make any specific provisions for the needs of law enforcement or security services, it is up to each Member State to arrange the framework for law enforcement access through domestic legislation. While the *Law Enforcement Directive* establishes special data protection rules for the law enforcement context, it does not articulate the government powers to compel access to third party C-ITS and AV data, which is governed by national legislation of Member States.

For example, in the UK, government powers to compel access to private sector data, including laws enforcement and national security access, are established in the *Investigatory Powers Act 2016.*[104] The Act grants authorization to various law enforcement agencies to carry out surveillance and investigation, interception of communications and bugging of vehicles undertaken for wide ranging purposes such as national security, prevention and detection of serious crime or safeguarding economic well-being of the UK.[105] A warrant from the Home Secretary is required for

<http://ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v5.pdf>, visited 15/05/2018. See also EU C-ITS Platform Final Report, September 2017, available at <https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf>, p. 28. The C-ITS platform is an initiative of Directorate for Transport and Mobility of the EU Commission, which started at the end of 2014 with the creation of specialized working groups, each addressing various aspects of C-ITS deployment, ranging from security, to technical standardization, to data protection. The Data Protection and Privacy Working Group of C-ITs stated that broadcast messages exchanged by vehicles are personal data because: *1) the messages contain authorisation certificates that are univocally associated to the sender, and; 2) the messages contain heading, timestamp, location data and the dimension of the vehicle.*

[100] Article 29 Working Party, *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)* <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171> p. 6. The Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy whose tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[101] Rec 26 GDPR.

[102] Article 4(7) of the GDPR defines 'controller' as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.

[103] Article 23, para. 1 of the GDPR. See House of Lords Science and Technology Select Committee, *Connected and Autonomous Vehicles: The future?* [172].

[104] See <http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted>.

[105] See Part II of the *Investigatory Powers Act 2016*.

wiretaps and reading posts, but in case of surveillance measures, such as bugging of vehicles, authorization from the head of relevant agency is sufficient.[106] By contrast, in Germany, judicial approval is required for wiretapping by the police in criminal cases and interception for national security and intelligence purposes is conducted upon the approval of the Interior Minister and a commission appointed by the Parliament.[107] Similarly, in France, the most intrusive forms of data searches for the purposes of criminal investigation, such as real-time interceptions of private correspondence, whether a telephone conversation, email, or instant message, requires the prior authorization of an independent judge.[108] Generally, police authorities can require disclosure of stored data with varying levels of approval, depending on the stage of the investigation.[109] The access to data by intelligence agencies is governed by the French Internal Security Code, which provide less data protection than the Code of Criminal procedure, however, data collection for intelligence purposes can be implemented only when a specific authorization is given by the Prime Minister.[110] The specific requirements thus vary in each Member State.

8.4 GDPR Protection

The updated EU data protection regime under the GDPR is not fundamentally different from the earlier *Data Protection Directive* in its substance (for example, it does not redefine personal data or the core principles of data protection law), however it introduces several novel elements that are worthy of attention in the context of government access to C-ITS and AVs data.

8.4.1 Privacy by Design/Privacy by Default

The GDPR explicitly incorporates an obligation for data controllers to comply with principles of 'privacy by design' and 'privacy by default'.[111] The former approach aims at ensuring that privacy protections are built into the design and development of new technologies and services, as opposed to being implemented subsequently as part of a legal review process. In relation to C-ITS and AVs, 'privacy by design' would mean, for example, an interactive dashboard, allowing the driver to customize and turn on/off the technology's ability to collect different types of personal data, thereby giving the data subject more control over their personal data. Similarly, a 'privacy by default' approach would mean having sensors that collect personal data switched off by default (a so-called 'opt-in' approach). This would help to ensure that data subjects' personal data are not processed automatically without their consent.

---

[106] Woods, Lorna. 'The Investigatory Powers Act 2016,' *Eur. Data Prot. L. Rev.* 3 (2017), 103.
For more on the UK system, see also Brown, Ian, 'Government access to private-sector data in the United Kingdom,' (2012), *International Data Privacy Law* 2.4 230–238.

[107] § 3, § 5 Artikel 10-Gesetz, <http://www.gesetze-im-internet.de/bundesrecht/g10_2001/ gesamt.pdf>. Germany's Constitutional Court has played a crucial role in overseeing and establishing limits on the surveillance activities of Germany's foreign intelligence agency, forcing several amendments to the regulation of the so-called 'strategic surveillance' for intelligence purposes; see further Paul Shwartz, 'Systematic Government Access to Private Sector Data in Germany', in Fred Cate and James Dempsey (eds), *Bulk Collection*, OUP, 2017.

[108] Articles 100 and 706-95, Code of Criminal procedure.

[109] See further W. Maxwell, 'Systematic Government Access to Private-Sector Data in France,' in Fred Cate and James Dempsey (eds), *Bulk Collection*, OUP, 2017.

[110] Article L821-1, Internal Security Code. See also 2015 Surveillance Law n° 2015-912 of July 24, 2015, o.J. July 26, 2015, p. 12735.

[111] Recital 78 of the GDPR. The recital requires that the producers of the products, services and applications to be encouraged to take into account the two principles to make sure that the controllers and processors are able to fulfil their obligations.

8.4.2 Data Minimisation/Data Avoidance

The GDPR explicitly incorporates an obligation for data controllers to comply with principles of 'data minimization' and 'data avoidance' which require that personal data be adequate, relevant and **limited to what is necessary** in relation to the purposes for which those data are processed.[112] This means that both C-ITS and AV manufacturers and government agencies must limit personal data collection only to what is needed for their legitimate business purposes and delete it when it is no longer 'necessary'. Certain AV data categories such as image data external to the vehicle (see section 2.2 above), which are collected for the purposes of supporting vehicle operation, should be deleted a short amount of time after they are collected since their main purpose is to enable the vehicle to operate. Similarly, if data internal to the vehicle and biometric data is collected for the purpose to support AV operation and ensure safety, then such data should be deleted after relatively short period of time, provided that no accidents have occurred. On the other hand, manufacturers could claim that such data is necessary for future research and improvements of the C-ITS and AVs operation. In theory, this requirement should therefore reduce the availability of data which government may compel or request from manufacturers or their service providers, as it would be deleted soon after it was collected. However, it remains to be seen whether the 'necessity' requirement will be interpreted broadly and how effective these principles will be in practice.

8.4.3 Right to be Forgotten, or Right to Erasure

The GDPR articulates the so-called 'right to be forgotten', formally known as the 'right to erasure,' which entitles individuals to require data controllers to delete their data when they are no longer necessary for the purposes for which it was collected, or when the individual withdraws their consent and there is no other legal ground for processing personal data.[113] Right to erasure, which does not have an equivalent under the Australian *Privacy Act 1988,* could cover image data internal to the vehicle, audio data, and data covering biometric and biological factors in particular, which could be argued to be not necessary after a short period of time after their collection. However, similar to the principle of data minimization, it remains to be seen how strictly 'necessity' requirements will be interpreted by the EU regulators and the EU Court of Justice.

8.4.4 Sanctions and Fines for Violations of the GDPR

The powers and influence of the data protection authorities (DPAs) are significantly increased under the GDPR, in particular the ability to impose very high fines for non-compliance with the GDPR.[114] This provision might have the strongest impact on the willingness of the C-ITS and AV manufacturers to share personal data with government agencies voluntarily and/or in secret arrangements.

8.5 Data Protection Safeguards in the Context of Law Enforcement

When law enforcement agencies access private sector data, the general rules applicable to the processing of personal data for law enforcement purposes are regulated on the EU level under Directive 2016/680 (the *Law Enforcement Directive*). Certain sector

[112] Rec. 39; Art. 5(1)(c) of the GDPR.
[113] Article 17 of the GDPR.
[114] See Article 83, paras. 4–5 of the GDPR.

specific laws, such as the *Anti-Money Laundering Directive,* also govern law enforcement access to data held by financial sector.[115]

The law enforcement purposes under the *Law Enforcement Directive* include 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.'[116] They are formulated broadly, and potentially imply a wide range of processing contexts which, in principle, may involve private parties and public-private partnerships. Recital 12 clarifies that the material scope of the Directive includes 'police activities without prior knowledge if an incident is a criminal offence or not. Such activities ... also include maintaining law and order ... where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence'. Under Recital 27, the data processing covered by the *Law Enforcement Directive* does not have to be conducted exclusively in the limited context of the prevention, investigation, detection, or prosecution of specific criminal offences, but also includes processing in order 'to develop an *understanding* (emphasis added) of criminal activities and to make links between different criminal offences detected'.[117]

8.5.1 Competent Authorities & Vague Purposes

The 'competent authorities' for law-enforcement purposes under the *Law Enforcement Directive* include two types of actors: 'traditional' law-enforcement authorities such as police, national courts and other judicial authorities,[118] prosecution, customs, and specialized law enforcement agencies (i.e., with investigatory powers in specific contexts, for example, fiscal fraud);[119] and 'any other body or entity entrusted by national law to exercise public authority and public powers'.[120] This could include private parties or even public-private partnerships, if they are sufficiently 'entrusted'. They might also include traffic law enforcement agencies under the specialized enforcement category.

Any data processing by such competent authorities for other purposes, including archiving in public interest, scientific or historical research, statistical purposes, generally falls under the GDPR.[121] Data processing for administrative and traffic law

---

[115] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance)

[116] Article 1 of Directive 2016/680.

[117] Recital 27 of the Law Enforcement Directive reads as follows: 'For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.'

[118] Recital 90 of the *Law Enforcement Directive*.

[119] Article 3(7)(a) of the *Law Enforcement Directive*, read in light of Article 87 TFEU that establishes police cooperation within the EU.

[120] Article 3(7)(b) of the Law Enforcement Directive, read in light of Article 87 TFEU that establishes police cooperation within the EU.

[121] See Article 9(2) and Recitals 11 and 12 of Law Enforcement Directive. The Recital 11 of the Law Enforcement Directive reads as follows: 'Where ... a body or entity processes personal data for purposes other than for the purposes of this Directive, Regulation (EU) 2016/679 applies. Regulation ... therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to

enforcement or imposition of penalties also is formally excluded from the *Law Enforcement Directive* and so also falls under the GDPR. However, vague formulations render most of information sharing between C-ITS and AV manufacturers or operators and law enforcement (or between government and law enforcement agencies; or between two or more law enforcement agencies), for broadly defined 'criminal purposes' capable in principle of falling within processing under the *Law Enforcement Directive,* and not the GDPR. Therefore, crash investigations and traffic law enforcement could fall under the Law Enforcement Directive.

8.5.2 Law Enforcement Directive Offers Less Protection than GDPR

From a data protection perspective, the law enforcement authorities have much more leeway with respect to processing of personal data under the *Law Enforcement Directive* as compared with the GDPR regime. For instance, while Article 9 GDPR explicitly bans processing of 'sensitive' data (e.g., biometric data) unless one or more of the listed exceptions apply, Article 10 of the *Law Enforcement Directive* does not use prohibitive language. EU legal scholars have argued that the *Law Enforcement Directive* does not provide the level of protection articulated by the European Court of Justice in its recent case-law on data retention for law enforcement purposes.[122] In particular, the *Law Enforcement Directive* is regarded as insufficiently articulating objective criteria to limit law enforcement access, and thus seriously undermining the key 'purpose limitation' principle of EU data protection law.

8.6 EU-Wide Data Sharing Among Competent Authorities

Competent national law enforcement authorities in EU are able to further share C-ITS and AV personal data on an EU-wide accessible database known as the *Schengen Information System* (SIS). According to EU Home Affairs, 'SIS is a highly secure and protected database which is exclusively accessible to the authorised users within competent authorities, such as national border control, police, customs, judicial, visa and vehicle registration authorities.' This suggests that the C-ITS and AV information may be entered and shared on SIS. The basic principle of data protection within SIS 'is that the state that entered the alert is responsible for its content.'[123] This means that the authorities entering data to and/or accessing SIS are governed by the *Law Enforcement Directive* (if personal data relates to high level alert for criminal activities) or they are exempt from data protection rules entirely if the data in question relates to high-level alerts related to national security.

processors pursuant to this Directive, while the application of Regulation ... remains unaffected for the processing of personal data by the processor outside the scope of this Directive.'

[122] See, e.g, Jasserand Catherine, 'Law Enforcement Access to personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?' *Computer Law & Security Review*, 34 (2018) 154–165.

[123] Read more at EU Home Affairs Website, at <https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/access-rights-and-data-protection_en>.

9 THE RELEVANT LEGAL FRAMEWORK IN THE USA – OVERVIEW

In stark contrast to the EU legal framework, the US legal system does not have a general data protection or privacy framework that would comprehensively regulate the activities of both the public and private sectors. Instead, many different sectoral laws exist that establish separate rules for specific industries, such as banking and finance. US law and federal legislation thus does not generally regulate the collection and use of personal data derived from C-ITS and AVs by the private sector.[124] It also does not entail an equivalent of the GDPR transnational rule which would require some Australian C-ITS and AVs companies to comply with US law. The US legal framework limiting government powers to access and process personal data is comprised of Constitutional protections against governmental intrusion, federal legislation, and state legislation.

9.1 US definition of 'personal data' or 'personally identifiable information'

The US legal system lacks uniform definition of terms such as personal data or personal information. Instead of defining personal information/data in a coherent and consistent manner, privacy law in the US offers multiple competing definitions. Numerous federal and state statutes in the US turn on the definition of 'personal data' or 'personally identifiable information'[125] (often abbreviated to PII), and three dominant approaches to defining personal information could be seen: (1) the 'tautological' approach, (2) the 'non-public' approach, and (3) the 'specific types' approach.

- Under the 'tautological' approach, US privacy law simply defines 'personal' as meaning any information that identifies a person.[126]
- The 'non-public' approach defines 'personally identifiable financial information' as 'non-public personal information.'[127]

The 'specific types' approach, found in State data breach notification laws, is to list specific types of data that constitute personal information under specific statutes, rather than offer a general definition.[128]

Three distinct classifications means that the same information may or may not be personal data under different statutes and in different processing contexts. As a general rule, 'personally identifiable information' (PII) in the US is largely limited to instances where data refers to an actually *identified* individual. There is a clear contrast with 'personal data' in the EU or 'personal information' in Australia (see section 3. 'Personal information' above), where data protection law extends expansively to any data that is *identifiable* – i.e., that could reasonably be linked to an individual.[129] It is widely acknowledged by US privacy scholars that the existence of three definitions obscures

[124] A detailed overview and discussion on private sector use and collection or C-ITS and AVs users' personal data, please see William J. Kohler & Alex Colbert-Taylor, 'Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles,' 31 *Santa Clara Computer & High Tech. L.J.* 99, 121 (2015).
[125] Examples of federal laws include the *Children's Online Privacy Protection Act*, the *Gramm-Leach Bliley Act*, the *HITECH Act*, and the *Video Privacy Protection Act*. Examples of state laws include California's *Song-Beverly Credit Card Act* and the numerous state breach notification laws. The wide-ranging recent *California Consumer Privacy Act of 2018* defines 'personal information' using a mix of 'specific types' and 'non-public' approaches.
[126] For example, the *Video Privacy Protection Act of 1988* (VPPA) 18 U.S.C. § 2710 (2006), which safeguards the privacy of video sales and rentals, defines 'personally identifiable information' as 'information which identifies a person.' Id. § 2710(a)(3).
[127] See e.g., *Gramm-Leach-Bliley Act of 1999* (GLBA) 15 U.S.C. § 6809(4)(A) (2006). The statute fails to define 'non-public,' but presumably this term means information not found within the public domain.
[128] See the notes to section 9.3.3 below on State Data Breach Notification Laws.
[129] Article 2 and 4 of the GDPR, and sections on EU legal framework; definitions in s 6 Privacy Act 1988 (Cth) and similar parts of state and territory privacy laws – see Appendix B below.

regulatory clarity, creates potential for confusion, and increases associated compliance costs for regulated entities.[130]

9.2 US Government Powers to Compel or Access Third Party Data / US Domestic Authorizations for Law Enforcement

Generally, the US legal system does not directly authorize ongoing and indiscriminate government access to third-party-held personal data or personal information.[131] Law enforcement officials can use the domestic legal framework to access such data located within the relevant US jurisdiction.[132] The primary US law that governs domestic law enforcement powers to compel an individual or third party to provide electronic communications are the *Electronic Communications Privacy Act of 1986* (ECPA)[133] and the *Stored Communications Act of 1986* (SCA). They provide law enforcement agencies with a variety of legal tools, such as subpoenas (access to metadata only),[134] court orders (access to metadata plus additional info, such as IP address),[135] and search warrants (access to content data, physical devices which store digital communications) to seek access to *stored* communications data (see Appendix G for more detail). Electronic surveillance and access to real-time data – as opposed to data already collected in the past – requires separate legal processes and orders by the law enforcement agencies under the *Federal Wiretap Statute*[136] and/or the *Pen Register, Trap and Trace Statute* enacted as part of ECPA.[137]

Additionally, national security laws authorize law enforcement access to third-party data under certain specific circumstances. For example, the *Foreign Intelligence Surveillance Act of 1978* (FISA)[138] allows law enforcement to compel access to physical and electronic evidence or conduct surveillance if the applicant (national security agency) can show probable cause that the target is a foreign power or agent of a foreign power. Similarly, the National Security Act of 1947139 and the Patriot Act of 2001140 allow the Federal Bureau of Investigations (FBI) to issue administrative subpoenas, commonly called 'National Security Letters', to compel access to personal metadata

---

130 See Solove, Daniel J. and Schwartz, Paul M., 'Reconciling Personal Information in the United States and European Union' (2013). GW Law Faculty Publications & Other Works. Paper 956. <http://scholarship.law.gwu.edu/faculty_publications/956> p. 16.

131 Certain third-party disclosures of various types of data are required by the US, such as, e.g, cargo and passengers coming into the US (so-called Passenger Name Records), and financial data for money laundering and terrorist financing (SWIFT). See generally Pell, Stephanie, 'Systematic Government Access to Private-Sector Data in the Unites States I' in Cate, F., and Dempsey, J., *Bulk Collection: Systematic Government Access to Private-Sector Data*, OUP, 2017.

132 In cases when data is not located in US jurisdiction, law enforcement officials may work through international processes, such as treaties for mutual legal assistance or police-to-police cooperation agreements, to access that data.

133 *Electronic Communications Privacy Act of 1986*, 18 U.S.C. §121 (1986).

134 '279 Subpoenas,' Offices of the U.S. Attorneys, Criminal Law Manual, accessed 29 June 2017, 〈https://www.justice.gov/usam/criminal-resource-manual-279-subpoenas>.

135 *Electronic Communications Privacy Act of 1986*, 18 U.S.C. § 2703(d) (1986). E.g., SCA court orders may compel access to IP addresses associated with a particular email sent from that account and 'to' and 'from' fields in an email, see 'Google Transparency Report,' Google, <https://transparencyreport.google.com/>.

136 ('Title III'), 18 USC 2510 et seq., which requires a probable cause order from a judge for real-time interception of the content of voice and data communications. This legal standard is high.

137 This governing real-time interception of 'the numbers dialed or otherwise transmitted on the telephone line to which such device is attached.'

