DATA PRIVACY AND AUTOMATED VEHICLES: NAVIGATING THE PRIVACY CONTINUUM

MARK BRADY*

Australia's information privacy framework fails to protect personal information contained within data generated by automated vehicles. Automated vehicles will increasingly store, share and broadcast data about the vehicle (and by implication the occupants) with rising levels of automation. Using data mining techniques, personal information contained within disparate data streams can be compiled to allow profiling of individuals to a high degree. Following the recent decision in Privacy Commissioner v Telstra Corporation Ltd *(*'Telstra'*), Australian law does not recognise personal information unless contained within a single data stream and remains silent on how to identify personal information within data having multiple subject matters. This article argues that, post-*Telstra*, the privacy framework will not safeguard personal information contained within data produced by automated land vehicles.*

I INTRODUCTION

There is increased attention directed toward the introduction of automated and connected land vehicles ('automated vehicles') in Australia.[1] The arrival of automated vehicles on Australian roads will result in an exponential increase in

* Lecturer, Adelaide Law School, Faculty of the Professions, University of Adelaide; BA, LLB (Hons), GDLP; PhD Candidate, School of Law, Queensland University of Technology, Queensland. The author would like to thank Professor Kieran Tranter and Associate Professor Kylie Burns for comments and suggestions made during the writing of this paper.

1 See National Transport Commission, 'Regulatory Options for Automated Vehicles' (Discussion Paper, May 2016) ('Regulatory Options for Automated Vehicles'); Clayton Utz, *Driving into the Future: Regulating Driverless Vehicles in Australia* (Report, 2016); Atkins, *Connected & Autonomous Vehicles: Introducing the Future of Mobility* (Report, 2016) <www.atkinsglobal.com/~/media/Files/A/Atkins-Corporate/uk-and-europe/uk-thought-leadership/reports/CAV_A4_080216.pdf>; Sophie Vorrath, 'All Cars on Australian Roads Will Be Driverless by 2030: Telstra Exec', *Renew Economy* (Web Page, 1 August 2016) <reneweconomy.com.au/2016/all-cars-on-australian-roads-will-be-driverless-by-2030-telstra-exec-33821>; Bureau of Infrastructure, Transport and Regional Economics, Department of Infrastructure and Regional Development (Cth), *Impact of Road Trauma and Measures to Improve Outcomes* (Research Report No 140, 2014); National Transport Commission, 'Cooperative Intelligent Transport Systems' (Final Policy Paper, December 2013); Standing Council on Transport and Infrastructure, *Policy Framework for Intelligent Transport Systems in Australia* (Report, 2012) ('*Policy Framework for Intelligent Transport Systems*').

the volume of data transmitted and received by automobiles.[2] Automated vehicles will generate numerous data streams containing information about multiple subject matters, such as dynamic vehicle parameters, external inputs, or other person-specific data.[3] Accessing information within data streams ('data mining') represents 'a technological and social shift that is rapidly morphing society'[4] as multiple data streams can now be compiled to allow profiling of individuals to a very high degree.[5] Concerns raised regarding the need for a response to the introduction of automated vehicles[6] come from researchers,[7] law reform bodies,[8] and the road safety community.[9] The Australian Law Reform Commission ('ALRC') recognised data mining as a concern in 2008.[10] Data mining may enable identification of 'sensitive information' regarding inter alia an individual's biometric data, political opinions, race, movements, beliefs, affiliations, criminal

2 See generally Andrew McAfee and Erik Brynjolfsson, 'Big Data: The Management Revolution' (2012) 90(10) *Harvard Business Review* 60, 62; Bharti Thakur and Manish Mann, 'Data Mining for Big Data: A Review' (2014) 4(5) *International Journal of Advanced Research in Computer Science and Software Engineering* 469, 471.

3 Chasel Lee, 'Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars' (2017) 69(1) *Federal Communications Law Journal* 25, 33–4.