138 *Foreign Intelligence Surveillance Act of 1978*, 50 18 U.S.C. Ch. 36 (2015), Cornell University, <https://www.law.cornell.edu/uscode/text/50/chapter-36>.

139 *National Security Act of 1947*, 50 U.S.C. § 3162 (1947).

140 *USA PATRIOT Act of 2001*, Section 505, P.L. 107-56, 115 Stat. 365-66 (2001).

stored in the US.[141] These letters often entail a so-called 'gag' provision which prevents a private company receiving the subpoena from disclosing it.[142] In some cases, legislation which has nothing to do with government powers to access data, such as *All Writs Act of 1911* governing the judiciary,[143] have been used to gain access to password-protected mobile phones in domestic drug related and/or terrorism investigations and could similarly be used to gain access to C-ITS and AV data in exceptional circumstances.

Moreover, the US has recently adopted legislation, which gives US law enforcement powers to access to data stored abroad. In particular, on March 23 2018, the US President Trump signed the *Clarifying Lawful Overseas Use of Data* (CLOUD) Act,[144] which requires service providers such as Microsoft or Google to disclose all data in their possession, custody, or control, pursuant to lawful process, regardless of the location of the data.[145] This means that C-ITS and AV data, which is stored in Australia, could nonetheless be accessed by US law enforcement agencies if the data in question is related to US citizens (not Australian or other citizens) and is under the control by US technology companies.[146]

9.3 US Legal Protections Against Government Access to Personal Information

US law and federal legislation does not generally regulate the collection and use of personal data derived from C-ITS and AVs by the private sector.[147] Some limited protections do however exist preventing the government from unrestrained access to personal data derived from C-ITS and AVs. The US legal framework governing government powers to access such data comprises:

- Constitutional protections against governmental intrusion,

---

[141] If the metadata of a target citizen is deemed 'relevant' to an investigation into terrorism or clandestine activities, the FBI can send a national security letter to a provider to access non-content, and the provider is prohibited from revealing receipt of the letter for 180 days. These letters are also authorized by several federal sector-specific statutes, such as the *Right to Financial Privacy Act of 1978*, 12 U.S.C. § 3414 (1978); the *Fair Credit Reporting Act of 1970*, 15 U.S.C. §1681u, v.); and the *USA PATRIOT Act of 2001*, Section 505, P.L. 107-56, 115 Stat. 365-66 (2001) including the *Electronic Communications Privacy Act of 1986*, 18 U.S.C. § 2709 (1986); the *National Security Act of 1947*, 50 U.S.C. § 3162 (1947).

[142] See Federal Bureau of Investigation, 'Termination Procedures for National Security Letter Nondisclosure Requirement,' <https://www.fbi.gov/file-repository/nsl-ndp-procedures.pdf>, visited 14 May 2018. The FBI reviews whether to disclose a letter at the close of each investigation or three years or more after it issues the letter. Although court decisions and the *USA FREEDOM Act* have since limited these gag provisions, such as by requiring prompt judicial review and a 'reciprocal notice' requirement, whereby the government must justify gag orders if the recipient of the letter requests juridical review, it is still an open question whether national-security-letter gag clauses are constitutional. See *In re National Security Letter*, No. C 11-02173 SI (N.D. Cal. 2013), Electronic Frontiers Foundation, <https://www.eff.org/document/nsl-ruling-march-14-2013>; *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, 18 U.S. Code § 2709 (2015). Several companies and activist groups are currently challenging national security letters and other gag orders under 18 U.S. Code § 2709. See, Andrew Crocker, 'Adobe puts an End to Indefinite Gag Orders,' Electronic Frontier Foundation, 24 April 2017, visited July 14, 2017, <https://www.eff.org/deeplinks/2017/04/adobe-puts-end-indefinite-gag-order>.

[143] *All Writs Act* 28 U.S.C. § 1651 authorizes the United States federal courts US federal courts to 'issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.' This Act is not used for typical investigations, and could be understood as the 'last resort' by law enforcement agencies.

[144] *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, H.R. 1625, 115th Cong. div. V (2018) (enacted) (to be codified in scattered sections of 18 U.S.C.). The *CLOUD Act* was enacted following the litigation by the US government and Microsoft over access to e-mails stored on Microsoft servers in Ireland.

[145] HR. 1625, 115th Cong. div. V, § 103(a) (2018) (enacted) (to be codified at 18 U.S.C. § 2713).

[146] For an overview of the *CLOUD Act*, see Jennifer Daskal, 'Microsoft Ireland, *CLOUD Act,* and International Law-Making 2.0', 71 *Stan. L. Rev. Online* 9 (2018).

[147] A detailed overview and discussion on private sector use and collection or C-ITS users' personal data, please see William J. Kohler & Alex Colbert-Taylor, Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles, (2015) 31 *Santa Clara Computer & High Tech. L.J.* 99, 121.

- Federal legislation, and
- State legislation.

9.3.1 Constitutional Protections Against Government Access to Personal Data

The primary legal limitation on the government's access to the personal data of individuals in the US legal system is addressed and dealt with via the Fourth Amendment to the US Constitution, which prohibits unreasonable searches and seizures.[148] In the specific context of C-ITS and AVs, a vehicle exception to the 4th Amendments has to be noted, which permits law enforcement officials to stop and search vehicles based on 'probable cause' without having to get a judicial warrant.[149] Arguably, this exception is hard to sustain with regards to personal data derived from C-ITS and AVs, which involves much more than a mere physical inspection of the vehicle and its contents. Indeed, the US courts have recognized that warrantless GPS tracking of vehicles by government is contrary to the 4th Amendment.[150] Relevant case law covering direct collection of information by government and the Fourth Amendment is discussed in Appendix G.

In relation to government access to information held by a third party, the law is in flux as to whether the 4th Amendment protects location information in the possession of a third-party. The infamous 'Third Party Doctrine' in the US limits 4th Amendment privacy protections whenever law enforcement (and national security) agencies seek to access personal information from third parties to whom data subjects have voluntarily disclosed it.[151] It allows for the circumvention of privacy protection by law enforcement agencies without a judicial warrant. There is currently no case law to specifically address the application of the 'Third Party Doctrine' to C-ITS and AVs.[152] However, as some C-ITS and AV information is arguably voluntarily disclosed by drivers and passengers, the Fourth Amendment may not provide any real privacy protection from law enforcement access to personal information held by a third party.[153] See by comparison sections 4.2, 4.3 and 4.6 above, for the Australian situation.

9.3.2 Federal Legislation Protecting Data Privacy

In response to Supreme Court opinions limiting 4th Amendment protections, the US Congress enacted various statutes ensuring privacy protection for personal information held by a third-party. Several federal statutes focus on data privacy issues that are relevant for (federal or state) government access and use of personal data derived from C-ITS:

- *The Privacy Act of 1974,* 5 U.S.C. § 552a – applicable to federal agencies;

---

148 US Fourth Amendment.

149 For more detailed discussion, see Myers, David. 'The Warrantless Use of GPS Tracking Devices: Fourth Amendment Protection Restored Through Application of an Analytical Framework.' *Case W. Res. JL Tech. & Internet* 3 (2012): 1.

150 See *United States v Jones*, 132 S. Ct. 945, 955 (2012).

151 *United States v Miller*, 425 U.S. 435 (1976); *Smith v Maryland*, 442 U.S. 735 (1979). See also Orin S. Kerr, 'The Case for the Third-Party Doctrine', (2009) 107 MICH. L. REV. 561; see also *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d*), Misc. Nos. 1:11–DM–3, 10–GJ–3793, 1:11–EC–3, 2011 WL5508991 (E.D. Va. Nov. 10, 2011).

152 The recent *Carpenter* case below may however be directly relevant to vehicle related telecommunications data geo-location, and potentially of wider application in principle to other forms of C-ITS or AV system data.

153 Stop press: the US Supreme Court in *Carpenter v. United States,* 585 U.S. (2018), No. 16–402, 22 June 2018, very recently decided that the government generally needs a warrant to track an individual's location through cell phone records over an extended period of time, overturning the previous approach based on analogies to the postal service. Further analysis will be required to assess the degree to which this affects other data of relevance here. See <http://cdn.cnn.com/cnn/2018/images/06/22/16-402_h315.pdf>.

- *Paperwork Reduction Act of 1980,* 44 U.S.C. § 3501 *et seq.* – applicable to federal agencies;
- *E-Government Act of 2002,* Pub.L.107–347, 44 U.S.C. § 101 – applicable to federal agencies;
- *Driver's Privacy Protection Act of 1994* (DPPA) – applicable to state agencies;
- *Drivers Privacy Act of 2015* – covers Event Data Recorder (EDR) data, applicable to both state and federal agencies;
- *Electronic Communications Privacy Act,* 18 U.S.C. §§ 2510–2522 (ECPA) – may cover certain aspects of C-ITS and AVs communications, applicable to both federal and state law enforcement agencies;
- *Telecommunications Act of 1996*, 47 U.S.C. § 222 – may cover certain aspects of C-ITS and AVs communications, applicable to private actors ('telecommunications carriers').

9.3.2.1 General Framework Governing Federal Agencies' Data Collection

The *Privacy Act of 1974*, *Paperwork Reduction Act of 1980* and *E-Government Act of 2002* establish the general framework of 'good practices' for processing PII for the US federal agencies that are relevant in theory, but not necessarily in practice, for C-ITS or AVs. See Appendix G below.

9.3.2.2 Driver's Privacy Protection Act of 1994 (DPPA)

The *Driver's Privacy Protection Act of 1994* (DPPA) applies to personal information collected and used by State (as opposed to Federal) Departments of Motor Vehicles (DMVs).[154] (See section 4.1 above for similar Australian regulatory features). In particular, the DPPA limits the use of a driver's motor vehicle record to certain purposes, prohibits the release or use personal data about an individual obtained by the department in connection with a motor vehicle record, and sets penalties for violations and makes violators liable on a civil action to the individual to whom the released information pertains.[155]

The latest amendment to the DPPA requires states to get permission from individuals before their personal motor vehicle record may be sold or released to third-party marketers. However, the DPPA permits the access to personal data by *any* government agency in carrying out its functions, and when there is a 'use in connection with matters of motor vehicle or driver safety and theft,' and the use and sharing of data in connection civil, criminal, administrative or arbitral proceedings.[156] The nuances in applicability of the DPPA to C-ITS and AVs have not yet been explicitly addressed by the US Courts or policy-makers, and the ability of the DPPA to cover personal data beyond the traditional categories to include information derived from C-ITS and AVs remains questionable.[157]

---

[154] See *Driver's Privacy Protection Act*, 18 U.S.C. §§ 2721 (2012); see also EPIC, 'The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record', <https://epic.org/privacy/drivers/> visited 8 May 2018. § 2725(3) defines personal information to include individual's photograph, social security number, driver identification number, name, address, telephone number, and medical or disability information. *Reno v Condon*, 528 U.S. 141 (2000). In *Condon*, the Supreme Court upheld the constitutionality of the *Drivers Privacy Protection Act* following a challenge by the state of South Carolina which alleged that the Act violated principles of federalism. The Court held that the Act is a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause.

[155] 18 U.S.C. §§ 2721(a). The statue also sets penalties for those who are found liable in violating it.

[156] Legitimate purposes for personal data used are defined in 18 U.S.C. § 2721.

[157] Dorothy J. Glancy, 'Symposium: Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem', 16 *Minn. J.L. Sci. & Tech*. 619, (2015), at 676–77.

9.3.2.3 Drivers Privacy Act of 2015

The *Drivers Privacy Act of 2015*[158] applies to any data retained by an Event Data Recorder (EDR) installed in a vehicle, and stipulates that such data belongs to the *owner* or *lessee* of the vehicle in which the EDR is installed, and can only be downloaded with the consent of the vehicle owner/lessee.[159] However, exceptions apply for court and administrative orders, vehicle safety research, responses to medical emergencies after car accidents, as well as investigations authorized by federal law, subject to limitations on the disclosure of personally identifiable information and the vehicle identification number.

9.3.2.4 Electronic Communications Privacy Act of 1986 (ECPA) and Stored Communication Act of 1986

Data stored within C-ITS and AV could also bring it within the scope of the *Electronic Communications Privacy Act of 1986* (ECPA) and *Stored Communication Act of 1986*. As mentioned above, ECPA regulates when electronic communications can be intercepted, monitored, or reviewed by third parties, and makes it a crime to intercept or procure electronic communications unless otherwise provided for under law or an exception to ECPA. The ECPA of 1986 was originally adopted to address the interception of data transferred between telephones and has not been revised since then despite the enormous changes brought by digitalization and the ubiquity of mobile computing devices. Courts have found that the ECPA 'protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility', and that it 'reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility.'[160] It is not clear, however, whether ECPA would provide protections for personal data held in the cloud computing servers that are often utilized by C-ITS and AV manufacturers.

9.3.2.5 Telecommunications Act of 1996

The *Telecommunications Act of 1996* requires 'telecommunications carriers' to 'protect the confidentiality of 'proprietary information' of their customers. (See section 4.2 and section 7 above for Australian regulatory features affecting telecommunications). However, it is not clear whether C-ITS and AVs system manufacturers or service providers could fall under the category of 'telecommunication carrier', which usually covers the landline or mobile phone network providers. The nature of any dedicated technical channels in addition to those of existing general carriers will influence this question. On the other hand, because elements of C-ITS and AVs are connected to the Internet, network service providers would probably fall under this category and trigger data privacy protections for some personal data derived from C-ITS and AVs.

9.3.3 State Legislation

Many US states have adopted data breach notification laws that require notification of personal data breaches to the data subject and/or a regulator. These laws however do

[158] The *Driver Privacy Act of 2015* was enacted as part of the Fixing America's Surface Transportation Act (H.R. 22).

[159] For purposes of the *Driver Privacy Act of 2015*, an EDR is defined in 49 CFR section 563.5 and generally means a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to or during a crash event, but does not include audio and video data. Installed in nearly all new cars, EDRs capture data elements such as speed, braking, use of a seat belt, and other information.

[160] *Theofel v Farey-Jones*, 341 F.3d 978, 982 (9th Cir. 2003).

not provide for substantive data privacy protection. As of 29th January 2018, 17 states[161] have laws addressing privacy concerns arising from EDR, similar to the federal *Drivers Privacy Act of 2015.*

9.3.4 Future Potential for Legislation

Existing federal legislation on information and data privacy in the USA is largely inapplicable to private sector collection and use of personal data, and only provides limited protections against government access to such data. A significant potential for specific legislation focussing on personal data derived from C-ITS and AVs, similar to legislation covering Event Data Recorder (EDR), has been recognized by numerous scholars and commentators,[162] suggesting that the US Congress and state legislatures could enact laws to cover the entire data set from C-ITS and AVs. However, there does not appear to have been any specific discussion or comment by Congress or government on this issue.

[161] See US Congressional Research Service, 'Privacy Of Data From Event Data Recorders: State Statutes', <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx>, describing in detail the laws of the seventeen states – Arkansas, California, Colorado, Connecticut, Delaware, Maine, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Oregon, Texas, Utah, Virginia and Washington – that have enacted statutes relating to Event Data Recorders and privacy. Among other provisions, these states provide that data collected from a vehicle Event Data Recorder may only be downloaded with the consent of the vehicle owner or policyholder, with certain exceptions.

[162] See, e.g, Dorothy J. Glancy, 'Symposium, Privacy in Autonomous Vehicles', 52 *Santa Clara L. Rev*. 1171 (2012), at p. 1202.

10 CONCLUSIONS AND OBSERVATIONS: GAPS AND AMBIGUITIES IN COVERAGE OF CURRENT/ANTICIPATED C-ITS & AV DATA

This section draws out some observations about gaps, inconsistencies or ambiguities, particularly in the coverage or treatment of current and anticipated C-ITS & AV data by existing law.

10.1 Information sources and data as 'personal information'?

10.1.1 A continuum rather than certainty

The information involved in C-ITS and AV systems will often, but not necessarily in all circumstances, constitute 'personal information' and thus come under privacy and data protection law in Commonwealth and state and territory jurisdictions.

The analysis of the types of data in section 2.2, the nature of the information derived from it, and of the degree to which each type may be 'personal information' in section 3.6 shows a range between data more likely to be PI (in all or some circumstances) such as in-cabin audio and image data and data less likely to be so, including raw DSRC C-ITS and raw GNSS data. Numerous cases, included those cited in *Waters v TFNSW* (see Appendix A) reiterate that whether information counts as personal is contextual as much as it is categorical. The range of data and the range of contexts in the C-ITS and AV environment is likely to be large, with variations and special factors at every level.

Therefore, it should be recognised that it will rarely be feasible to assign a certain attribution as PI or not PI to categories of C-ITS and AV system data. This is due to:

- the broad diversity of data types, contexts for each data type, and information derivable from specific instances;
- the fluid and evolving nature of the technology and data in C-ITS and AV systems; and
- the legal recognition that the question of whether a certain piece of information is PI is significantly context dependent.

Further, in the case of some categories of data, such as internal voice and audio data as well as location data, some parts of it may be sensitive data (in those jurisdictions recognising this category). Because separating this data will be complex, there may be advantages in treating entire categories of data as if they were sensitive.

10.1.2 Err on the side of caution if data might be PI

The federal privacy commissioner's May 2017 Guidelines after *PC v Telstra* (see Appendix A) propose that entities should err on the side of caution where there is a possibility that certain information or data could constitute personal information in certain circumstances.

This advice suggests that most data types associated with C-ITS and AV systems should be treated as if they could be PI, unless there is compelling, reliable and stable evidence to the contrary in all contexts. The alternative, categorising many data types as not PI where there is uncertainty could lead to complaints and distrust, as well as legal risk.

10.1.3 Processing may enable identification and extraction of personal information

Raw sensor data of some kinds might be initially be less capable of contributing to identifiability than where it is put in context with other data, or after it has also been processed and subjected to pattern matching (including speaker or voice recognition, in the case of audio data, or face recognition, in the case of image data).

The use of sophisticated software and big data tools may thus increase the ease of identification or information extraction; in some case this is their purpose. For instance, a combination of internal image and audio data may, when subject to processing, generate a transcript. This capacity will only develop over time, given the intensive investment in improving such processing methods.

Noting this, the contribution of sophisticated pattern recognition and AI software to increasing identifiability, or extraction of further personal information, from a data set or data stream may affect the extent to which C-ITS and AV data are personal information.

10.2 Privacy laws

10.2.1 Absence of privacy laws in some jurisdictions.

Much of the collection or use of C-ITS & AV data will be done by state and territory instrumentalities. The privacy legislation, where it is exists, is broadly similar but some jurisdictions do not have privacy statutes. For instance, South Australia's implementation of privacy and data protection law is found not in a statute but in a cabinet circular, and Western Australia has no privacy law.

State and territory differences create potential inconsistency, complexity and uncertainty for citizens, regulators and industry.

10.3 Surveillance device laws

10.3.1 Surveillance by software that converts a device to do surveillance

As noted by the ALRC, the present set of definitions (one or more of listening device, optical surveillance device, data surveillance device and tracking device – see Appendix E) is not technology neutral, and excludes surveillance implemented by software which turns something that might not be a surveillance device into a device which can be used for surveillance.

Some categories of C-ITS and AV data or data collection systems might fit the existing definition of listening devices, but if implemented purely as software they may not. This creates uncertainty.

10.4 Law enforcement and criminal law

Law enforcement powers to access data under using specific tools such as search warrants and authorisations are broad, generally enabling targeted investigation. However, many of the existing information protection principles related to law enforcement, and law enforcement powers, pre-date the current ability to collect and analyse large data sets. Noting the breadth of information that can be produced by C-ITS and AV technology, there are risks that the law enforcement exception to privacy law may permit mass surveillance without a warrant by allowing law enforcement bulk acquisition or access to these large data sets.

This issue should be subject to consultation, further inquiry and clarification.

10.5 Road and traffic laws

10.5.1 Difference between vehicle types

Passenger vehicles and some light commercial vehicles are treated differently to heavy transport vehicles, with the latter subject to more stringent and comprehensive information collection and disclosure regimes.

10.5.2 Difference between existing purposes and C-ITS and AV system purposes

Road traffic laws, including speeding, CCTV and ANPR already authorise certain targeted collection of data. But the scale and purpose of these data schemes is quite different from that involved in C-ITS and AV systems. Further analysis of the difference between existing road traffic law collection practices and practices that may occur in the future should be considered.

10.6 Other issues

The scope for research use of C-ITS and AV data is unclear. Some research is essential for continued development, but there are potentially a much larger range of entities who may like to do research with these data than just the AV system operators, including potentially government entities and city planning researchers.

Telecoms: the status of location information from various systems is unclear. In most cases it will not be telecommunications metadata, but this may need further examination.

The distinction between 'contents' of a communication and the metadata may also become more indistinct with a greater volume of location information tied to telecommunications networks.

Transparency and access to data: many of the laws considered do not give extensive rights of access to data subjects. This should arguably be reviewed in the context of C-ITS and AV systems, given the larger volumes of often compulsorily collected data, greater scope for use and misuse of the data, and the lowered cost of delivery.

Sensitive information: Data collected in the cabin is particularly likely to become sensitive by context. This requires further review.

APPENDICES

Appendix A – Key court cases

There are few modern Australian cases about privacy or the *Privacy Act 1988* (Cth) because there is still no common law or statutory right to sue for breach of privacy in Australia,[163] and individuals also cannot sue to either enforce their statutory rights under the *Privacy Act*, or to appeal against the merits of the few determinations about a complaint under the Act. The federal Privacy Commissioner cannot be compelled to make a decision about a complaint and rarely does so, and any such determinations are not enforceable without further resort to a tribunal, leaving only a very narrow scope for court appeals on jurisdictional issues.[164] The few cases which emerge are often appeals on jurisdictional points by information holders unsatisfied that one of the rare complaints which results in a determination has turned out adversely, such as *PC v Telstra*.

This is not the case with some state jurisdictions, which enable wider review of decisions, and appeals on merits. *Waters v TFNSW* is an example, further below.

Because the definitions of key terms like 'personal information' are different between the two levels of jurisdiction (except for ACT, which mirrors the Commonwealth – see Appendix B), the use of these decisions to interpret federal law is less certain than it would be if the key terms were identical.

1. *PC v Telstra* – 'About an individual'

Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (19 January 2017) <http://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/full/2017/2017fcafc0004>

This is discussed in section 3.2 Definitions of 'personal information' in statutes, above.

Is information about my car 'about' me if I am in it, but not physically driving?

In *Privacy Commissioner v Telstra*, Telstra succeeded in an appeal against a decision by the privacy commissioner to order them under then National Privacy Principle 6.1 to give a customer his own 'metadata', including Internet Protocol address (IP) and similar technical information.

It turned on the meaning of 'about an individual', and thus whether this technical information, used to identify a device, was 'personal information' under the pre-2014 definition.

Limitations

This case is not necessarily a definitive guide to the meaning of 'personal information' in current or future transport contexts for a number of reasons.

Firstly, the decision notes that it refers to an old now-obsolete version of the *Privacy Act 1988* (Cth) definition of 'personal information', from the version of the Act as it was prior to the coming into force in 2014 of the 2012 amendments. These changed the

[163] See *ABC v Lenah Game Meats* [2001] HCA 63; and *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) 2008 and *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123) 2014, the last of five ALRC papers recommending a privacy tort of some sort (Greg Foyster, 'Australian law and data protection', *The Saturday Paper*, 26 May 2018, citing High Court judge Michael Kirby).
[164] *Privacy Act* 1988 (Cth) section s 52.

definition of personal information by removing a requirement that the person be reasonably identifiable '*from the information'*. The old definition in force in 2013 says:

> ***'personal information*** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, *from the information or opinion*.' (emphasis added)

The case was also about the version of this law prior to the explicit statutory provision that retained telecommunications metadata is 'personal information' (PI) for the purposes of the Privacy Act – inconsistent to what the court found the old version meant.

The note to the current definition of 'personal information' explicitly states that section 187LA of *Telecommunications (Interception and Access) Act 1979* (Cth) 'extends the meaning of personal information to cover information kept under Part 5–1A of that Act'. In other words, the device and network metadata retained by Telstra under the new retention law is defined as 'personal information' by the Act which created the retention regime. This statutory provision applies directly to that data, and to the version of the *Privacy Act* now in force.

This s 187LA amendment to the definition of PI also offers persuasive support for the notion that Parliament has now accepted that telecommunications data and 'metadata' of the sort required to be retained to assist law enforcement and surveillance bodies trying to find and locate individuals, including location data, may be 'personal information'.

Finally, the court's narrow reading of the meaning of 'about' to find that, at that time and in those circumstances, information about an individual excluded certain retained metadata is inconsistent with EU practice. This is significant, since EU privacy law is based on the same 1980 OECD Privacy Guidelines roots as our law, and their definition of 'personal data' is quite close to our definition of PI. By contrast, the fragmented US privacy law is not based on a broad Privacy Principles approach, and its definition of 'personally identifiable information' (PII) is significantly narrower than ours. (This aspect is discussed in more detail in sections 8 and 9.)

Note that this case from the full bench of the Federal Court of Australia arose from an appeal against OAIC's decision in *Ben Grubb and Telstra* [2015] AICmr [35] 1 May 2015. That first instance decision was referred to briefly in section 3.2.2 above for its use by the NSW IPC to help conclude that use of data matching or linking can be taken into account in considering identifiability of certain information.

This case was also discussed at length in *Waters v Transport for NSW*, outlined below.

2. *Waters v Transport for NSW* – 'personal information', 'reasonably necessary to collect'

Waters v Transport for NSW [2018] NSWCATAD 40 (NSW CAT, Administrative and Equal Opportunity Division, McAteer J, 15 February 2018) <https://www.caselaw.nsw.gov.au/decision/5a8351f1e4b074a7c6e1c492>

These proceedings concern whether the requirements of Transport for NSW in respect of electronic (Opal) ticketing for public transport concession entitlement holders contravene an Information Protection Principle (IPP) under the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act). The dominant concern was that the

introduction of electronic ticketing removed the ability of certain concession entitlement holders to travel anonymously under that entitlement, with their movements tracked by the respondent agency (as an arm of the Government), contrary to the privacy protections of citizens under the PPIP Act. One issue was whether the collection of personal information for that purpose is reasonably necessary having regard to the stated purpose that the information is collected.[165]

None of the exemptions in the definition of 'personal information' applied, and the information was found to be PI. Reliance was placed by the government on the cases of *WL v Randwick City Council (No 2)* [2010] NSWADT 84 at [33] and *Office of Finance and Services v APV and APW* [2014] NSWCATAP 88 at [54]-[70] to argue that the raw travel movement data was not personal at the point of collection and hence there was no PI.

The applicant's general grievance was that the change in the policy to require concession holders to register

> 'has introduced an effective form of surveillance over his ingress and egress within the relevant parts of the State by the lack of any equivalent option for anonymous travel. The applicant ties this grievance to various IPPs but predominantly his grievance is that the 'requirement' of collection of his personal information is not reasonably necessary for the unstated purpose of travel on public transport as an eligible Senior. This central argument equates to a breach of IPP 1 and as a result is contrary to the requirements in s 8 of the PPIP Act.'[166]

At issue was whether the routine and automatic collection of travel movement information about identifiable individuals was a contravention of s 8 of the PPIP Act, in that such a collection is not reasonably necessary for the purpose of managing ongoing entitlement (use or disclosure was not at issue). Section 8 provides:

> **8 Collection of personal information for lawful purposes**
>
> (1) A public sector agency must not collect personal information unless:
>
> (a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and
>
> (b) the collection of the information is reasonably necessary for that purpose.
>
> (2) A public sector agency must not collect personal information by any unlawful means. (emphasis added by court)

The tribunal found that 'when one looks to the totality of the complaint, and the fact that it concerns a grievance about the collection of personal information for a purpose that goes beyond the matters raised in the evidence (verification of entitlement and enforcement), then the majority of the respondent's preliminary arguments [that it was not PI] fall away.'[167]

There was extensive analysis of past cases on the question of what constitutes 'personal information' in particular circumstances, although under the NSW definition where the words 'from the information' have not yet been removed, as they have been at federal and ACT level, and has been recommended by NSWLRC. Several of the cases referred to the *PC v Telstra* case, and distinguished it on various grounds, one of them cited with

[165] [2018] NSWCATAD 40, [1].
[166] Ibid, [6].
[167] Ibid [59].

approval saying 'on the assumption that the information refers to the totality of the information requested, then even if a single piece of information is not 'about an individual' it might be about the individual when combined with other information.'[168]

In finding the information was clearly 'about' the applicant, the tribunal said:

> It would appear … the information collected under section 8 was clearly about CNS, and it would also appear (from the evidence given about travel history etc. during the hearing) that the tapping on and off at various locations was information about CNS, as his identity could be ascertained both by combining it with other information (in respect of the respondent seeking a travel history for law enforcement purposes or customer queries), or the customer checking their own travel history seamlessly. In addition (noting the *Telstra* case) for all relevant purposes, especially concerning a mandatorily registered Gold Opal card, the travel information was more about CNS than about the card. There was no purpose attached to the card information (unique to its requirement for registration) **that was not about CNS**.[169]
>
> (emphasis in original)

It also refers to the Guide issued in May 2017 by the Privacy Commissioner after *PC v Telstra*, which notes that 'Information will also be "about" someone where it reveals or conveys something about them – even where the person may not, at first, appear to be a subject matter of the information'.[170] It also encourages entities to err on the side of caution by treating it as PI if there is doubt.

DAB v Byron Shire Council [2017] NSWCATAD 104 was also considered. That case was distinguished because in that case a check of motor vehicle registration number by a smart meter to an offshore server of exempt numbers left records at neither meter nor server that there had been a check. In the absence of logging or other records, there was no way to associate the meter information with the car owner.

The NSW Privacy Commissioner also made submissions about the implications of the Telstra decision, saying 'The network data in Mr Grubb's case may well have been far along the continuum of relevance and proximity, so that they do not trigger the privacy right, but travel history information is especially close and relevant.'[171] She also said, in relation to splitting of data in separate databases,

> 'The fact that the agency stores the information in question in separate databases does not take away the agency ability to bring the data together as it may choose or as it may be required and therefore aggregate it. … Separate storage is more an indication that the agency has recognised its privacy and security obligations **because the information is "personal information" rather than the opposite**.' (emphasis in original)

This assisted the tribunal to find that the travel history as recoded and accessible from the registered Opal card is PI.

There was also extensive analysis of the 'reasonably necessary issue'. The tribunal found that the TFNSW 'collected the personal information of the applicant (through the travel, billing, location) history for a purpose (by the nature of that

---

[168] *CRP v Department of Family and Community Services* [2017] NSWCATAD 164, [76], quoting [63] in *PC v Telstra*.
[169] *Waters v TFNSW*, [67].
[170] 'What is personal information', May 20917, OAIC, <https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information>.
[171] *Waters v TFNSW*, [81].

collection/information) that is not necessary (or reasonably necessary) for ensuring entitlement and enforcement of eligibility for the Gold Seniors Opal card,'[172] and hence ordered that this practice cease. The design of the card was seen as being open to remedial modification to retain necessary cancellation functionality but omit the unnecessary travel history.

3. *R v Gittany* – surveillance using software, rather than a 'device'

   R v Gittany (No 5) [2014] NSWSC 49 (11 February 2014) McCallum J <http://www.austlii.edu.au/au/cases/nsw/NSWSC/2014/49.html>

   NSW Supreme Court described surveillance carried out by the accused that involved the use of software surreptitiously installed onto the mobile telephone and personal computer of his partner.

   This is an example of the factual scenario of a non-'device' method of surveillance, which might escape coverage by surveillance devices law if the person had been charged with this as an offence, since it used neither a 'listening device' nor a 'data surveillance device' per se, but instead converted other devices to have this surveillance function.

   (The main legal focus of the case, and the later cases which cite it, was on the murder conviction. The consideration of the surveillance method was a peripheral feature of the facts.)

[172] Ibid, [172].

Appendix B – 'Personal information'

Table 1 – 'Personal information' definitions in various jurisdictions' privacy legislation

State	Definition
Cth *Privacy Act 1988* (current version)	This definition is similar to that in the ACT, in that the phrase 'from the information or opinion' was removed by amendment. s 6(1) **Interpretation** '"***personal information***" means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not. Note: Section 187LA of the *Telecommunications (Interception and Access) Act 1979* extends the meaning of personal information to cover information kept under Part 5-1A of that Act.'
ACT *Information Privacy Act 2014*	This definition is close to the Commonwealth version, but with the addition of an exclusion to ensure that health information is only covered under another Act. Unlike many other states, it omits the condition 'from the information or opinion'. s 8 '**Meaning of personal information** (1) For this Act, "***personal information***"— (a) means information or an opinion about an identified individual, or an individual who is reasonably identifiable— (i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not; but (b) does not include personal health information about the individual. (2) In this section: "personal health information"—see the *Health Records (Privacy and Access) Act 1997*, dictionary.'
ACT *Health Records (Privacy And Access) Act 1997*	This definition is intended to cover only information related to health services, so it is couched in terms of a consumer, not an individual, and consumer refers to someone who uses a health service or about whom a health record is created. This may exclude it from coverage of many items of personal information that might otherwise be considered personal health information derived from sensors in a C-ITS or AV system context. **Dictionary** "***personal information***", in relation to a *consumer*, means any information, recorded or otherwise, about the consumer where the identity of the consumer is apparent, whether the information is— (a) fact or opinion; or

State	Definition
	(b) true or false. "***personal health information***", of a consumer, means any personal information, whether or not recorded in a health record— (a) relating to the health, an illness or a disability of the consumer; or (b) collected by a health service provider in relation to the health, an illness or a disability of the consumer. "***consumer***" means an *individual who uses, or has used, a health service, or in relation to whom a health record has been created*, and includes— (a) if the consumer is a child or young person—a person with parental responsibility for the consumer; and (b) if the consumer is a legally incompetent person—a guardian of the consumer; and (c) if the consumer has died and there is a legal representative of the deceased consumer—a legal representative of the deceased consumer; and (d) if the consumer has died and there is no legal representative of the deceased consumer—an immediate family member of the deceased consumer.
NSW *Privacy And Personal Information Protection Act 1998*	This starts with the same core definition as Qld and Vic, but with a long list of exclusions, most or all of which do not apply for our purposes; and an inclusive example about physical or biological traits, suggesting biometric information would also be included. S 4 **Definition of "personal information"** '(1) In this Act, **"*personal information*"** means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. (2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics. (3) Personal information does not include any of the following: (a) information about an individual who has been dead for more than 30 years, (b) information about an individual that is contained in a publicly available publication, (c) information about a witness who is included in a witness protection program under the *Witness Protection Act 1995* or who is subject to other witness protection arrangements made under an Act, (d) information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth [should be read to also apply to this Act's replacement, TIAA], (e) information about an individual that is contained in a public interest disclosure within the meaning of the *Public Interest Disclosures Act 1994* , or that has been collected in the course of an investigation arising out of a public interest disclosure, (f) information about an individual arising out of, or in connection with, an authorised operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*, (g) information about an individual arising out of a Royal Commission or Special Commission of Inquiry,

State	Definition
	(h) information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990*, (i) information about an individual that is contained in Cabinet information or Executive Council information under the *Government Information (Public Access) Act 2009*, (j) information or an opinion about an individual's suitability for appointment or employment as a public sector official, (ja) information about an individual that is obtained about an individual under Chapter 8 (Adoption information) of the *Adoption Act 2000*, (k) information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations for the purposes of this subsection. (4) For the purposes of this Act, personal information is **"held"** by a public sector agency if: (a) the agency is in possession or control of the information, or (b) the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement, or (c) the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998* . (5) For the purposes of this Act, personal information is not **"collected"** by a public sector agency if the receipt of the information by the agency is unsolicited.'
NT s 4A *Information Act*	This is superficially different in limiting the scope of PI to '*government* information' only. See discussion in section 3.2. It also, like the current Commonwealth and ACT definitions, omits the extra condition that 'reasonably identifiable' be assessed '*from the information'*. **Personal information** '(1) Government information that discloses a person's identity or from which a person's identity is reasonably ascertainable is ***personal information***.' [subsections (2) and (3) exclude certain information about a person having acted in an official capacity – not relevant here.]
Queensland s 12 *Information Privacy Act 2009*	The emphasized last phrase was removed from the Cth Act by amendment passed in 2012. Its presence narrows the scope a bit, although guidance from the federal privacy commissioner about the old version (the current Qld one) suggests that information from external sources could still be taken into account in assessing whether their identify could be reasonably ascertained. It is unlikely there is much significance in the difference between 'identify is reasonably ascertained' and 'reasonably identifiable'. ' **'"Personal information"** is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, *from the information or opinion*.' (emphasis added)
SA Cabinet Circular	This is differently constructed but broadly similar to NSW, Qld and Vic. It adds in the 'natural person', and the concept of their affairs, and uses the term 'relating to' not 'about'. Note that this is not in an Act.