4 Jay P Kesan, Carol M Hayes and Masooda N Bashir, 'A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy' (2016) 91(2) *Indiana Law Journal* 267, 269.

5 Mark Brady, 'Is Australian Law Adaptable to Automated Vehicles?' [2019] (Special Issue) *Griffith Journal of Law & Human Dignity* 35, 49; Daniel J Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53(6) *Stanford Law Review* 1393, 1394.

6 National Transport Commission, 'Regulatory Reforms for Automated Road Vehicles' (Policy Paper, November 2016) 71 ('Regulatory Reforms'); National Transport Commission, 'Regulating Government Access to C-ITS and Automated Vehicle Data' (Discussion Paper, September 2018) ('Automated Vehicle Data'). See generally Joint Standing Committee on Road Safety (Staysafe), Parliament of New South Wales, *Driverless Vehicles and Road Safety in NSW* (Report No 2/56, September 2016) ('*Driverless Vehicles and Road Safety in NSW*'); House of Representatives Standing Committee on Industry, Innovation, Science and Resources, Parliament of Australia, *Social Issues Relating to Land-Based Automated Vehicles in Australia* (Report, August 2017) ('*Social Issues Relating to Land-Based Automated Vehicles in Australia*'). See also Australian Law Reform Commission, *Review of Privacy* (Issues Paper No 31, 2006) ('*Review of Privacy*'); Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Final Report No 123, June 2014) ('*Serious Invasions of Privacy in the Digital Era*'); *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)* [2002] OJ L 201/37, 37–8 [6]–[9], arts 6, 9 ('*Directive on Privacy and Electronic Communications*').

7 Brady (n 5) 49–51. See generally Jake Goldenfein, 'Australia's Privacy Laws Gutted in Court Ruling on What is "Personal Information"', *The Conversation* (online, 19 January 2017) <theconversation.com/australias-privacy-laws-gutted-in-court-ruling-on-what-is-personal-information-71486>; Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) *International Data Privacy Law* 74. For a comprehensive overview of data privacy in the automated vehicle context see David Vaile, Monika Zalnieriute and Lyria Bennett Moses, *The Privacy and Data Protection Regulatory Framework for C-ITS and AV Systems: Report for the National Transport Commission* (Report, 2 July 2018) <www.ntc.gov.au/Media/Reports/(A4689742-E776-D8B3-1837-C4F6F3969B2E).pdf>.

8 'Automated Vehicle Data' (n 6). See generally *Review of Privacy* (n 6); 'Regulatory Reforms' (n 6) 71; *Driverless Vehicles and Road Safety in NSW* (n 6) 56; *Serious Invasions of Privacy in the Digital Era* (n 6); Goldenfein (n 7); Rubinstein (n 7).

9 See National Transport Commission, 'Changing Driving Laws to Support Automated Vehicles' (Discussion Paper, October 2017); 'Regulatory Reforms' (n 6); *Policy Framework for Intelligent Transport Systems* (n 1).

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 1, ch 9, 402–4 ('*For Your Information*').

record, or sexual proclivities.[11] Where vehicular information is cross-referenced,[12] identification of an individual is possible.[13] According to Vaile, Zalnieriute and Moses:

> 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 …[14]

Moreover, in Australia this data is not considered to be 'personal information' at law.[15] The recent full Federal Court decision in *Privacy Commissioner v Telstra Corporation Ltd* ('*Telstra*')[16] leaves open how information *about* an individual is to be understood, and disregards the potential for data mining altogether. The Court, quoting the earlier Tribunal judgement,[17] stated that the 'starting point must be whether the information or opinion is *about* an individual … *it does not matter whether that information or opinion could be married with other information to identify a particular individual*'.[18]