State	Definition
12 of 2016, cl 3	'"**personal information**" means information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion.'
Tasmania s 3 *Personal Information Protection Act 2004*	This uses a similar core formulation to NSW, Qld and Vic, but omits reference to truth or not, and includes those dead for less than 25 years. The differences are not critical. '"***personal information"*** means any information or opinion in any recorded format about an individual – (a) whose identity is apparent or is reasonably ascertainable from the information or opinion; and (b) who is alive or has not been dead for more than 25 years'
Victoria s 3 *Privacy and Data Protection Act 2014*	This is like the Queensland definition in retaining the additional condition about 'from the information'. "***personal information***" means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the *Health Records Act 2001* applies.
WA *FOI Act 1992* - Glossary	This is not in a privacy statute, but the closest WA has to one. The core definition is similar to NSW and Qld etc, but explicitly includes the dead, and also adds that individuals can be identifiable not only from that information but from 'an identification number or other identifying particular' – presumably different to the information. This alternative might extend to an 'identifying particular' embedded in a device, though the examples given in the provision do not include this approach. They do give biometric examples. "***personal information"*** means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead — (a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or (b) who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample"

Table 2. 'Sensitive information' about a person – compare definitions, and principles about collection and use in privacy legislation

Jurisd.	"Sensitive information"	Collection principle	Use and Disclosure Principles	
Cth S 6	… means (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates. [(b)-(d) means health, genetic and biometric information is sensitive even if it is not PI, in Cth]	**APP 3--collection of solicited personal information** **Personal information other than sensitive information** 3.1 If an APP entity is an agency, the entity must not collect personal information (other than **sensitive** information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. 3.2 If an APP entity is an organisation, the entity must not collect personal information (other than **sensitive** information) unless the information is reasonably necessary for one or more of the entity's functions or activities. **Sensitive information** 3.3 An APP entity must not collect **sensitive** information about an individual unless: (a) the individual consents to the collection of the information and: (i) if the entity is an agency--the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or (ii) if the entity is an organisation--the information is reasonably necessary for one or more of the entity's functions or activities; or (b) subclause 3.4 applies in relation to the information. 3.4 This subclause applies in relation to **sensitive** information about an individual if: (a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or (b) a permitted general situation exists in relation to the collection of the information by the APP entity; or (c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or (d) the APP entity is an enforcement body and the entity reasonably believes that: (i) if the entity is the Immigration Department--the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or (ii) otherwise--the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or (e) the APP entity is a non-profit organisation and both of the following apply: (i) the information relates to the activities of the organisation; (ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities..	**APP 6--use or disclosure of personal information** 6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless: (a) the individual has consented to the use or disclosure of the information; or (b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information. 6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if: (a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is: (i) if the information is **sensitive** information -- directly related to the primary purpose; or (ii) if the information **is not sensitive** information--related to the primary purpose; or (b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or (c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or (d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or (e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body. [– APP 6.3 is about certain disclosures of biometric information by an agency to an enforcement body under OAIC guidelines] [– TPP 6.2(a)(i) is the main variant of the standard 'directly' related rule about use of SI for a secondary	

Jurisd.	"Sensitive information"	Collection principle	Use and Disclosure Principles	
			purpose]	
ACT IPA	… in relation to an individual, means personal information that is— (a) about the individual's— (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; or (b) genetic information about the individual; or (c) biometric information about the individual that is to be used for the purpose of automated biometric verification or biometric identification; or (d) a biometric template that relates to the individual. [(b)-(d) means genetic and biometric information is sensitive even if it is not PI, in ACT. Health information is excluded and covered by *Health Records (privacy and Access) Act 1997,* so this is the same as the Cth definition except for health info]	**TPP 3—collection of solicited personal information** **Personal information other than sensitive information** 3.1 A public sector agency must not collect personal information (**other than sensitive** information) unless the information is reasonably necessary for, or directly related to, 1 or more of the agency's functions or activities. Note The equivalent provision in the Commonwealth APPs includes a provision applying to certain private sector entities (see Commonwealth APP 3, s 3.2). **Sensitive information** 3.3 A public sector agency must not collect **sensitive** information about an individual unless— (a) the individual consents to the collection of the information and the information is reasonably necessary for, or directly related to, 1 or more of the agency's functions or activities; or (b) TPP 3.4 applies in relation to the information. 3.4 This subsection applies in relation to **sensitive** information about an individual if— (a) the collection of the information is required or authorised by or under an Australian law or a court or tribunal order; or (b) a permitted general situation exists in relation to the collection of the information by the public sector agency; or (d) the public sector agency is an enforcement body and the agency reasonably believes that the collection of the information is reasonably necessary for, or directly related to, 1 or more of the agency's functions or activities.	**TPP 6—use or disclosure of personal information** **Use or disclosure** 6.1 If a public sector agency holds personal information about an individual that was collected for a particular purpose (the primary purpose), the agency must not use or disclose the information for another purpose (the "secondary purpose") unless— (a) the individual has consented to the use or disclosure of the information; or (b) TPP 6.2 or TPP 6.3 applies in relation to the use or disclosure of the information. 6.2 This subsection applies in relation to the use or disclosure of personal information about an individual if— (a) the individual would reasonably expect the public sector agency to use or disclose the information for the secondary purpose and the secondary purpose is— (i) if the information is **sensitive** information—directly related to the primary purpose; or (ii) if the information is **not sensitive** information—related to the primary purpose; or [(b), (c) and (e) list of other grounds for use for a secondary purpose] [– TPP 6.2(a)(i) is a variant of the standard 'directly' related rule about use of SI for a secondary purpose]	
NSW	[SI not mentioned in *PPIPA,* nor in *HRIPA* covering health info]	-	-	
NT s 4	… means (a) personal information about: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or	**IPP 1 Collection** [appears to apply to collection of PI only; IPP 10 applies to collection of sensitive information] **IPP 10 Sensitive information** 10.1 A public sector organisation must not collect **sensitive** information about an individual unless:	**IPP 2.1** A public sector organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose for collecting it unless one or more of the following apply: (a) if the information is **sensitive** information: (i) the secondary purpose is directly related to the	

Jurisd.	"Sensitive information"	Collection principle	Use and Disclosure Principles	
	(v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) a criminal record; or (b) health information. [(b) means health information is sensitive even if it is not PI, in NT. Genetic and biometric are not covered.]	(a) the individual consents to the collection; or (b) the organisation is authorised or required by law to collect the information; or (c) the individual is: (i) physically or legally incapable of giving consent to the collection; or (ii) physically unable to communicate his or her consent to the collection; and collecting the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another individual; or (d) collecting the information is necessary to establish, exercise or defend a legal or equitable claim. 10.2 Despite IPP 10.1, a public sector organisation may collect **sensitive** information about an individual if: (a) the collection: (i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or (ii) is of information relating to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services; and (b) there is no other reasonably practicable alternative to collecting the information for that purpose; and (c) it is impracticable for the organisation to seek the individual's consent to the collection.	primary purpose; and (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; (b) if the information is **not sensitive** information: (i) the secondary purpose is related to the primary purpose; and (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; [(c)–(i) list of other grounds to use for secondary purpose] [– IPP 2(1)(a) is standard 'directly' related rule]	
Qld	... about an individual, for the NPPs, means— (a) personal information about the individual that includes any of the following— (i) the individual's racial or ethnic origin; (ii) the individual's political opinions; (iii) the individual's membership of a political association; (iv) the individual's religious beliefs or affiliations; (v) the individual's philosophical beliefs; (vi) the individual's membership of a professional or trade association; (vii) the individual's membership of a trade union;	**NPP 9—SENSITIVE INFORMATION** (1) A health agency must not collect **sensitive** information about an individual (the "relevant individual") unless— (a) the relevant individual has consented; or (b) the collection is required by law; or (c) the collection is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of an individual, and the relevant individual— (i) is physically or legally incapable of giving consent to the collection; or (ii) physically can not communicate consent to the collection; or (d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim; or (e) the information is a family medical history, social medical history or other relevant information about any individual, that is collected for the purpose of providing any person, whether or not the relevant individual, with a health service, and is collected by a health agency from— [(i)–(ix) list of permitted sources for this sort of information]	**NPP 2—LIMITS ON USE OR DISCLOSURE OF PERSONAL INFORMATION** (1) A health agency must not use or disclose personal information about an individual for a purpose (the "secondary purpose") other than the primary purpose of collection unless— (a) both of the following apply— (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is **sensitive** information, directly related to the primary purpose of collection; (ii) the individual would reasonably expect the health agency to use or disclose the information for the secondary purpose; or [– (b)– (g) other grounds to use for secondary purpose]	

Jurisd.	"Sensitive information"	Collection principle	Use and Disclosure Principles	
	(viii) the individual's sexual preferences or practices; (ix) the individual's criminal record; or (b) information that is health information about the individual for the NPPs. [(b) means health information is sensitive even if it is not PI, in Qld. Genetic and biometric are not covered.]	[(2)-(4) list of other grounds and conditions for collecting sensitive information for certain purposes] [–no mention of sensitive information in NPP 1 covering ordinary collection, so this 'sensitive' collection principle only applies to health agency collection]	[(2)–(4) list of other collection rules] (5) Despite subsection (1) , a health agency may use an individual's personal information that is **not sensitive** information for a commercial purpose involving the health agency's marketing of anything to the individual, but only if— [list of requirements for use for marketing] [– NPP 2(1) is the standard 'directly' related rule; – NPP 2(5) excludes use of sensitive info from health agency marketing]	
SA	[no Act, SI not mentioned in cabinet minute**.]**	-	-	
Tas	… means – (a) personal information or an opinion relating to personal information about an individual's – (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) criminal record; and (b) health information about an individual [(b) means health information is sensitive even if it is not PI, in Tas. Genetic and biometric are not covered.]	**PIPP 1 Collection** [– presumably only covers PI, not sensitive PI] **PIPP 10. Sensitive information** (1) A personal information custodian must not collect **sensitive** information about an individual unless – (a) the individual has consented; or (b) the collection is required or permitted by law; or (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual and the individual to whom the information relates – (i) is physically or legally incapable of giving consent to the collection; or (ii) physically cannot communicate consent to the collection; or (iii) is subject to a guardianship order under the Guardianship and Administration Act 1995 or an assessment order or treatment order under the Mental Health Act 2013 ; or (d) the information is collected in the course of the activities of a non-profit personal information custodian that has only racial, ethnic, political, religious, philosophical, professional, trade or trade union aims and – (i) the information relates solely to the members of that personal information custodian or to individuals who have regular contact with it in connection with its activities; and (ii) at or before the time of collection, the personal information custodian undertakes to the individual to whom the information relates that it will not disclose the information without the individual's consent; or (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim; or	**PIPP 2. Use and disclosure** (1) A personal information custodian must not use or disclose personal information about an individual for a purpose other than the purpose for which it was collected unless – (a) both of the following apply: (i) that purpose is related to the primary purpose and, if the personal information is **sensitive** information, that information is directly related to the primary purpose; (ii) the individual would reasonably expect the personal information custodian to use or disclose the information for that purpose; or [(b)–(k) list other grounds for use for secondary purpose] [– PIPP 2 (a) is the standard 'directly' related rule]	

Jurisd.	"Sensitive information"	Collection principle	Use and Disclosure Principles	
		(f) subclause (2) , (3) , (4) or (6) applies. (2) A personal information custodian may collect **sensitive** information about an individual if – (a) either of the following applies: (i) the collection is necessary for research or the compilation or analysis of statistics in the public interest and any resulting publication does not identify the individual; (ii) the information relates to an individual's racial or ethnic origin and is collected for the purpose of welfare or educational services funded by government; and (b) there is no reasonably practicable alternative to collecting the information for a purpose referred to in paragraph (a) ; and (c) it is impracticable for the personal information custodian to seek the individual's consent to the collection. **(3)** A personal information custodian may collect **sensitive** information that is health information about an individual if – (a) the information is necessary to provide a health service to the individual; and (b) the information is collected – (i) as required by law, other than this Act; or (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the personal information custodian. **(4)** A personal information custodian may collect **sensitive** information that is health information about an individual if – (a) the collection is necessary for any of the following purposes: (i) research relevant to public health or public safety; (ii) the compilation or analysis of statistics relevant to public health or public safety; (iii) the management, funding or monitoring of a health service; and (b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and (c) it is impracticable for the personal information custodian to seek the individual's consent to the collection; and (d) the information is collected – (i) as required by law, other than this Act; or (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the personal information custodian. **(5)** If a personal information custodian collects **sensitive** information that is		

Jurisd.	"Sensitive information"	Collection principle	Use and Disclosure Principles	
		health information about an individual in accordance with subclause (4) , it must take reasonable steps to permanently de-identify the information before disclosing it. (6) A personal information custodian may collect sensitive information that is health information from an individual about another person without the consent of that other person, or without complying with clause 1(5) , if both the following apply: (a) the collection is necessary for the provision of any health service provided to the individual; (b) the information is relevant to the social or family history of the individual.		
Vic	~ means information or an opinion about an individual's— (a) racial or ethnic origin; or (b) political opinions; or (c) membership of a political association; or (d) religious beliefs or affiliations; or (e) philosophical beliefs; or (f) membership of a professional or trade association; or (g) membership of a trade union; or (h) sexual preferences or practices; or (i) criminal record— that is also personal information; [–SI is a true subset of PI in Vic alone. SI does not mention health or medical info, which is excluded from PI but is covered by *Health Records Act*. Genetic and biometric are not covered as SI.]	**IPP 1 Collection** [– presumably only covers PI, not sensitive PI] **IPP 10— Sensitive Information** **10.1** An organisation must not collect sensitive information about an individual unless— (a) the individual has consented; or (b) the collection is required or authorised under law; or (c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns— (i) is physically or legally incapable of giving consent to the collection; or (ii) physically cannot communicate consent to the collection; or (d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim. **10.2** Despite IPP 10.1, an organisation may collect sensitive information about an individual if— (a) the collection— (i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or (ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and (b) there is no reasonably practicable alternative to collecting the information for that purpose; and (c) it is impracticable for the organisation to seek the individual's consent to the collection.	**IPP 2—Use and Disclosure** **2.1** An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless— (a) both of the following apply— (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or [– (b)–(h) list of other grounds for use for secondary purpose] [– IPP 2(a) is a minor variant of the standard 'directly' related rule]	
WA	[– no Privacy Act, SI not in FOIA.]	-	-	

Appendix C – Privacy principles

Table 1. Privacy principles compared

While there are common themes in privacy principles in Australian law, their names, structure and details vary. This is only a sample. Victoria also has Health Privacy Principles, different from those in NSW. SA has *Cabinet Instruction* not an Act, 10 principles are untitled except headings. WA does not have a privacy act or privacy principles.

Cth APPs	ACT TPPs	NSW IPPs	NSW Health HPPs	NT (Tas,* Vic) IPPs	Qld IPPs & NPPs**	SA IPPs
Australian Privacy Principles, Sched 1	Territory Privacy Principles, Sched 1	Information Protection Principles, Pt 2 Div 1	Health Privacy Principles, Sched 1, HRIPA	Information Privacy Principles, Sched 2	Information Privacy Principles, Sched 3	Information Privacy Principles, cl 4
APP 1--open and transparent management of personal information APP 2--anonymity and pseudonymity APP 3--collection of solicited personal information APP 4--dealing with unsolicited personal information APP 5--notification of the collection of personal information APP 6--use or disclosure of personal information APP 7--direct marketing APP 8--cross-border disclosure of personal information APP 9--adoption, use or disclosure of government related identifiers APP 10--quality of personal information APP 11--security of personal information APP 12--access to personal information APP 13– correction of personal information	TPP 1—open and transparent management of personal information TPP 2—anonymity and pseudonymity TPP 3—collection of solicited personal information TPP 4—dealing with unsolicited personal information TPP 5—notification of the collection of personal information TPP 6—use or disclosure of personal information *[no APP 7 equiv.]* TPP 8—cross-border disclosure of personal information *[no APP 9 equiv.]* TPP 10–quality of personal information TPP 11–security of personal information TPP 12– access to personal information TPP 13–correction of personal information.	s 8 Collection of personal information for lawful purposes s 9 Collection of personal information directly from individual s 10 Requirements when collecting personal information s 11 Other requirements relating to collection of personal information s 12 Retention and security of personal information s 13 Information about personal information held by agencies s 14 Access to personal information held by agencies s 15 Alteration of personal information s 16 Agency must check accuracy of personal information before use s 17 Limits on use of personal information s 18 Limits on disclosure of personal information s 19 Special restrictions on disclosure of personal information	HPP 1 – purposes of collection of health information HPP 2 –information must be relevant, not excessive, accurate and not intrusive HPP 3 – collection to be from individual concerned HPP 4–individual to be made aware of certain matters HPP 5–retention and security HPP 6–information about health information held by organisations HPP –7 access to health information HPP 8–amendment of health information HPP 9–accuracy HPP 10–limits on use of health information Hpp 11–limits on disclosure of health information HPP 12–identifiers HPP 13–anonymity HPP 14–transborder data flows and data flow to Cth agencies HPP 15–linkage of health records	IPP 1 –Collection IPP 2–Use and disclosure IPP 3–Data quality IPP 4–Data security IPP 5–Openness IPP 6–Access and correction IPP 7–Identifiers IPP 8–Anonymity IPP 9–Transborder data flows (Tas: Disclosure of information outside Tasmania) IPP 10–Sensitive information (*Tas PIPPs: 'Personal Information Protection Principles')	IPP 1—Collection Of Personal Information (Lawful And Fair) IPP 2—Collection Of Personal Information (Requested From Individual) IPP 3—Collection Of Personal Information (Relevance Etc.) IPP 4—Storage And Security Of Personal Information IPP 5—Providing Information About Documents Containing Personal Information IPP 6—Access To Documents Containing Personal Information IPP 7—Amendment Of Documents Containing Personal Information IPP 8—Checking Of Accuracy Etc. Of Personal Information Before Use By Agency IPP 9—Use Of Personal Information Only For Relevant Purpose IPP 10—Limits On Use Of Personal Information IPP 11—Limits On Disclosure ** NPPs are used for health, copied from old Cth NPPs.	Collection of Personal Information [3 short untitled principles unlawful or unfair means, notification, accuracy etc.] Storage of Personal Information [1 principle – secure, not misused.] Access to Records of Personal Information [1 principle – access under FOIA] Correction of Personal Information [1 principle – correct if inaccurate etc.] Use of Personal Information [3 principles – use only if relevant, use for secondary purpose, keep accurate etc.] Disclosure of Personal Information [1 long principle – disclosure for secondary purpose]

Table 2. HVNL Intelligent Access Program equivalents of privacy principles

The items in bold below implement forms of protections using the language found in privacy principles. These provisions and obligations are mirrored in Part 7.5 for Transport Certification Australia, and in the Queensland equivalent *Heavy Vehicle National Law 2012,* Schedule, which is the national model.

Heavy Vehicle National Law (NSW), 42a of 2013

PART 7.4 - POWERS, DUTIES AND OBLIGATIONS OF INTELLIGENT ACCESS PROGRAM SERVICE PROVIDERS

409 Powers to collect and hold intelligent access program information

410 Collecting intelligent access program information

411 Keeping records of intelligent access program information collected

412 Protecting intelligent access program information

413 Making individuals aware of personal information held

414 Giving individuals access to their personal information

415 Correcting errors etc.

416 General restriction on use and disclosure of intelligent access program information

417 Giving intelligent access program auditor access to records

418 Powers to use and disclose intelligent access program information

419 Keeping record of use or disclosure of intelligent access program information

420 Keeping noncompliance report etc.

421 Destroying intelligent access program information etc.

422 Reporting relevant contraventions to Regulator

423 Reporting tampering or suspected tampering with approved intelligent transport system

424 Restriction on disclosing information about tampering or suspected tampering with approved intelligent transport system

In recognition of the partial exclusion from general privacy laws, section 427 of the NSW and Queensland versions of the HVNL also create a remarkable, criminally sanctioned version of a collection privacy principle in respect only of 'intelligent access program information'. There are maximum $6,000 fines for breaching prohibitions on collection which intrudes 'to an unreasonable extent' on the privacy of the individual, or which are not necessary for the purpose, excessive or not necessary, complete or up to date.

There are other fines for similar rudimentary de facto privacy principles (so described as such) to support the purpose of 'appropriate collection, keeping and handling of intelligent access program information' in s 400(1)(b):

(a) allowing entities to collect, hold, use and disclose intelligent access program information for only limited purposes and subject to restrictions; and

(b) requiring entities with monitoring or auditing functions to ensure intelligent access program information collected is accurate, complete and up to date; and

(c) requiring entities who collect intelligent access program information to protect the information and destroy it when it is no longer required by the entities; and

(d) providing for persons about whom an entity holds personal information to have access to the information and have it corrected in appropriate circumstances.

These protective measures are both much simpler and more strongly enforceable than other general privacy principles in Australia.[173] This may be in recognition for the intensive surveillance regime for heavy vehicle drivers using the 'intelligent access program information'. That heavy vehicle intelligent access program is peripheral to the focus of this report but it illustrates one potential application of intensive road data collection to enforce driver and vehicle compliance, and a model of potentially quite rigorous protection of personal information around the core of an intrinsically intensive data program with a limited role for voluntary consent. It is also interesting for using somewhat differently framed rules many of which are nevertheless close approximations of a privacy principles model.

[173] Most breaches of privacy principles and data protection rules are civil and administrative matters, rather the criminal offences with a $6,000 fine.

Appendix D – Exemptions from privacy principles, including for enforcement, law enforcement and investigation purposes

Table 1. Provisions implementing enforcement, law enforcement, or intelligence exemptions

Jurisdiction	Exemptions	Entity definitions
		[Note that law enforcement functions are not defined apart from the list of entities included]
Cth *Privacy Act 1988* Australian Privacy Principles	**APP 3 collection of solicited personal information** [APP 3.1 and 3.2 only require, as justification for collection by an 'APP entity' agency or organisation, that non-sensitive personal information be reasonably necessary for – or directly related to, in the case of an agency – one or more of their functions or activities. It is quite permissive cf. APP 3.3, which deals with sensitive information.] *[emphasis added, paraphrased]* APP 3.3 An APP must not collect ***sensitive*** information about an individual unless— (a) the individual ***consents*** to the collection of the information *and* [the information is reasonably necessary for – or directly related to, in the case of an agency – one or more of the agency's functions or activities]; or (b) *APP 3.4* applies in relation to the information. 3.4 This subsection applies in relation to sensitive information about an individual if – (a) the collection of the information is ***required or authorised*** *by or under an Australian law* or a court or tribunal order; or (b) [*Permitted General Situation* exists: see s 16A, esp. items 1 and 2, where entity reasonably believes collection, use or disclosure of PI is necessary to lessen or prevent ***serious threat to life, health or safety of an individual, or public health or safety*** and it is impractical to obtain consent; or to take action about ***suspected unlawful activity or serious misconduct*** related to its functions] (c) [Permitted Health Situation: see s 16B – not relevant here?]; or (d) the APP entity is an ***enforcement body*** and the entity reasonably believes that [the collection of the information is *reasonably necessary for, or directly related to, one or more of the entity's functions or activities* – or if it is the Immigration Department, to enforcement related activities	S 6 "***enforcement body***"means: (a) Australian Federal Police; or (aa) Integrity Commissioner; or (b) ACC; or (ca) Immigration Department; or (d) Australian Prudential Regulation Authority; or (e) Australian Securities and Investments Commission; or (ea) Office of the Director of Public Prosecutions, or a similar body established under a law of a State or Territory; or (f) another agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or (g) another agency, to the extent that it is responsible for administering a law relating to the protection of the public revenue; or (h) a police force or service of a State or a Territory; or (i) New South Wales Crime Commission; or (j) Independent Commission Against Corruption of New South Wales; or (k) Law Enforcement Conduct Commission of New South Wales; or (ka) the Independent Broad-based Anti-corruption Commission of Victoria; or (l) Crime and Corruption Commission of Queensland; or (la) Corruption and Crime Commission of Western Australia; or (lb) Independent Commissioner Against Corruption of South Australia; or (m) another prescribed authority or body that is established under a law of a State or Territory to conduct criminal investigations or inquiries; or (n) a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or (o) a State or Territory authority, to the extent that it is responsible for administering a law relating to the protection of the public revenue.

Jurisdiction	Exemptions	Entity definitions
	conducted by or on its behalf.] (e) [entity is a non-profit – not relevant here?] **APP 6 use or disclosure of personal information** APP 6.1 [an APP entity can use or disclose personal information for a purpose secondary to the primary purpose of collection if the individual ***consents***, or if the entity reasonably believes 'that the use or disclosure of the information is reasonably necessary for one or more ***enforcement related activities*** conducted by, or on behalf of, an ***enforcement body***" (APP 6.2), or if it is ***biometric information*** *or templates*, the recipient is an *enforcement body* and the discloser is not, and disclosure complies with Commissioner's guidelines. (APP 6.3)] S 6 "***enforcement related activity***" means: (a) the prevention, detection, investigation, prosecution or punishment of: (i) criminal offences; or (ii) breaches of a law imposing a penalty or sanction; or (b) the conduct of surveillance activities, intelligence gathering activities or monitoring activities; or (c) the conduct of protective or custodial activities; or (d) the enforcement of laws relating to the confiscation of the proceeds of crime; or (e) the protection of the public revenue; or (f) the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations; or (g) the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders.	
ACT *Information Privacy Act 2014* Territory privacy principles	TPP 3 – **Collection of solicited personal information** [this replicates most of APP 3.1, 3.2, 3.3 and 3.4 mentioned above under Cth, above, with the differences being 'public sector agency' instead of 'APP entity', and omission of inapplicable provisions about certain privacy sector entities, Immigration Department, and non-profits.] TPP 6—**use or disclosure of personal information** [this similarly replicates most of APP 6.1, 6.2 and 6.3, mentioned above under Cth] s 25 **Exempt acts or practices** (1) This Act does not apply to the following acts and practices: [(a)–(d) exclusions for certain acts of a Minister, ACT court, Office of Legislative	S 25 (2) for the purposes of this section: "***Commonwealth enforcement or intelligence body***" means … : [(a)–(h) a Commonwealth intelligence body; Office of National Assessments; Defence Intelligence Organisation; Defence Imagery and Geospatial Organisation; staff or commissioner of Australian Commission for Law Enforcement Integrity; Australian Crime Commission.] "***Commonwealth intelligence body***" means … : [(a)-(d) [Australian Security Intelligence Organisation; Australian Secret Intelligence Service; Defence Signals Directorate.] *(emphasis added, some provisions truncated)*

Jurisdiction	Exemptions	Entity definitions
	Assembly, officers of Assembly]; (e) an act done, or a practice engaged in, by a public sector agency in relation to information that is taken to be contrary to the public interest to disclose under the FOI Act, schedule 1; (f) an act done, or a practice engaged in, by a public sector agency in relation *to a record that has originated with, or has been received from, a Commonwealth enforcement or intelligence body*; (g) an act done, or a practice engaged in, by a public sector agency that involves the *disclosure of personal information to a Commonwealth intelligence body* if the body, in connection with its functions, requests that the agency disclose the personal information and— (i) the disclosure is made to an officer or employee of the Commonwealth intelligence body authorised in writing by the head (however described) of the body to receive the disclosure; and (ii) the officer or employee certifies in writing that the disclosure is connected with the performance of the body's functions; (h) for an agency prescribed by regulation—an act done, or a practice engaged in, by the agency in relation to a matter prescribed by regulation.	
NSW *Privacy And Personal Information Protection Act 1998*	S 23 **Exemptions relating to law enforcement and related matters** (1) A law enforcement agency is not required to comply with section 9 if compliance by the agency would prejudice the agency's law enforcement functions. (2) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 9 if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal. (3) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 10 if the information concerned is collected for law enforcement purposes. However, this subsection does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence. (4) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 17 if the use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary for law enforcement purposes or for the protection of the public	S 3 "***law enforcement agency***" means any of the following: (a) NSW Police Force, or the police force of another State or a Territory, (b) New South Wales Crime Commission, (c) Australian Federal Police, (d) Australian Crime Commission, (e) Director of Public Prosecutions of New South Wales, of another State or a Territory, or of the Commonwealth, (f) Department of Justice, (g1) Office of the Sheriff of New South Wales, (h) a person or body prescribed by the regulations for the purposes of this definition.

Jurisdiction	Exemptions	Entity definitions
	revenue. (5) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 18 if the disclosure of the information concerned: (a) is made in connection with proceedings for an offence or for law enforcement purposes (including the exercising of functions under or in connection with the *Confiscation of Proceeds of Crime Act 1989* or the *Criminal Assets Recovery Act 1990*), or (b) is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or (c) is authorised or required by subpoena or by search warrant or other statutory instrument, or (d) is reasonably necessary: (i) for the protection of the public revenue, or (ii) in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed. (6) Nothing in subsection (5) requires a public sector agency to disclose personal information to another person or body if the agency is entitled to refuse to disclose the information in the absence of a subpoena, warrant or other lawful requirement. (6A) A public sector agency is not required to comply with the information protection principles with respect to the collection, use or disclosure of personal information if: (a) the agency is providing the information to another public sector agency or the agency is being provided with the information by another public sector agency, and (b) the collection, use or disclosure of the information is reasonably necessary for law enforcement purposes. (7) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 19 if the disclosure of the information concerned is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed. (8) In this section: (a) a reference to law enforcement purposes includes a reference to law	

Jurisdiction	Exemptions	Entity definitions
	enforcement purposes of another State or a Territory or the Commonwealth, and (b) a reference to an offence includes a reference to an offence against a law of another State or a Territory or the Commonwealth, and (c) a reference to the protection of the public revenue includes a reference to the protection of the public revenue of another State or a Territory or the Commonwealth. *See also:* s 23A **Exemptions relating to ASIO** [public sector agencies not required to comply with ss 13, 14 or 18 in certain circumstances – not quoted here] S 24 **Exemptions relating to investigative agencies** (1) An investigative agency is not required to comply with section 9, 10, 13, 14, 15, 18 or 19 (1) if compliance with those sections might detrimentally affect (or prevent the proper exercise of) the agency's complaint handling functions or any of its investigative functions. (2) An investigative agency is not required to comply with section 17 if the use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary in order to enable the agency to exercise its complaint handling functions or any of its investigative functions. (3) An investigative agency is not required to comply with section 18 or 19 (1) if the information concerned is disclosed to another investigative agency. (4) A public sector agency (whether or not an investigative agency) is not required to comply with section 18 or 19 (1) if non-compliance is reasonably necessary to assist another public sector agency that is an investigative agency in exercising its investigative functions. (5) An investigative agency is not required to comply with section 18 if: (a) the information concerned is disclosed to a complainant, and (b) the disclosure is reasonably necessary for the purpose of: (i) reporting the progress of an investigation into the complaint made by the complainant, or (ii) providing the complainant with advice as to the outcome of the complaint or any action taken as a result of the complaint. (6) The exemptions provided by subsections (1)-(5) extend to: (a) any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or	"***investigative agency***" means: (a) any of the following: (i) Ombudsman's Office, (ii) Independent Commission Against Corruption, (iii) Inspector of the Independent Commission Against Corruption, (iv) Law Enforcement Conduct Commission, (v) Inspector of the Law Enforcement Conduct Commission and any staff of the Inspector, (vi) Health Care Complaints Commission, (vii) Office of the Legal Services Commissioner, (viii) a person or body prescribed by the regulations for the purposes of this definition, or (b) any other public sector agency with investigative functions if: (i) those functions are exercisable under the authority of an Act or statutory rule (or where that authority is necessarily implied or reasonably contemplated under an Act or statutory rule), and (ii) the exercise of those functions may result in the agency taking or instituting disciplinary, criminal or other formal action or proceedings against a person or body under investigation, or (c) a public sector agency conducting an investigation for or on behalf of an agency referred to in paragraph (a) or (b).

Jurisdiction	Exemptions	Entity definitions
	made to an investigative agency , or that has been referred from or made by an investigative agency , and (b) the Office of Local Government, or any person employed in that Office, who is investigating or otherwise handling (formally or informally) a complaint or other matter even though it is or may be the subject of a right of appeal conferred by or under an Act. (7) The Ombudsman's Office is not required to comply with section 9 or 10. (8) An investigative agency is not required to comply with section 12 (a). See also: more in Part 2 Div 3 **Specific Exemptions from Principles** [emphasis added] S 25 Exemptions where non-compliance is ***lawfully authorised or required*** S 26 Other exemptions where non-compliance would ***benefit the individual concerned*** S 27 ***Specific exemptions*** (ICAC, ICAC Inspector and Inspector's staff, NSW Police Force, LECC, Inspector of LECC and Inspector's staff and NSW Crime Commission) S 27A Exemptions relating to ***information exchanges between public sector agencies*** S 27B Exemptions relating to ***research*** S 27C Exemptions relating to credit information S 28 Other exemptions	
NT *Information Act*	s 70 **Law enforcement agencies** A law enforcement agency is not required to comply with an IPP if the agency believes on reasonable grounds that non-compliance is necessary for one or more of its or another law enforcement agency's functions, including the following: (a) to prevent, detect, investigate, prosecute or punish the commission of an offence against a law of the Territory or any other offence or breach of a law imposing a penalty or sanction for a breach; (b) to manage property seized or restrained under laws relating to the confiscation of the proceeds of crime or the enforcement of those laws or orders under those laws; (c) to execute or implement an order or decision of a court or tribunal, including to execute warrants, to provide correctional services and to make decisions relating to the release of a person from lawful custody;	Law enforcement agency is not defined.

Jurisdiction	Exemptions	Entity definitions
	(d) to locate missing persons and next of kin; (e) to provide services in emergency and disaster situations; (f) if the agency is the Police Force of the Northern Territory – its community policing function.	
Qld *Information Privacy Act 2009*	S 29 **Special provision for law enforcement agencies** (1) A law enforcement agency is not subject to IPP 2, 3, 9, 10 or 11, but only if the law enforcement agency is satisfied on reasonable grounds that noncompliance with the IPP is necessary for— (a) if the enforcement agency is the Queensland Police Service—the performance of its activities related to the enforcement of laws; or (b) if the enforcement agency is the Crime and Corruption Commission—the performance of its activities related to the enforcement of laws and its intelligence functions; or (c) if the enforcement agency is the community safety department—the containment, supervision and rehabilitation of offenders under the *Corrective Services Act 2006* and the supervision of prisoners subject to supervision orders or interim supervision orders under the *Dangerous Prisoners (Sexual Offenders) Act 2003* ; or (d) if the enforcement agency is any other law enforcement agency — the performance of its responsibility mentioned in schedule 5 , definition "law enforcement agency", paragraph (b)(iv), including the conduct of proceedings started or about to be started in a court or tribunal in relation to the responsibility. (2) In this section— "intelligence functions" means the functions mentioned in the *Crime and Corruption Act 2001* , section 53 .	"***law enforcement agency***" means— (a) for the purposes of IPP 11(1)(e)—an enforcement body within the meaning of the *Privacy Act 1988* (Cwlth) or any entity mentioned in paragraph (b); or (b) otherwise— (i) the Queensland Police Service under the *Police Service Administration Act 1990* ; or (ii) the Crime and Corruption Commission; or (iii) the community safety department; or (iv) any other agency, to the extent it has responsibility for— (A) the performance of functions or activities directed to the prevention, detection, investigation, prosecution or punishment of offences and other breaches of laws for which penalties or sanctions may be imposed; or (B) the management of property seized or restrained under a law relating to the confiscation of the proceeds of crime; or (C) the enforcement of a law, or of an order made under a law, relating to the confiscation of the proceeds of crime; or (D) the execution or implementation of an order or decision made by a court or tribunal.
Tas *Personal Information Protection Act 2004*	S 9 **Law enforcement information** Clauses 1(3), (4) and (5), 2(1), 5(3)(c), 7, 9 and 10(1) of Schedule 1 do not apply to any law enforcement information collected or held by a law enforcement agency if it considers that non-compliance is reasonably necessary – (a) for the purpose of any of its functions or activities; or (b) for the enforcement of laws relating to the confiscation of the proceeds of crime; or (c) in connection with the conduct of proceedings in any court or tribunal.	S 3: ***"law enforcement agency***" means any of the following: (a) a police force or police service of – (i) the Commonwealth; or (ii) this State; or (iii) any other State or a Territory of the Commonwealth; or (iv) any country; (b) the Australian Crime Commission; (c) a commission established or appointed under any Act of this State or any other State or a Territory of the Commonwealth or of the Commonwealth to investigate matters relating to criminal activity generally or of a specified

Jurisdiction	Exemptions	Entity definitions
		class; (d) a personal information custodian responsible for the performance of functions relating to – (i) the prevention, detection, investigation or prosecution of criminal offences or other offences that impose a penalty or sanction; or (ii) the management of property seized or restrained under a law relating to the confiscation of the proceeds of crime or the enforcement of such a law; (e) an agency established under the Public Service Act 1999 of the Commonwealth responsible for the performance of functions relating to – (i) the prevention, detection, investigation or prosecution of criminal offences or other offences that impose a penalty or sanction; or (ii) the management of property seized or restrained under a law relating to the confiscation of the proceeds of crime or the enforcement of such a law; (f) a personal information custodian or an individual or body contracted by a personal information custodian responsible for the execution or implementation of an order, decision or determination of a court or tribunal; (g) a personal information custodian – (i) responsible for the issue of warrants; or (ii) that provides correctional services; or (iii) responsible for decisions relating to the release of persons from custody; (h) a personal information custodian responsible for the protection of public revenue under any Act; (i) a personal information custodian responsible for the administration or performance of a function under a law that imposes a penalty or sanction; (j) the Attorney-General; (k) the Solicitor-General appointed and holding office under the Solicitor-General Act 1983 ; (l) the Director of Public Prosecutions appointed and holding office under the Director of Public Prosecutions Act 1973 ; (m) the Ombudsman; (ma) the Anti-Discrimination Commissioner appointed under the Anti-Discrimination Act 1998 ; (n) a prescribed organisation;
Vic *Privacy and*	s 15 **Exemption — law enforcement** It is not necessary for a law enforcement agency to comply with IPP 1.3 to 1.5,	"**law enforcement agency**" means— (a) Victoria Police; or