Accordingly, there is limited protection afforded to personal information contained within the data produced by automated vehicles, with 'personal information' being 'context dependent' in every case.[19] This article argues the current regulatory framework that protects information privacy will not adequately cover the introduction of automated vehicles in Australia. The Article is in three parts. Part II argues that problems associated with data and automated vehicles increase as the level of automation rises. It shows that problems arise where automated vehicle data can have multiple subject matters which change with the level of automation. Part III argues that following the *Telstra* decision, the current regulatory framework fails to protect data produced by automated vehicles as it does not recognise data that may be compiled from multiple data streams to identify personal information about a person. It analyses the current information privacy law where it intersects with various stakeholders that consume data produced by automated vehicles: vehicle owners, manufacturers,

11 *Privacy Act 1988* (Cth) s 6(1) (definition of 'sensitive information') ('*Privacy Act 1988*'). See also Rubinstein (n 7) 77.

12 For an overview of cross-referencing information see Thakur and Mann (n 2) 471; Rubinstein (n 7) 77.

13 Rubinstein (n 7) 77.

14 Vaile, Zalnieriute and Moses (n 7) 16. 'IMEI' number refers to the International Mobile Equipment Identity number which is unique to each mobile electronic device connected to mobile networks.

15 *Privacy Act 1988* (n 11) s 6(1) (definition of 'personal information'). See below n 56 and accompanying text.

16 (2017) 249 FCR 24 ('*Telstra*').

17 *Re Telstra Corp Ltd and Privacy Commissioner* (2015) 254 IR 83, 115 [95] (Forgie DP) ('*Re Telstra Corp Ltd*').

18 *Telstra* (n 16) 32 [40] (Kenny and Edelman JJ) (emphasis added), quoting ibid.

19 Vaile, Zalnieriute and Moses (n 7) 15.

government, and third party entities, at various levels of automation. Part IV argues that legislative reform of the information privacy framework is necessary to ensure protection of data produced by automated vehicles.

II PROBLEMS WITH DATA AND AUTOMATED VEHICLES

This section argues that problems associated with data and automated vehicles increase as the level of automation rises. It sets out the different Society of Automotive Engineers ('SAE') levels of automation and potential problems with different types of data having multiple subject matters. It argues that these problems are affected by the level of automation. This section concludes by suggesting the problems associated with data and automated vehicles require an investigation of the existing law surrounding information privacy in Australia.

A *Levels of Automation*

A detailed categorisation of automated vehicle systems is provided by the SAE standard J3016.[20] It provides for a nuanced graduation between human control, and monitoring of the automated system in lower levels of automation, and fully automated vehicles.[21] It has been adopted by Australian, the European Union and United States ('US') regulators.[22] The SAE standard J3016 levels are displayed in Table 1.[23]

20 SAE International, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* (at June 2018) ('J3106'), cited in Bryant Walker Smith, 'SAE Levels of Driving Automation', The Centre for Internet and Society (Blog Post, 18 December 2013) <cyberlaw.stanford.edu/blog/2013/12/sae-levels-driving-automation>.

21 For an analysis of the SAE standard as being fundamentally flawed: see Toshiyuki Inagaki and Thomas B Sheridan, 'A Critique of the SAE Conditional Driving Automation Definition, and Analyses of Options for Improvement' [2018] *Cognition, Technology & Work* 10.1007/s10111-018-0471-5:1–10.

22 Susanne Pillath, 'Automated Vehicles in the EU' (Briefing, No PE 573.902, European Parliamentary Research Service, January 2016) 3–5 <www.europarl.europa.eu/RegData/etudes/BRIE/2016/573902/EPRS_BRI(2016)573902_EN.pdf>. In May 2016 the Australian National Transport Commission adopted the SAE J3016 (n 20) as the standard for automated vehicles in Australia: 'Regulatory Options for Automated Vehicles' (n 1) 4. In September 2016, the US *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety* report also recommended adoption of the SAE standard: Department of Transport (US), *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety* (Report, September 2016) 9.