Jurisdiction	Exemptions	Entity definitions
Data Protection Act 2014	2.1, 6.1 to 6.8, 7.1 to 7.4, 9.1 or 10.1 if it believes on reasonable grounds that the noncompliance is necessary— (a) for the purposes of one or more of its, or any other law enforcement agency's, law enforcement functions or activities; or (b) for the enforcement of laws relating to the confiscation of the proceeds of crime; or (c) in connection with the conduct of proceedings commenced, or about to be commenced, in any court or tribunal; or (d) in the case of Victoria Police, for the purposes of its community policing functions.	(b) the police force or police service of another State or a Territory; or (c) the Australian Federal Police; or (d) the Australian Crime Commission established under section 7 of the Australian Crime Commission Act 2002 of the Commonwealth; or (e) the Commissioner appointed under section 8A of the Corrections Act 1986; or (ea) the Director, Fines Victoria employed under section 4 of the Fines Reform Act 2014 ; (f) the Business Licensing Authority established under Part 2 of the Business Licensing Authority Act 1998 ; or (g) a commission established by a law of Victoria or the Commonwealth or of any other State or a Territory with the function of investigating matters relating to criminal activity generally or of a specified class or classes; or (h) the Chief Examiner and Examiners appointed under Part 3 of the Major Crime (Investigative Powers) Act 2004 ; or (i) the IBAC; or (j) the sheriff within the meaning of the Sheriff Act 2009 ; or (k) the Victorian Inspectorate; or (l) the Adult Parole Board established by section 61 of the Corrections Act 1986 ; or (la) the Post Sentence Authority established by section 192C of the Serious Sex Offenders (Detention and Supervision) Act 2009 ; or (m) the Youth Parole Board within the meaning of the Children, Youth and Families Act 2005 ; or (n) an agency responsible for the performance of functions or activities directed to— (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction for a breach; or (ii) the management of property seized or restrained under laws relating to the confiscation of the proceeds of crime or the enforcement of such laws, or of orders made under such laws; or (o) an agency responsible for the execution or implementation of an order or decision made by a court or tribunal; or

Jurisdiction	Exemptions	Entity definitions
		(p) an agency that provides correctional services, including a contractor within the meaning of the Corrections Act 1986 , or a subcontractor of that contractor, but only in relation to a function or duty or the exercise of a power conferred on it by or under that Act; or (q) an agency responsible for the protection of the public revenue under a law administered by it;
WA	[No WA or SA Acts]	-

Appendix E – Scope of 'Surveillance device' laws

Table 1. Types of information or device covered by surveillance laws

Act	Devices covered
Surveillance Devices Act 2004 (Cth) [FLR]	Surveillance device: Any combination of 'data surveillance device', 'listening device', 'optical surveillance device' or 'tracking device', or prescribed by regs
Listening Devices Act 1992 (ACT)	Listening device
Crimes (Surveillance Devices) Act 2010 (ACT)	Surveillance device: Any combination of 'data surveillance device', 'listening device', 'optical surveillance device' or 'tracking device', or prescribed by regs
Surveillance Devices Act 2007 (NSW) [LN]	Surveillance device: Any combination of 'data surveillance device', 'listening device', 'optical surveillance device' or 'tracking device', or prescribed by regs
Workplace Surveillance Act 2005 (NSW) [LN]	"Surveillance" of an employee: Any of 'camera surveillance', 'computer surveillance', 'tracking surveillance' [different terms, focuses on the method rather than the device]
Invasion of Privacy Act 1971 (Qld)	Listening device
Surveillance Devices Act (NT)	Surveillance device: Any combination of 'data surveillance device', 'listening device', 'optical surveillance device' or 'tracking device'
Surveillance Devices Act 2016 (SA) [LSA]	Surveillance device: Any combination of 'data surveillance device', 'listening device', 'optical surveillance device' or 'tracking device', or prescribed by regs
Listening Devices Act 1991 (Tas)	Listening device
Surveillance Devices Act 1999 (Vic)	Surveillance device: Any combination of 'data surveillance device', 'listening device', 'optical surveillance device' or 'tracking device', or prescribed by regs
Surveillance Devices Act 1998 (WA) [WAL]	Surveillance device: 'Listening device', 'optical surveillance device' or 'tracking device' [omits *data* surveillance device]

Table 2. – Key definitions terms in various jurisdictions' surveillance device legislation

State	Devices, powers	Information, other provisions
Commonwealth *Surveillance Devices Act 2004* (Cth) [FLR]	"**surveillance device**": any combination of 'data surveillance device', 'listening device', 'optical surveillance device' or 'tracking device', or a kind prescribed by Regs "**data surveillance device**": any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device. ***"device"*** includes instrument, apparatus and equipment. "**listening device**": any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing […]. – in car microphones? **"optical surveillance device**": any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight […] – in car cameras "**tracking device**" means any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object. – many elements of C-ITS and AV would meet this. "**premises**" includes: […] (d) any place, whether built on or not, whether within or beyond Australia. – query meaning of 'place' – vehicle? "**record**" includes: (a) an audio, visual or audio-visual record; and (b) a record in digital form; and (c) a documentary record prepared from a record referred to in paragraph (a) or (b). – would cover much C-ITS and AV data	Focus on procedures for law enforcement officers to obtain surveillance or retrieval warrants, emergency authorisations and tracking device authorisations for the installation and use of surveillance devices and tracking devices. S 3 Purposes include criminal investigations, location and safe recovery of children to whom recovery orders relate, and protecting from and preventing terrorism related acts where a control order is in place. S 3 Also imposes restrictions on use, communication and publication of information obtained through use of surveillance devices, and prohibits use of devices without one of the forms of warrant or authorisation. Requirement for secure storage and destruction, and reporting. S 39 Use and retrieval of tracking devices is permitted without warrant in certain circumstances [12 categories] S 45 offences of use, recording, communication or publication of protected information without the authorisation under the extensive list of permitted purposes in s 45(4) or (5), or ss 45A or 65B. The items in 44(d) below are restricted in their use. s 44 What is protected information? "***protected information***" means: (a) any information obtained from the use of a surveillance device under a warrant, an emergency authorisation or a tracking device authorisation; or (b) any information relating to: (i) an application for, the issue of, the existence of, or the expiration of, a warrant, an emergency authorisation or a tracking device authorisation; or (ii) an application for approval of powers exercised under an emergency authorisation; or (c) any information that is likely to enable the identification of a person, object or premises specified in a warrant, an emergency

State	Devices, powers	Information, other provisions
	" **relevant proceeding**" and "**relevant offence**": – detailed definitions of the scope of offences and proceedings covered by warrants and authorisations federal agencies include ACLEI, and (a) the Australian Federal Police; (b) the Australian Crime Commission; (c) the Immigration and Border Protection Department – these are the federal LEAs, see also s 6A(7) for state. **Warrants** generally required: Part 2. s 37 Use of optical surveillance devices **without warrant** –it can only be done without a warrant if it does not involve 'interference without permission of any **vehicle** or thing" – this would exclude implanting on a C-ITS or AV purposes for the authorisations or warrants, s 3: • criminal investigations, • location and safe recovery of children to whom recovery orders relate; where a control order is in force, • the use of a surveillance device or tracking device would be likely to substantially assist (certain anti-terror activities)	authorisation or a tracking device authorisation; or (d) any other information obtained by a law enforcement officer: (i) without the authority of a warrant or a tracking device authorisation; or (ii) without the authority of an emergency authorisation that was subsequently approved; or (iii) in a case where the information was obtained through the use of a surveillance device in a foreign country, or on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limit of Australia's territorial sea--without the agreement of the appropriate consenting official of that foreign country, and of any other foreign country, whose agreement is required under section 42; in contravention of the requirement for such a warrant, tracking device authorisation or emergency authorisation. (2) For the avoidance of doubt, information obtained under an emergency authorisation falls under paragraph (a) and not paragraph (d) of the definition of ***protected information*** unless: (a) an eligible Judge or nominated AAT member refuses to approve the giving of the emergency authorisation; or (b) contrary to the requirement of section 33, no application for such an approval has been made. – a very broad scope of information is 'protected', but certain types collected without authorisation in (d) are unable to be used in many circumstances.
ACT *Crimes (Surveillance Devices) Act 2010* (ACT) See also *Listening Devices*	"**surveillance device**": any combination of 'data surveillance device', 'listening device', 'optical surveillance device' or 'tracking device', or a kind prescribed by Regs – same as Cth "**data surveillance device**" means a device capable of being used to monitor or record the information being put on to or retrieved from a computer, but does not include an optical surveillance device;	*Crimes (Surveillance Devices) Act 2010* has Offences for misuse of 'protected information and definitions similar to those in in the older *Listening Devices Act,* but omits some such as "private activity" or "premises", and in other cases follows the more recent Commonwealth Act, such as with 'tracking device'. It omits the complex definitions of protected information sub categories, but has a definition of protected information to similar effect. It also protects operations and methods. It does not have prohibitions on installation and use like some other Acts.

State	Devices, powers	Information, other provisions
Act 1992 (ACT)	"**listening device**" means a device capable of being used to listen to, monitor or record a conversation or words spoken to or by a person in a conversation, but does not include a hearing aid or similar device used by a person with impaired hearing […]; **"optical surveillance device**" means a device capable of being used to monitor, record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight […]; "**tracking device**" means an electronic device that may be used to determine the geographical location of a person or thing; – says 'or thing', instead of Cth's 'an object or the status of an object'. The latter is broader. "**place**" includes vacant land, premises and a vehicle; "**premises**" includes the following, regardless of whether in or outside this jurisdiction: (a) a building or structure; (b) a part of a building or structure; (c) land on which a building or structure is situated; "**private activity**" means an activity carried on in circumstances that may reasonably be taken to indicate the parties to the activity desire it to be observed only by themselves, but does not include an activity carried on in circumstances in which the parties to the activity ought reasonably to expect the activity may be observed by someone else – not in the Cth version "**private conversation**" means a conversation carried on in circumstances that may reasonably be taken to indicate the parties to the conversation desire it to be listened to only by themselves, but does not include a conversation carried on in circumstances in which the parties to the conversation ought reasonably to expect the conversation may be overheard by someone else; – not in the Cth version "**vehicle**" means anything used for carrying any person or	S 4 *Listening Devices Act* creates offence of **Use of listening devices**, which is a broad prohibition of unauthorised use. (1) A person must not use a listening device with the intention of— (a) listening to or recording a private conversation to which the person is not a party; or (b) recording a private conversation to which the person is a party. "**Protected information**" s 51 – not permitted to be used, communicated or published except for purposes in s 52; two offences created (1) Protected information is local protected information or corresponding protected information. (2) **Local protected information** is: (a) any information obtained from the use of a surveillance device under a warrant or emergency authorisation; or (b) any information relating to: (i) an application for, issue of, existence of or expiry of a warrant or emergency authorisation; or (ii) an application for approval of powers exercised under an emergency authorisation. (3) **Corresponding protected information** is: (a) any information obtained from the use of a surveillance device under a corresponding warrant or corresponding emergency authorisation; or (b) any information relating to: (i) an application for, issue of, existence of or expiry of a corresponding warrant or corresponding emergency authorisation; or (ii) an application under a corresponding law for approval of powers exercised under a corresponding emergency authorisation. – these are quite different categories from those in the Cth Act

State	Devices, powers	Information, other provisions
	anything by land, water or air – this is not in the Cth version	[Both these ACT laws appear in Current Acts on the ACT Legislation Register, implying they are both in force concurrently; neither is repealed. However the Historical Versions show the older Act has not been amended since the new one.]
NSW *Surveillance Devices Act 2007* (NSW)	"**surveillance device**" means: one or more of a data surveillance device, a listening device, an optical surveillance device or a tracking device, or a device of a kind prescribed by the regulations. – consistent with Cth scheme also offence publish or communicate the information obtained without consent or authorisation "**data surveillance device**" means any device or program capable of being used to record or monitor the input of information into or output of information from a computer, but does not include an optical surveillance device "**listening device**" means any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear. "**optical surveillance device**" means any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment. "**private conversation**" means any words spoken by one person to another person or to other persons in circumstances that may reasonably be taken to indicate that any of those persons desires the words to be listened to only: (a) by themselves, or (b) by themselves and by some other person who has the consent, express or implied, of all of those persons to do	[Similar model to the Commonwealth Act, with some further prohibitions **Offences** of install, use or maintain devices without consent (express or implied) or authorisation; also of possess information collected, manufacture or supply devices without lawful use, and communication or publication of information derived. See Part 2. See also Part 5 Div 1, Restrictions on use etc., of Protected Information.] **"protected information"** - s 39 (a) any information obtained from the use of a surveillance device under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation, or (b) any information relating to: (i) an under a corresponding law for approval of powers exercised under a corresponding emergency authorisation, or (c) any information obtained from use of a surveillance device as referred to in section 7 (4), or (d) NY information obtained from the use, in accordance with section 50A, of body-worn video by a police officer. [much shorter than the Cth definition]

State	Devices, powers	Information, other provisions
	so, but does not include a conversation made in any circumstances in which the parties to it ought reasonably to expect that it might be overheard by someone else. "**tracking device**" means any electronic device capable of being used to determine or monitor the geographical location of a person or an object.	
NSW *Workplace Surveillance Act 2005* (NSW) [LN]	"**covert surveillance**" means surveillance of an employee while at work for an employer carried out or caused to be carried out by the employer and not carried out in compliance with the requirements of Part 2. "**surveillance**" of an employee means surveillance of an employee by any of the following means: (a) "**camera surveillance**" , which is surveillance by means of a camera that monitors or records visual images of activities on premises or in any other place, (b) "**computer surveillance**" , which is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites), (c) "**tracking surveillance**" , which is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device). – location information "**camera**" includes an electronic device capable of monitoring or recording visual images of activities on premises or in any other place. Note : This Act does not apply to surveillance by means of a **listening device**. See section 4 (3) of the *Surveillance Devices Act 2007*. Camera surveillance that is regulated by this Act will also be regulated by the Surveillance Devices Act 2007 if the camera is	S 26 **Privacy** Must Be Considered A Magistrate must not issue a covert surveillance authority unless the Magistrate has had regard to whether covert surveillance of the employee or employees concerned might unduly intrude on their privacy or the privacy of any other person. –only mention of privacy in any of the Acts s 19 **Covert surveillance prohibited without covert surveillance authority** An employer must not carry out, or cause to be carried out, covert surveillance of an employee while the employee is at work for the employer unless the surveillance is authorised by a covert surveillance authority. – no use of 'protected information' but there is a ban on collection and re-use without authority

State	Devices, powers	Information, other provisions
	used to record a private conversation.	
Queensland *Invasion of Privacy Act 1971* (Qld)	Much older, with less elaboration of devices "**listening device**" means any instrument, apparatus, equipment or device capable of being used to overhear, record, monitor or listen to a private conversation simultaneously with its taking place. "**private conversation**" means any words spoken by one person to another person in circumstances that indicate that those persons desire the words to be heard or listened to only by themselves or that indicate that either of those persons desires the words to be heard or listened to only by themselves and by some other person, but does not include words spoken by one person to another person in circumstances in which either of those persons ought reasonably to expect the words may be overheard, recorded, monitored or listened to by some other person, not being a person who has the consent, express or implied, of either of those persons to do so.	Key offences of use of listening device (other devices not mentioned), and passing on the information without authority, s 43. See also prohibitions on communication or publication of private conversations unlawfully listened to, or recorded by a party: s 44 and s 45. S 51 provides immunity for narrow group of crown persons. **43 PROHIBITION ON USE OF LISTENING DEVICES** (1) A person is guilty of an offence against this Act if the person uses a listening device to overhear, record, monitor or listen to a private conversation and is liable on conviction on indictment to a maximum penalty of 40 penalty units or imprisonment for 2 years. (2) Subsection (1) does not apply— (a) where the person using the listening device is **a party** to the private conversation; or (b) to the **unintentional** hearing of a private conversation by means of a telephone; or (c) to or in relation to the use of any listening device by— (i) an officer employed in the service of the Commonwealth in relation to **customs** authorised by a warrant under the hand of the Comptroller-General of Customs under the Customs Act 1901 (Cwlth) to use a listening device in the performance of the officer's duty; or (ii) a person employed in connection with the **security of the Commonwealth** when acting in the performance of the person's duty under an Act passed by the Parliament of the Commonwealth relating to the security of the Commonwealth; or (d) to or in relation to the use of a listening device by a **police officer** or another person under a provision of an Act authorising the use of a listening device; or (e) to or in relation to the use of a listening device that is a government network radio, activated by a communications centre operator for a **public safety entity**, in circumstances in which— (i) an officer of the entity has activated a duress alarm; or

State	Devices, powers	Information, other provisions
		(ii) an officer of the entity has contacted the communications centre operator to ask for assistance; or (iii) the communications centre operator has reasonable grounds to believe there may be a risk to the life, health or safety of an officer of the entity. (3) A person referred to in subsection (2) (c) who uses a listening device to overhear, record, monitor or listen to any private conversation to which the person is not a party shall not **communicate** or publish the substance or meaning of that private conversation **otherwise than in the performance of the person's duty**.
NT *Surveillance Devices Act 2007* (NT) [The year is not formally part of the title of the consolidated/ current version in NT]	Surveillance device includes the typical four: listening, optical surveillance, tracking, and data surveillance devices "**data surveillance device**" means a device capable of being used to monitor or record the information being put on to or retrieved from a computer, but does not include an optical surveillance device "**listening device**" means a device capable of being used to listen to, monitor or record a conversation or words spoken to or by a person in a conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit the person to hear only sounds ordinarily audible to the human ear; **"optical surveillance device**" means a device capable of being used to monitor, record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome the impairment and permit the person to see only sights ordinarily visible to the human eye "**private activity**" means an activity carried on in circumstances	Key offences in Part 2 for Installation, use and maintenance without authorisation, with minor variations for each type of device: s11 listening, s 12 optical, s 13 tracking, s 14 data. For example, tracking: **S 13 Installation, use and maintenance of tracking devices** (1) A person is guilty of an offence if the person: (a) installs, uses or maintains a tracking device to determine the geographical location of a person or thing; and (b) knows the device is installed, used or maintained without the express or implied consent of: (i) for a device to determine the location of a person – the person; or (ii) for a device to determine the location of a thing – a person in lawful possession or having lawful control of the thing. Maximum penalty: 250 penalty units or imprisonment for 2 years. (2) Subsection (1) does not apply to the installation, use or maintenance of a tracking device: (a) under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or (b) under a law of the Commonwealth; or (c) if the device is installed by a law enforcement officer in the performance of the officer's duty on a thing when the thing is in a public place; or (d) if the device is installed, used or maintained in prescribed

State	Devices, powers	Information, other provisions
	that may reasonably be taken to indicate the parties to the activity desire it to be observed only by themselves, but does not include an activity carried on in circumstances in which the parties to the activity ought reasonably to expect the activity may be observed by someone else; "**private conversation**" means a conversation carried on in circumstances that may reasonably be taken to indicate the parties to the conversation desire it to be listened to only by themselves, but does not include a conversation carried on in circumstances in which the parties to the conversation ought reasonably to expect the conversation may be overheard by someone else; "**place**" includes vacant land, premises and a vehicle; "**tracking device**" means an electronic device that may be used to determine the geographical location of a person or thing;	circumstances. [Absent a warrant or authorisation, statutory power, use by law enforcement, or a prescribed exception, collection and installation will be an offence.] Other offences are for: • unauthorised use, communication or publication of protected information, s 52. • exposure of 'technologies and methods'. There are exceptions for material already in the public domain, prevention of serious harm to persons or property, activities prejudicial to national security or to assist foreign law enforcement. "**protected information**", see section 51(1); (1) **Protected information** is local protected information or corresponding protected information. (2) **Local** protected information is: (a) any information obtained from the use of a surveillance device under a warrant or emergency authorisation; or (b) any information relating to: (i) an application for, issue of, existence of or expiry of a warrant or emergency authorisation; or (ii) an application for approval of powers exercised under an emergency authorisation. (3) **Corresponding** protected information is: (a) any information obtained from the use of a surveillance device under a corresponding warrant or corresponding emergency authorisation; or (b) any information relating to: (i) an application for, issue of, existence of or expiry of a corresponding warrant or corresponding emergency authorisation; or (ii) an application under a corresponding law for approval of powers

State	Devices, powers	Information, other provisions
		exercised under a corresponding emergency authorisation.
SA *Surveillance Devices Act 2016* (SA)	This covers the four standard devices. "**surveillance device**": any combination of 'data surveillance device', 'listening device', 'optical surveillance device' or 'tracking device', or a kind prescribed by Regs "**data surveillance device**" means— (a) a program or device capable of being used to access, track, monitor or record the input of information into, or the output of information from, a computer; and (b) associated equipment (if any), but does not include a device, or device of a class or kind, excluded […] by the regulations "**declared surveillance device**" means a surveillance device or a surveillance device of a class or kind to which for the time being section 36 applies; "**listening device**" means— (a) a device capable of being used to listen to or record a private conversation or words spoken to or by any person in private conversation (whether or not the device is also capable of operating as some other kind of surveillance device); and (b) associated equipment (if any), but does not include— (c) a device being used to assist a person with impaired hearing to hear sounds ordinarily audible to the human ear; or (d) a device, or device of a class or kind, excluded from the ambit of this definition by the regulations; "**tracking device**" means— (a) a device capable of being used to determine the geographical location of a person, vehicle or thing; […] "**premises**" includes—	Types of warrant: "**surveillance device warrant**" means— (a) a surveillance device (tracking) warrant; or (b) a surveillance device (general) warrant; Similar to Commonwealth scheme, with a further explicit data offence: S 8: 'without authorisation or consent, to knowingly install, use or maintain a data surveillance device to access, track, monitor or record the input of information into, the output of information from, or information stored in, a computer without the express or implied consent of the owner, or person with lawful control or management, of the computer.' s 8—**Data surveillance devices** [offence to use without authorisation or consent] (1) Subject to this section, a person must not knowingly install, use or maintain a data surveillance device to access, track, monitor or record the input of information into, the output of information from, or information stored in, a computer without the express or implied consent of the owner, or person with lawful control or management, of the computer.

State	Devices, powers	Information, other provisions
	(a) land; and […] (d) any place, whether built on or not, whether in or outside this State; "**private activity**" means— (a) an activity carried on by only 1 person in circumstances that may reasonably be taken to indicate that the person does not desire it to be observed by any other person, but does not include— (i) an activity carried on in a public place; or (ii) an activity carried on or in premises or a vehicle if the activity can be readily observed from a public place; or (iii) an activity carried on in any other circumstances in which the person ought reasonably to expect that it may be observed by some other person; or (b) an activity carried on by more than 1 person in circumstances that may reasonably be taken to indicate that at least 1 party to the activity desires it to be observed only by the other parties to the activity, but does not include— (i) an activity carried on in a public place; or (ii) an activity carried on or in premises or a vehicle if the activity can be readily observed from a public place; or (iii) an activity carried on in any other circumstances in which a party to the activity ought reasonably to expect that it may be observed by a person who is not a party to the activity; "**private conversation**" means a conversation carried on in circumstances that may reasonably be taken to indicate that at least 1 party to the conversation desires it to be heard only by the other parties to the conversation (but does not include a conversation made in circumstances in which all parties to the conversation ought reasonably to expect that it may be heard by a person who is not a party to the conversation);	

State	Devices, powers	Information, other provisions
Tasmania *Listening Devices Act 1991* (Tas)	This only covers listening devices, and omits references to optical surveillance, data or tracking device. There is also a different definition of private conversation, introducing the concept of a third party who has the implied consent of all parties to listen in. S 3(1) **Interpretation** ***listening device*** means any instrument, apparatus, equipment or device capable of being used to record or listen to a private conversation simultaneously with its taking place; ***private conversation*** means any words spoken by one person to another person or to other persons in circumstances that may reasonably be taken to indicate that any of those persons desires the words to be listened to only – (a) by themselves; or (b) by themselves and by some other person who has the consent, express or implied, of all those persons to do so; (2) A reference in this Act to a listening device does not include a reference to a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and to permit the person to hear only sounds ordinarily audible to the human ear. (3) A reference in this Act to – (a) a report of a private conversation includes a reference to a report of the *substance, meaning or purport* of the conversation; or (b) a record of a private conversation includes a reference to a *statement* prepared from such a record. (emphasis added)	The information covered is not addressed, other than as implied In the nature of the device: voice conversation between several parties. There are several types of warrant, including an urgent phone in variant. There are several offences. S 5 PART 2 - **Offences Relating to Listening Devices Prohibition on use of listening devices** (1) A person shall not use, or cause or permit to be used, a listening device – (a) to record or listen to a private conversation to which the person is not a party; or (b) to record a private conversation to which the person is a party. (2) Subsection (1) does not apply to – (a) the use of a listening device pursuant to a warrant granted under Part 4 ; or (b) the use of a listening device pursuant to an authority granted by or under the *Telecommunications (Interception) Act 1979* of the Commonwealth or any other law of the Commonwealth; or (ba) the use of a surveillance device pursuant to an authority granted by or under the *Police Powers (Surveillance Devices) Act 2006* or by or under a corresponding law as defined in section 3 of that Act; or (c) the use of a listening device to obtain evidence or information in connection with – (i) an imminent threat of serious violence to persons or of substantial damage to property; or (ii) a serious narcotics offence – if the person using the listening device believes on reasonable grounds that it was necessary to use the device immediately to obtain that evidence or information; or (d) the unintentional hearing of a private conversation by means of a listening device; or (e) the use of a listening device for the recording of an interview between a police officer and a person suspected by a police officer of having

State	Devices, powers	Information, other provisions
		committed an offence against any Act. There is an offence of communication of what was heard unlawfully: s 9 **Prohibition on communication or publication of private conversations unlawfully listened to** There is a exception in s 9(2): (b) where the person making the communication or publication believes on reasonable grounds that it was necessary to make that communication or publication in connection with – (i) an *imminent threat of serious violence to persons or of substantial damage to property*; or (ii) a serious narcotics offence; (emphasis added)
Victoria *Surveillance Devices Act 1999* (Vic)	"**surveillance device**" means: one or more of a data surveillance device, a listening device, an optical surveillance device or a tracking device, or a device of a kind prescribed by the regulations. – consistent with Cth scheme "**data surveillance device**" means any device capable of being used to record or monitor the input of information into or the output of information from a computer, but does not include an optical surveillance device; **'listening device'** means any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear; **"optical surveillance device"** means any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment; "**tracking device**" means an electronic device the primary purpose of which is to determine the geographical location of a	[Similar to NT. Key offences in Part 2 for Installation, use and maintenance without authorisation, with minor variations for each type of device: s6 listening, s 7 optical, s 8 tracking, s 9 data. For example, tracking:] **S 8 Regulation of Installation, use and maintenance of tracking devices** (1) Subject to subsection (2), a person must not knowingly install, use or maintain a tracking device to determine the geographical location of a person or an object— (a) in the case of a device to determine the location of a person, without the express or implied consent of that person; or (b) in the case of a device to determine the location of an object, without the express or implied consent of a person in lawful possession or having lawful control of that object. (2) Subsection (1) does not apply to— (a) the installation, use or maintenance of a tracking device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or (aa) the installation, use or maintenance of a tracking device in accordance with a detention order or supervision order or an interim order under the *Serious Sex Offenders (Detention and Supervision) Act 2009* ; or (ab) the installation, use or maintenance of a tracking device in accordance

State	Devices, powers	Information, other provisions
	person or an object; "**private activity**" means an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include— (a) an activity carried on outside a building; or (b) an activity carried on in any circumstances in which the parties to it ought reasonably to expect that it may be observed by someone else; "***private conversation***" means a conversation carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be heard only by themselves, but does not include a conversation made in any circumstances in which the parties to it ought reasonably to expect that it may be overheard by someone else;	with a parole order under the *Corrections Act 1986* ; or (ac) the installation, use or maintenance of an electronic monitoring device in accordance with a community correction order under the *Sentencing Act 1991* ; or (ad) the installation, use or maintenance of a tracking device in accordance with an order of the Governor of a prison under section 30 of the *Corrections Act 1986* ; or (b) the installation, use or maintenance of a tracking device in accordance with a law of the Commonwealth [Absent a warrant or authorisation, order, statutory power, collection and installation will be an offence.] Other offences are for: • use of optical or listening devices by employer, s 9B • unauthorised use, communication or publication of protected information or information permitted to be observed or private conversation, ss 30D and 9C and 11. • exposure of 'technologies and methods'. There are exceptions for material already in the public domain, prevention of serious harm to persons or property, activities prejudicial to national security or to assist foreign law enforcement. What is protected information? S. 30D def. of protected information "***protected information***" means— (a) any information obtained from the use of a surveillance device under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or (ab) any information obtained from the use of a body-worn camera or a tablet computer by a police officer or an ambulance officer acting in the course of the officer's duty; or (ac) any information obtained from the use of a body-worn camera or a tablet computer by a prescribed person, or a person belonging to a prescribed class of persons, acting in the course of the person's duties in the

State	Devices, powers	Information, other provisions
		prescribed circumstances; or (b) any information relating to— (i) an application for, issue of, existence of or expiry of a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or (ii) an application for approval of powers exercised under an emergency authorisation; or (iii) an application under a corresponding law for approval of powers exercised under a corresponding emergency authorisation. S 30E – prohibition on use etc or protected information
WA *Surveillance Devices Act 1998* (WA) [WAL]	"***surveillance device***" means a listening device, an optical surveillance device or a tracking device – *not* a data surveillance device, only 3 types "***listening device***" means any instrument, apparatus, equipment, or other device capable of being used to record, monitor or listen to a private conversation or words spoken to or by any person in private conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear; "***optical surveillance device***" means any instrument, apparatus, equipment, or other device capable of being used to record visually or observe a private activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment; "***tracking device***" means any instrument, apparatus, equipment, or other device capable of being used to determine the geographical location of a person or object; [similar to other state laws; warrants for each type of device are specified.]	[Similar to NT. Key offences in Part 2 for Installation, use and maintenance without authorisation, with minor variations for each type of device: s5 listening, s 6 optical, s 7 tracking, *NO data device offence*. For example, tracking offence is very similar to NT] One novel provision: Part 5, use of listening and optical devices in the public interest. Adds also a new type of order enabling a judge to permit a recorded item to be communicated. 31 . **Order allowing publication or communication in the public interest** (1) A judge may make an order that a person may publish or communicate a private conversation, or a report or record of a private conversation, or a record of a private activity that has come to the person's knowledge as a direct or indirect result of the use of a listening device or an optical surveillance device under Division 2 or 3, if the judge is satisfied, upon application being made in accordance with section 32, that the publication or communication should be made to protect or further the public interest.

State	Devices, powers	Information, other provisions
	"***private activity***" means any activity carried on in circumstances that may reasonably be taken to indicate that any of the parties to the activity desires it to be observed only by themselves, but does not include an activity carried on in any circumstances in which the parties to the activity ought reasonably to expect that the activity may be observed; "***private conversation***" means any conversation carried on in circumstances that may reasonably be taken to indicate that any of the parties to the conversation desires it to be listened to only by themselves, but does not include a conversation carried on in any circumstances in which the parties to the conversation ought reasonably to expect that the conversation may be overheard; **vehicle** includes a vessel	

Appendix F – Telecommunications laws

- *Telecommunications Act 1997* (Cth) [FLR]
- *Telecommunications (Interception and Access) Act 1979* (Cth) (TIAA) [FLR]
- *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) [FLR]
- *Law Enforcement Integrity Commissioner Act 2006* (Cth) (LEIC Act) [FLR]

- Telecommunications (Interception and Access) (Emergency Services Facilities – Australian Capital Territory) Instrument 2018 (Cth)
- *Telecommunications (Interception and Access) (New South Wales) Act 1987* (NSW) [LN]
- *Telecommunications (Interception) Northern Territory Act* (NT)
- *Telecommunications Interception Act 2009* (Qld)
- *Telecommunications (Interception) Act 2012 (SA)* [LSA]
- *Telecommunications (Interception) Tasmania Act 1999* (Tas)
- *Telecommunications (Interception) (State Provisions) Act 1988* (Vic)
- *Telecommunications (Interception and Access) Western Australia Act 1996* (WA)

Most of the state and territory provisions in effect require cooperation with and interaction with the federal law. They have record keeping obligations and review mechanisms, and involve local law enforcement agencies and oversight, but little else substantive.

Appendix G – EU and USA

1. European Union

C-ITS and AV Generated Data – Also Personal Data
[see section 8.2.3]

a) Competing Theories

There are different views as to whether C-ITS and AV generated data is personal data. A theory according to which data may be generally separated in different categories resulting in an 'either/or' distinction between non-personal and personal data has been prominent among various European automotive industry associations. These associations generally argue that with the exception of data for services requiring user or vehicle identification, CAV generated data is merely technical (non-personal data) with allegedly no relevance to data privacy law.[174]

This approach however has been rejected by the EU Commission,[175] EU data protection authorities and the Article 29 Working Party,[176] as well as majority of legal scholars, who argue that data generated by C-ITS communications and AV sensors, such as information about speed, acceleration and use of brakes, *could* constitute personal data. The unique identification number given to vehicles can be linked with the individuals who have registered as owners of those vehicles. The technical data generated by C-ITS and AVs and associated with the unique vehicle identifier may, therefore, be linked to individual drivers and relay information about their driving habits, for example.

b) Relative vs Absolute Approach

The important question then becomes whether such data can be linked to an identifiable person.[177] The GDPR definition of an 'identifiable person' focuses not on the nature of data but on actual capability to identify a person behind the data. (See

---

[174] German Association of the Automotive Industry - Verband der Automobilindustrie ('VDA'), *Data Protection Principles for Connected Vehicles*, 3 November 2014, <https://www.vda.de/en/topics/innovation-and-technology/network/data-protection-principles-for-connected-vehicles.html> retrieved 30 March 2017; VDA, in: *Access to the vehicle and vehicle generated data,* Position paper, 19 September 2016, p. 1, <https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html> visited 15 May 2018. See also European Automobile Manufacturers Association ('ACEA'), *ACEA Principles of Data Protection in Relation to Connected Vehicles and Services*, September 2015, p. 4, <http://www.acea.be/publications/article/acea-principles-of-data-protection-in-relation-to-connected-vehicles-and-se>, visited 24 March 2017; ACEA, *ACEA Strategy Paper on Connectivity*, April 2016, p.4, <http://www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf> visited 15 May 2018. British Society of Motor Manufacturers and Traders ('SMMT'). *Connected and Autonomous Vehicles – Position Paper*, February 2017, p.6 et seq., <http://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf>, visited 15/05/2018.

[175] European Commission, A European strategy on Cooperative Intelligent Transport Systems, a mile- stone towards cooperative, connected and automated mobility, COM(2016) 766 final, 30 November 2016, p. 8, <http://ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v5.pdf>, visited 15 May 2018. See also European Commission, EU C-ITS Platform Final Report, September 2017, <https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf>, p.28. The C-ITS platform is an initiative of Directorate for Transport and Mobility of the EU Commission, which started at the end of 2014 with the creation of specialized working groups, each addressing various aspects of C-ITS deployment, ranging from security and technical standardization to data protection.

[176] Article 29 Working Party, *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)*, <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171>, visited 15 May 2017, p. 6. The Working Party was set up under Article 29 of *Directive 95/46/EC*. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of *Directive 95/46/EC* and Article 15 of *Directive 2002/58/EC*.

[177] According to Art 2 lit a Data Protection Directive, data qualifies as personal data if it relates to an identifiable person and such 'identifiable person is one who can be identified, directly or indirectly'. Almost identically, the GDPR defines 'an identifiable natural person' as an individual 'who can be identified, directly or indirectly', Art 4 No 1 GDPR.

discussion in the EU section of the Report.) Because GDPR does not specify whose capabilities to actually identify data subject are actually relevant, two different approaches have emerged.

Under the so-called '*relative approach*', only the data controller is considered relevant (manufacturer or the government), and thus the exact same data might be considered 'personal data' with regard to data controller, but not in regard to other companies that do not control such data.

In contrast, the so-called '*absolute approach*' considers an individual identifiable if any third party may identify this individual, even if this requires additional knowledge exclusively assigned to such third party. Thus, under the latter approach, almost all data for any party is 'personal data' if someone can actually identify a person behind that data.

c) The CJEU in the *Breyer* Case

In what could be described as an *'extended relative approach',* the European Court of Justice (CJEU) explained in October 2016 that information not directly identifying a person will be deemed personal data in the hands of any party (but only in relation to that specific party) that can lawfully obtain sufficient additional data to link the information to a person and therewith identify that person.[178] The Court held that for data to be treated as personal data it is sufficient that the controller can or may employ legal means reasonably available to obtain corresponding additional knowledge from a third person through which the identification of the respective person is possible for the controller.

In sum, taking into account the official position of the EU bodies and the CJEU, C-ITS and AV generated technical data will in most cases be deemed personal data, but not for every third party. Instead, it depends on whether the data controller is in a position to identify the individual from the data.

2. USA

General Legal Framework for Law Enforcement Access: ECPA and SCA
[see section 9.2 on USA]

ECPA provides law enforcement agencies with a variety of legal tools to seek access to *stored* communications data. There are three main methods:

- subpoenas,
- court orders, and
- search warrants.

Firstly, US law enforcement can use a subpoena under the SCA, which requires a third party or an individual to collect physical or digital evidence in their direct possession or control and provide to the court which has jurisdiction over them. Subpoenas are limited to basic metadata and does not include 'content' data.[179]

[178] European Court of Justice, Judgment of 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland* – C-582/14. The Court further states, that for a qualification of data as personal it is not required 'that all the information enabling the identification of the data subject must be in the hands of one person'.

[179] '279 Subpoenas,' US Department of Justice, Offices of the U.S. Attorneys, *Criminal Resource Manual*, CRM 279, https://www.justice.gov/usam/criminal-resource-manual-279-subpoenas, accessed June 29, 2017. The Government has also argued that a subpoena can compel disclosure of opened email regardless of age. See:

Secondly, a court order under SCA compels access to metadata, but may also compel access to more detailed information, such as IP address.[180] SCA court orders are only issued when a judge or magistrate is satisfied that the requested information is relevant and material to an ongoing criminal investigation.[181]

Thirdly, a SCA search warrant allows law enforcement to acquire physical devices which store digital communications, such as computer hard-drive or C-ITS or AV devices. Warrants can compel access to content data (as opposed to merely metadata) but require the applicant to meet a high threshold of probability for the crime and evidence. They incorporate judicial review and require the specification of the data being sought as well as the location where the search will take place.

Constitutional Protections Against Government Access to Personal Data
[see Section 9.3.1]

The government's access to personal data derived from C-ITS and AV has not yet been explicitly addressed by the US Courts or legislatures, although recent US Supreme Court decisions regarding surveillance and the 'reasonable expectation of privacy' that one has in their vehicle, or with regards to their digital devices, may provide some guidance about how courts would view government access to personal data derived from C-ITS and AVs.[182] For example, in *United States v. Jones* (*Jones*), which involved placing a GPS tracker on a suspect's car, the majority of judges focused on the physical intrusion onto private property involved, but the concurring opinion placed emphasis on the so-called 'mosaic theory' – the idea that over time, disclosing simple location data can yield a large amount of personal information.[183] That same logic would appear to apply to data received and stored by C-ITS and AVs, which rely heavily on gathering and processing of location data, using methods such as GPS tracking and LIDAR. Direct applicability of *Jones* or 'mosaic theory' is nonetheless questionable for main two reasons.