23 Smith (n 20).

Table 1

LEVEL	Name	Narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of *dynamic driving task*	System capability (*driving modes*)	BASt level	NHTSA levels
***Human driver* monitors the driving environment**			Human driver	Human driver	Human driver	n/a		
0	**No Automation**	[T]he full-time performance by the human driver of all aspects of the dynamic driving task, even when the enhanced by warning or intervention systems					Driver only	0
1	**Driver Assistance**	[T]he driving mode-specific execution by a driver assistance system of either [the] steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task	Human driver and system	Human driver	Human driver	Some driving modes	Assisted	1
2	**Partial Automation**	[T]he driving mode-specific execution by one or more river assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task	**System**	Human driver	Human driver	Some driving modes	Partially automated	2
***Automated driving system* ("system") monitors the driving environment**			System	**System**	Human driver	Some driving modes		
3	**Conditional Automation**	[T]he driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene					Highly automated	3
4	**High Automation**	[T]he driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene	System	System	**System**	Some driving modes	Fully automated	3/4
5	**Full Automation**	[T]he full-time performance by an automated system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver	System	System	System	**All driving modes**		

The SAE categories are not mutually exclusive and shared technologies exist in the middle categories.[24] The SAE standard categorises the subtle graduation from non-automated, through semi-automated, and fully automated vehicles, and the level of human intervention, or control, required at each level.[25] As the levels of automation rise, reliance on human intervention decreases, and reliance on computer-generated control, and therefore computer-generated information, increases. Much of this information will be transmitted and received by the automated vehicle's systems as it operates to enable navigation of the immediate environment. For the purposes of information privacy this paper argues that the main difference between the categories rests with the type of information generated by each level of automation and the uses that various stakeholders may make of the information. Each stakeholder may have a different focus in relation to information generated by automated vehicles, and therefore be subject to different information privacy legislation. Additionally, individual data sets may also have multiple subject matters (such as dynamic vehicle parameters, external inputs, or person-specific data), which are all affected by the level of automation in operation.

B *Vehicles and Data*

Data produced by automated vehicles will not be homogenous but may contain data sets covering multiple subject matters which, according to Vaile, Zalnieriute and Moses, may come from various sources such as: image data external to the vehicle; image data internal to the vehicle; event data records; location/route data from navigation system; data location/route data from v2v/v2i (vehicle to vehicle/vehicle to infrastructure) communication; data covering biometric; biological or health factors; data from in-cabin microphones and entertainment systems; external microphone data; input unit data; and electronic control unit data.[26]

At all levels of automation there will likely be unique vehicle identifier tags, associated with each electronic control unit, anonymised through encryption and transmitted within the data stream while the automated vehicle is in operation.[27] The data generated by automated vehicles may be stored within the vehicle for system function or transmitted to the internet.[28]

24 Most vehicles share systems found in lower categories, eg, automatic transmissions and traction control.

25 Smith (n 20), citing J3016 (n 20).

26 Vaile, Zalnieriute and Moses (n 7) 19–23.

27 See generally Khali Persad, C Michael Walton and Shahriyar Hussain, 'Electronic Vehicle Identification: Industry Standards, Performance, and Privacy Issues' (Research Paper, Center for Transportation Research, January 2007); Khali Persad et al, *Electronic Vehicle Identification: Applications and Implementation Considerations* (Report, October 2007).