Firstly, *Jones* was limited to gathering basic locational data, whereas AVs would likely have the ability to collect and audio and visual data and store text messages and contacts, together with high-speed broadband capabilities. Some of these features are very similar to the capabilities of the modern smartphone. Thus the 4th Amendment case of *Riley v. California*, which held that the police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested, may be more applicable. However, US law is still in flux as to whether inspecting historical mobile phone data, through data mining of data from cell tower usage, constitutes a 'search' under the Fourth Amendment.[184] The decision in *Riley* may

'Microsoft Ireland Case: Backgrounder,' Center for Democracy and Technology, 17 July 2014, <https://cdt.org/files/2014/07/Microsoft-Ireland-Memo-formatted.pdf>.

[180] *Electronic Communications Privacy Act of 1986*, 18 U.S.C. § 2703(d) (1986). E.g., SCA court orders may compel access to IP addresses associated with a particular email sent from that account and 'to' and 'from' fields in an email, see 'Google Transparency Report,' Google, <https://transparencyreport.google.com/>.

[181] Alan McQuinn and Daniel Castro, 'How Law Enforcement Should Access Data Across Borders,' Information Technology & Innovation Foundation, July 2017, p. 5.

[182] For comparison, the US Department of Transport are of the view that data collected by C-ITS does not contain personally identifying information, see <https://www.its.dot.gov/factsheets/pdf/Privacy_factsheet.pdf>, visited 12 June 2018.

[183] See *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) 'GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.' (citing *People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009)); see also *State v. Jackson*, 76 P.3d 217, 223 (Wash. 2003) discussing the types of information GPS produces.

[184] In *United States v. Graham*, the Fourth Circuit also ruled that such a search does indeed constitute a 'search' for 4th Amendment purposes. However, see 5th Circuit In *re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 603-04 (5th Cir. 2013).

be relevant in the future development of courts' views on warrantless searches of personal data derived from C-ITS and AVs.

Secondly, applicability of *Jones* to AVs in particular is questionable because it involved GPS tracking placed externally on the vehicle by the government. AVs, by contrast, process and gather vast amounts of information without the government involvement. Albeit C-ITS information could be received by government-owned roadside equipment set up to capture this information.

General Framework Governing Federal Agencies' Data Collection
[see Section 9.3.2.1. of the Report]

The *Privacy Act of 1974* applies whenever federal US agencies collect and/or receive identifiable information about the users from individuals themselves, other agencies or third parties. It requires federal agencies to specify the purpose of personal information collection and allows individuals to access information in their records. Moreover, the *Paperwork Reduction Act of 1980* requires federal agencies to have an independent review process in place for information collection requests,[185] and ensures that federal agencies' requests for information are independently reviewed. In addition, the *E-Government Act of 2002* requires that all federal agencies conduct a 'privacy impact assessment' (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII), or for a new aggregation of information that is collected, maintained, or disseminated using information technology.[186] Given that most traffic and criminal law provisions are enforced by the agencies and police at state rather federal level, the *Privacy Act of 1974, Paperwork Reduction Act of 1980* and *E-Government Act of 2002* are of limited practical relevance in relation to C-ITS and AV data, except the circumstances involving federal agencies not dealing with the law enforcement (which has specific exceptions and is addressed via separate legislation, discussed in the report).

[185] '*Paperwork Reduction Act*: Federal Statutes Relevant in the Information Sharing Environment (ISE),' Justice Information Sharing, U.S. Department of Justice, <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1289>, visited 14 May 2018. As stated at 44 U.S.C. § 3501(8), the PRA was enacted, at least in part, to 'ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including law relating to ... privacy and confidentiality,' including the *Privacy Act of 1974*. 5 U.S.C. § 552a. 'With respect to privacy and security, the Director shall... develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies.' 44 U.S.C. § 3504(g).

[186] Pub.L. 107-347, 44 U.S.C. § 101, *Justice Information Sharing*, U.S. Department of Justice, <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1287>, visited 14 May 2018.

GLOSSARY

Legal terms

An Act, piece of legislation, statute, or law

These often all mean the same thing, an act of a particular parliament, like the *Privacy Act 1988* (Cth). The year they were first passed forms part of their name, even if they are later amended. Different jurisdictions can have an Act of the same name, like the *Defamation Act 2005* of NSW and Vic, but the contents, terms or definitions are not necessarily the same.

Definition, Interpretation

The proper legal meaning of a word or phrase (a term) in an Act can be given in parts of that Act which might be called 'Interpretation', 'Dictionary', or 'Definitions', or embedded in a particular section. It can also be given or refined by a court's interpretation of how it applies in a specific context, in a particular dispute. A term can be defined differently in different Acts, or in different versions of the same Act – see the discussion of 'personal information'. It can also mean different things in different contexts, so a court's interpretation of a term in one situation may not be applicable to another.

Regulation, Rule

These have several meanings. 'The Regulations' can mean a piece of subordinate legislation made under the power conferred by an Act. Regulation can also mean a particular provision of that overall Regulation, like 'Regulation 13'. Regulation generally means the process of regulating some activity.

Schedule, Appendix

These terms refer to parts of an Act or Regulation tacked on to the end, after the main body which is made up of sections (or regulations). Sometimes the central rules of an Act can be in a Schedule. For instance, the Australian Privacy Principles are in a Schedule at the end of the *Privacy Act 1988* (Cth), not in its main body; offences in 'the Criminal Code' are in a Schedule in the *Criminal Code Act*.

SOURCES

Australian legislation

The most relevant legislation is covered in the report. This list below also includes a sampling of other related legislation. Legislation here is grouped by type:

- Privacy and data protection
- Surveillance devices
- Telecommunications
- Criminal and other law enforcement,
- Roads, transport or traffic law where relevant to access or use of data
- Archives
- Other

Links: Most Act titles have an embedded link to AustLII's online source since it covers the field, and you can use 'Noteup' in a section to find cases and other material referring to that section. There is also a citator Lawcite which does this in more depth. (Case decisions about these laws are not listed here, as they would be too numerous. A few key cases are noted in Appendix A.) Each jurisdiction's official source for legislation, where it exists, may also be linked in brackets after the title, like this: [NSW] links to Legislation NSW's version of the Act. The features in these government legislation sites vary widely, but usually cannot find cases.
(Check with the authors if links don't work your version of this document.)

Commonwealth

Privacy or FOI

- *Privacy Act 1988* (Cth) [FLR]

Surveillance devices

- *Surveillance Devices Act 2004* (Cth) [FLR]

Telecoms

- *Telecommunications Act 1997* (Cth) [FLR]
- *Telecommunications (Interception and Access) Act 1979* (Cth) (TIAA) [FLR]
- *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) [FLR]
- *Law Enforcement Integrity Commissioner Act 2006* (Cth) (LEIC Act) [FLR]

Traffic

- Heavy Vehicle National Law (HVNL) – see *Heavy Vehicle National Law Act 2012* (Qld)

Criminal

- *Criminal Code Act 1995* (Cth) Schedule 1 [FLR]
  – ss 473-475 telecommunications offences, ss 476-478 computer offences
  – part 474
- *Crimes Act 1914* (Cth) [FLR]
- *Australian Crime Commission Act 2002* (Cth) [FLR]
- *Mutual Assistance In Criminal Matters Act 1987* (Cth) [FLR]

Archives

- *Archives Act 1983* (Cth) [FLR]

Other

- *Australian Security Intelligence Organisation Act 1979* (Cth) [FLR]
  – see s 25A(4)(a) Minister can authorise hacking of computers to access data
- *Inspector-General of Intelligence And Security Act 1986* (Cth) [FLR]

- *Data-matching Program (Assistance and Tax) Act 1990* (Cth) [FLR]

ACT

Privacy or FOI
- *Information Privacy Act 2014* (ACT) [ACTLR]
- *Human Rights Act 2004* (ACT) [ACTLR]
- *Health Records (Privacy And Access) Act 1997* (ACT) [ACTLR]
- *Workplace Privacy Act 2011* (ACT) [ACTLR]

Surveillance devices
- *Listening Devices Act 1992* (ACT) – 'listening devices' [ACTLR]
- *Crimes (Surveillance Devices) Act 2010* (ACT) [ACTLR]

Telecoms
- Telecommunications (Interception and Access) (Emergency Services Facilities – Australian Capital Territory) Instrument 2018 (Cth)
  – obliges ACT cooperation under TIAA

Traffic and Roads
- *Road Transport (Safety and Traffic Management) Act 1999* (ACT) [ACTLR]
  – administered by ACT Transport Canberra and City Services Directorate

Criminal
- *Crimes Act 1900* (ACT) [ACTLR]
  – s 61B(1) includes offence of capturing visual data when a breach of privacy

Archives
- *Freedom of Information Act 2016* (ACT) [ACTLR]
- *Territory Records Act 2002* (ACT) [ACTLR]

NSW

Privacy or FOI
- *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA) [LN]
- *Health Records and Information Privacy Act 2002* (NSW) (HRIPA) [LN]
- *Government Information (Public Access) Act 2009* (NSW) [LN]
- *Privacy and Government Information Legislation Amendment Act 2010* (NSW) [LN]

Surveillance
- *Surveillance Devices Act 2007* (NSW) [LN]
- *Workplace Surveillance Act 2005* (NSW) [LN]

Telecoms
- *Telecommunications (Interception and Access) (New South Wales) Act 1987* (NSW) [LN]

Traffic and Roads
- *Heavy Vehicle (Adoption of National Law) Act 2013* (NSW)
  – s 25 of this adoption Act authorize RMS to breach confidences and other law to disclose and to authorize the disclosure of information.
- *Heavy Vehicle National Law* (NSW) No 42a
  – 729B warrant; collection powers in Div 4 of Part 9.4, particularly s 570C, which requires third party to provide location, route and origin and destination of journeys.
- *Roads Act 1993* (NSW) [LN]
- *Road Transport Act 2013* (NSW) [LN]
  – administered by Roads and Maritime Services NSW
- *Road Transport and Other Legislation Amendment (Digital Driver Licences and Photo Cards) Act 2018* (NSW) [LN]
- *Road Transport and Related Legislation Amendment Act 2017* (NSW) [LN]

- *Road Transport Legislation Amendment (Road Safety) Act 2018* (NSW) [LN]
- *Road Obstructions (Special Provisions) Act 1979* (NSW)
- *Road Transport Act 2013* (NSW)
- Passenger Transport Regulation 2007 (NSW) (repealed September 1 2017)
  – Schedule 1 Approved Security Camera systems, cl 1 'authorised purpose'.
- *Transport Administration Act 1988* (NSW)
  – s 39 approved scheme of subsidised travel – see *Waters v Public Transport* case.

Criminal

- *Crimes Act 1900* (NSW) [LN]
- *Crimes (Forensic Procedures) Act 2000* (NSW) [LN]
- *Criminal Records Act 1991* (NSW) [LN]
- *Criminal Procedure Act 1986* (NSW)
- *Drug Misuse and Trafficking Act 1985* (NSW)
- *Law Enforcement and National Security (Assumed Identities) Act 2010* (NSW)
- *Law Enforcement (Controlled Operations) Act 1997* (NSW)
- *Police Powers (Vehicles) Act 1998* (NSW)

Other

- *Essential Services Act 1988* (NSW)
- *State Emergency and Rescue Management Act 1989* (NSW)
- *State Emergency Service Act 1989* (NSW)

Archives

- *State Records Act 1998* (NSW) [LN]

NT (their Acts do not include year)

Privacy or FOI

- *Information Act 2002* (NT)

Surveillance devices

- *Surveillance Devices Act 2000* (NT)

Telecoms

- *Telecommunications (Interception) Northern Territory Act* (NT)

Traffic and Roads

- *Motor Vehicles Act* (NT)
  [admin by NT Department of Infrastructure, Planning and Logistics]

Qld

Privacy or FOI

- *Information Privacy Act 2009* (Qld)
- *Right to Information Act 2009* (Qld)

Surveillance

- *Invasion of Privacy Act 1971* (Qld)
  – listening devices.

Telecoms

- *Telecommunications Interception Act 2009* (Qld)

Traffic and Roads

- *Transport Operations (Road Use Management) Act 1995* (Qld)
  – administered by Queensland Department of Transport and Main Roads.
- *Heavy Vehicle National Law Act 2012* (Qld), Schedule [LQ]
  – contains NHVL

- Heavy Vehicle (Fatigue Management) National Regulation (Qld) [PDF]
  – potential basis to collect data required for fatigue monitoring; see schedule 2 covering risk categories.
- Heavy Vehicle (General) National Regulation [PDF]
  – general powers for collection.

Criminal

- *Police Powers and Responsibilities Act 2003* (Qld)
  – incl. ss 211-220 covert evidence gathering powers
- *Police Powers and Responsibilities Act 2000* (Qld)
  – ss 321-364.
- *Criminal Code 1899* (Qld)
  – see s 227A-227C, observations in breach of privacy

Archives

- *Public Records Act 2002* (Qld)

SA

Privacy or FOI

- [Still no SA Privacy act]
- Information Privacy Principles Instruction (IPPI)
  – published as Premier and Cabinet Circular No. 12, June 2016
- *Freedom of Information Act 1991* (SA) [LSA]

Surveillance devices

- *Surveillance Devices Act 2016* (SA) [LSA]
- *Listening and Surveillance Devices Act 1972* (SA)
  – replaced by SDA 2016.

Telecoms

- *Telecommunications (Interception) Act 2012* (SA) [LSA]

Traffic and Roads

- *Road Traffic Act 1961* (SA) [LSA]
- *Motor Vehicles Act 1959* (SA) [LSA]
  – admin by Department of Planning, Transport and Infrastructure South Australia

Criminal

- *Summary Offences Act 1953* (SA) [LSA]
- *Criminal Law Consolidation Act 1935* (SA) [LSA]

Archives

- *State Records Act 1997* (SA) [LSA]

Tasmania

Privacy or FOI

- *Personal Information Protection Act 2004* (Tas)
- *Right to Information Act 2009* (Tas)

Surveillance devices

- *Listening Devices Act 1991* (Tas)
  – and Regulations 2014

Telecoms

- *Telecommunications (Interception) Tasmania Act 1999* (Tas)

Traffic and Roads

- *Traffic Act 1925* (Tas)

- *Vehicle and Traffic Act 1999* (Tas)
  – administered by Department of State Growth Tasmania.

Archives

- *Archives Act 1983* (Tas)

Vic

Privacy or FOI

- *Charter of Human Rights and Responsibilities Act 2002* (Vic)
- *Privacy Data and Protection Act 2014* (Vic)
- *Health Records Act 2001* (Vic) including Health Privacy Principles
- *Freedom of Information Act 1982* (Vic)

Surveillance

- *Surveillance Devices Act 1999* (Vic)

Telecoms

- *Telecommunications (Interception) (State Provisions) Act 1988* (Vic)

Traffic and Roads

- *Road Safety Act 1986* (Vic)
  – administered by VicRoads

Criminal

- Victoria Police Records Information Release Policy

Archives

- *Public Records Act 1973* (Vic)

WA

Privacy or FOI

- *Freedom of Information Act 1992* (WA) [WAL]
- [still no Privacy Act in WA]

Surveillance devices

- *Surveillance Devices Act 1998* (WA) [WAL]

Telecoms

- *Telecommunications (Interception and Access) Western Australia Act 1996* (WA)

Traffic and Roads

- *Road Traffic (Vehicles) Act 2012* (WA) [WAL]
  – administered by Main Roads Western Australia
- *Road Traffic Act 1974* (WA) [WAL]
- *Road Traffic (Administration) Act 2008* (WA) [WAL]
  – s 6 person responsible for vehicle
  – part 5 Div 3 photographic images for infringement?
- *Road Traffic (Authorisation to Drive) Act 2008* (WA) [WAL]
  – Division 3A Disclosure of photographs; s 11C to police, ASIO, LEO.

Foreign regulatory materials

EU

- British Society of Motor Manufacturers and Traders ('SMMT'), *Connected and Autonomous Vehicles,* Position Paper, February 2017 <http://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf

- EU Article 29 Committee (2004) 'Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance', Article 29 Data Protection Working Party, document 11750/02/EN WP 89, 11 February 2004.
- EU Article 29 Working Party (2017), *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)*, <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171>
- European Automobile Manufacturers Association ('ACEA'), *ACEA Principles of Data Protection in Relation to Connected Vehicles and Services*, September 2015, <http://www.acea.be/publications/article/acea-principles-of-data-protection-in-relation-to-connected-vehicles-and-se>
- European Automobile Manufacturers Association ('ACEA'), *ACEA Strategy Paper on Connectivity*, April 2016 <http://www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf>
- European Commission, *A European strategy on Cooperative Intelligent Transport Systems, a mile- stone towards cooperative, connected and automated mobility*, COM(2016) 766 final, 30 November 2016, <http://ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v5.pdf>
- European Commission*, EU C-ITS Platform Final Report*, September 2017, <https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf>
- European Court of Justice, Judgment of 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland* – C-582/14.
- German Association of the Automotive Industry - Verband der Automobilindustrie ('VDA'), *Data Protection Principles for Connected Vehicles*, 3 November 2014, <https://www.vda.de/en/topics/innovation-and-technology/network/data-protection-principles-for-connected-vehicles.html>
- German Association of the Automotive Industry - Verband der Automobilindustrie ('VDA'), *Access to the vehicle and vehicle generated data*, Position paper, 19 September 2016 <https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html>
- OPCC (2006) 'Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities', Office of the Privacy Commissioner of Canada, March 2006 (CCTV regulation)

US

- *California Consumer Privacy Act of 2018,* California Civil Code § 1790-1798.78 (2018) <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>
- *E-Government Act of 2002*, 44 USC § 101, Pub.L. 107-347, (2002) <https://www.congress.gov/bill/107th-congress/house-bill/2458/text>
- *Electronic Communications Privacy Act of 1986*, 18 U.S.C. § 2510 (1986)
- *Foreign Intelligence Surveillance Act of 1978*, 50 18 U.S.C. Ch. 36 (2015), <https://www.law.cornell.edu/uscode/text/50/chapter-36>.
- *Paperwork Reduction Act of 1980*, 44 U.S.C. §§ 3501–3521
- *Privacy Act of 1974,* 5 U.S.C. § 552a

- *United States v. Jones*, 132 S. Ct. 945, 955 (2012)
- *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 603-04 (5th Cir. 2013)

- '279. Subpoenas', US Department of Justice, Offices of the U.S. Attorneys, Criminal Resource Manual, CRM 279 < https://www.justice.gov/usam/criminal-resource-manual-279-subpoenas>

- *'Paperwork Reduction Act*: Federal Statutes Relevant in the Information Sharing Environment (ISE)', Justice Information Sharing, U.S. Department of Justice, <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1289>