28 James M Anderson et al, *Autonomous Vehicle Techology: A Guide for Policymakers* (Report, 2016) 42–3, 75–92.

1 *Stored Data*

In relation to the vehicle, stored data is data retained in the event data recorder ('EDR')[29] used on most modern vehicles to determine the functional parameters of a vehicle in the 5 to 30 seconds surrounding a collision. All modern vehicles store collision information in some form of EDR regardless of the level of autonomy. The EDR indelibly stores data when the system is triggered by a significant event,[30] such as a rapid deceleration, change in velocity in any direction (delta-V),[31] or by the deployment of airbags.[32] The EDR records various parameters of the vehicle and may be used to determine the accuracy of a driver's account of events leading up to a collision.[33] The data recorded by the EDR includes dynamic vehicle information such as the longitudinal, lateral and vertical delta-V, speed, throttle position, engine revolutions per minute, brake application, body roll angle, safety belt usage, steering input, airbag deployment, location, and the rate of change for each parameter.[34] This information allows the reconstruction of vehicle behaviour during a collision. As the level of automation increases the importance of driver data will diminish along with the driving input. The use of stored data impacts privacy where it could be used to profile a driver beyond identifying liability in a collision. Issues relating to the use of stored data turn on who owns the data,[35] and ultimately, whether consent has been given to use the information.[36]

2 *Shared Data*

Shared data is the data shared by automated vehicles and some Cooperative Intelligent Transport Systems ('CITS')[37] such as connected, networked or platooned vehicles (collectively 'connected vehicles'). Shared data is a function of higher levels of automation, typically levels 3, 4 and 5. At levels 3 and 4, where the driver still has input into the driving task, information about the driver may

29 'Event Data Recorder', *National Highway Traffic Safety Administration* (Web Page) <www.nhtsa.gov/research-data/event-data-recorder> ('Event Data Recorder').

30 Steven T Kean, 'Event Data Recorder: An Overview' (Web Document) 2 <cdn.ymaws.com/mcaa-mn.org/resource/resmgr/files/tsrp/Resources/EDR_Overview_2-2015_-_Virgin.pdf>.

31 Delta-V represents a relative change in velocity in any direction: Hampton C Gabler, Carolyn E Hampton and John Hinch, 'Crash Severity: A Comparison of Event Data Recorder Measurements with Accident Reconstruction Estimates' (Technical Paper, SAE International, 8 March 2004).

32 Kean (n 30).

33 See generally Hampton C Gabler et al, 'Use of Event Data Recorder (EDR) Technology for Highway Crash Data Analysis' (Research Paper, Transporation Research Board of the National Academies, December 2004).

34 *Event Data Recorders*, 49 CFR § 563.7 (2008).

35 In the US for example, § 24302 of the *Driver Privacy Act of 2015* expressly holds the contents of an EDR to be the property of the vehicle owner: 49 USC § 30101 (2015).

36 Damian Kraemer, 'Who Owns Vehicle Data?', *Geotab* (Blog Post, 29 December 2016) <www.geotab.com/blog/vehicle-data-ownership/>.

37 Transport for New South Wales, 'Cooperative Intelligent Transport Systems', *Centre for Road Safety* (Web Page, 21 August 2017) <roadsafety.transport.nsw.gov.au/research/roadsafetytechnology/cits/index.html>.

be necessary for the operation of the vehicle and to allocate liability in the event of a collision. At level 5 information about the driver becomes information about the occupant and is incidental to the operation of the level 5 vehicle. Shared data technology uses Dedicated Short Range Communications ('DSRC'),[38] and between connected vehicles and infrastructure, and operate on a narrower bandwidth than that generally used in other automated vehicles.[39] Connected vehicles use DSRC to share the relative position, vector and proximity of other connected and non-connected vehicles.[40] Connected vehicles gather information in real time, sharing it with other connected vehicles in their vicinity, obviating the need for a direct line of sight as required by human-driven vehicles.[41] Connected vehicles are able to transmit and share information between vehicles up to 1,000 m away.[42] The potential data exchanged by connected vehicles, beyond that necessary for dynamic operation of the vehicle, may include vehicle identification data,[43] vehicle attributes, manufacturer information systems, accident information retrieval systems, vehicle navigation devices, driver assistance devices, Bluetooth devices, cellular devices, electronic tags for tollways, electronic tags for employers and rental car owners, and vehicle/driver log books.[44] Connected vehicles are most vulnerable at the point where they transmit data, as the shared data is transmitted in a similar manner to vehicles broadcasting directly to the internet.[45] For this reason shared data may more properly be categorised as a subset of broadcast data.

3 *Broadcast Data*

It seems likely that automated vehicles will engage with broadcast data particularly at higher levels of automation. Broadcast data is data transmitted (and received) by an automated vehicle over telecommunication networks, to a cloud repository established by the vehicle manufacturers,[46] or relevant traffic authorities.[47] Automated vehicles will transmit data, in real time, regarding vehicular kinetic parameters and control settings, in addition to location, velocity,

38 See Peter van Dijk, *Privacy Impact Assessment (PIA) for Cooperative Intelligent Transport System (C-ITS) Data Messages* (Corporate Report, March 2017) 11.

39 Typically DSRC uses the 5.9 GHz frequency: ibid.

40 'Cooperative Intelligent Transport Systems' (n 1) 7–8.

41 Brandon Schoettle, *Sensor Fusion: A Comparison of Sensing Capabilities of Human Drivers and Highly Automated Vehicles* (Report No SWT-2017-12, August 2017) 6, 9.

42 'Connected Vehicles Solutions', *Kapsch* (Web Page) <connectedvehicles.kapsch.net>; van Dijk (n 38) 11.

43 See Persad et al (n 27) 51.

44 van Dijk (n 38) 12–13.

45 See ibid 37.

46 Antonette Igbenoba, 'Autonomous Vehicles and the Internet of Things', *LeClairRyan* (Blog Post, 10 November 2016) <informationcounts.com/autonomous-vehicles-and-the-internet-of-things/>.

47 See Linghe Kong et al, 'Millimeter-Wave Wireless Communications for IoT-Cloud Supported Autonomous Vehicles: Overview, Design, and Challenges' (2017) 55(1) *IEEE Communications Magazine* 62; ibid.

and vector and occupancy information.[48] The most serious problem lies with the potential for misuse of the broadcast data produced by automated vehicles as the volumes of data involved are much greater. As automation increases, the driver input diminishes, the reliance on external information becomes greater and the quantity of data broadcast and received increases. Therefore, as the quantity of data, stored or broadcasted to repositories increases, so does the risk of interference with individual privacy, due to the greater amount of potential information exposure.[49] Accordingly, broadcast data poses the highest risk to privacy, as it may be intercepted and decrypted with the correct codes.[50]

The quality of data also changes with increasing automation. At level 3, where the driver still has input into the driving task, information about the driver may be necessary for the operation of the vehicle and for determining liability following a collision. Level 3 data is likely to relate to vehicle location and the relative position of other automated or non-automated vehicles for the purposes of navigation and collision avoidance and presumably also monitoring the internal cabin to allow it to forewarn distracted occupants if a hazard is imminent. At level 4 the identity of the driver/occupant may be necessary to determine if warnings were heeded in the event of a collision. Level 4 data would include all level 3 data and likely include geolocation data, information about the vehicle's external physical environment for internal navigation and internal occupant behaviour monitoring.[51] At level 5 information about the driver in lower levels of automation becomes information about the occupant and is likely incidental to the operation of a level 5 vehicle. Level 5 information would still include all information produced at lower levels but with a greater focus on navigation and operation of the vehicle as the human occupant would have almost no input in the control of the vehicle beyond destination requests. The unique nature of the information produced by each automated vehicle would still render them susceptible to data mining and re-identification of personal information about the driver or occupant of the vehicle.[52]

This section highlighted that as the level of automation increases, the way in which automated vehicles gather and manage data varies. As the level of automation rises, the quantity of data transmitted and received by automated vehicles increases, while the subject matter focus of the data sets also changes.

48 See Kong et al (n 47) 82; Roderick Currie, 'Developments in Car Hacking' (Paper, SANS Institute Information Security Reading Room, 2016) 20 <www.sans.org/reading-room/whitepapers/internet/developments-car-hacking-36607>.

49 See Vaile, Zalnieriute and Moses (n 7) 2.

50 See generally Bahram Honary and Garik Markarian, *Trellis Decoding of Block Codes: A Practical Approach* (Springer Science+Business Media, 1997).

51 The monitoring of occupants would likely also focus on prevention of crime within the vehicles in a similar manner to that currently used on mass transit systems: see Paul Cozens and Tiffany van der Linde, 'Perceptions of Crime Prevention through Environmental Design (CPTED) at Australian Railway Stations' (2015) 18(4) *Journal of Public Transportation* 73, 74.

52 Vaile, Zalnieriute and Moses (n 7) 7–8, 21, 55.

Part II(A) identified the different levels of automation under the SAE standard. Part II(B) argued that data created by automated vehicles can be stored, shared or broadcasted, and may contain person-specific information, in addition to dynamic vehicle data, which changes in focus with the level of automation. Closer scrutiny is therefore necessary in order to understand whether Australian information privacy law protects personal information contained within data generated by automated vehicles.

III AUTOMATED VEHICLES AND AUSTRALIAN INFORMATION PRIVACY

The main privacy issues arising from autonomous vehicles relate to interference with, or misuse of, data and that protection depends upon existing legislation covering the data generated by these vehicles. Protection under the information privacy framework turns on whether the data can be construed as information about a person. This section is structured in four parts. Part III(A) traces the development of information privacy in Australia and evaluates the decision in *Telstra* showing how it negatively impacts information privacy in Australia. Part III(B) analyses existing privacy legislation where it intersects stored data and the four main categories of data-using entities in Australia — vehicle owners, manufacturers, government, and third party entities — at various levels of automation. It highlights gaps in the ability of the privacy framework to protect stored data. Part III(C) shows that existing privacy legislation provides only limited protection where it intersects broadcast data and the four main categories of data-using entities in Australia. Part III(D) argues Commonwealth telecommunications legislation offers only minimal protection to broadcast data where it intersects the four main categories of data-using entities.

A *Information Privacy in Australia*

Privacy law in Australia has been described as 'a patchwork of common law and statute at both Commonwealth and state/territory levels'.[53] There are many pieces of legislation in Australia that make reference to privacy,[54] some of which are

53 Des Butler, 'The Dawn of the Age of the Drones: An Australian Privacy Law Perspective' (2014) 37(2) *University of New South Wales Law Journal* 434, 440.

54 For a comprehensive review of privacy legislation in Australia, see Vaile, Zalnieriute and Moses (n 7).

specific to computers and data,[55] but Australia lacks a clear statutory definition of information privacy.[56] The principal definition comes from the common law,[57] with privacy in Australia more often referred to by stating what it is not.[58] However, Australian privacy law is not as inefficient as it is generally regarded.

55 *Privacy Act 1988* (n 11); *Telecommunications Act 1997* (Cth) ('*Telecommunications Act* (Cth)'); *National Health Act 1953* (Cth) ('*National Health Act*'); *Data-Matching Program (Assistance and Tax) Act 1990* (Cth) ('*Data-Matching Act*'); *Crimes Act 1914* (Cth) ('*Crimes Act* (Cth)'); *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ('*Anti-Money Laundering Act*'); *Healthcare Identifiers Act 2010* (Cth) ('*Healthcare Identifiers Act*'); *Personally Controlled Electronic Health Records Act 2012* (Cth) ('*PCEHR Act*'); *Health Records (Privacy and Access) Act 1997* (ACT) ('*Health Records (Privacy and Access) Act*'); *Freedom of Information Act 2016* (ACT) ('*FOI Act* (ACT)'); *Territory Records Act 2002* (ACT) ('*Territory Records Act*'); *Spent Convictions Act 2000* (ACT) ('*Spent Convictions Act* (ACT)'); *Listening Devices Act 1992* (ACT) ('*Listening Devices Act* (ACT)'); *Privacy and Personal Information Protection Act 1998 (No 133)* (NSW) ('*PPIP Act*'); *Health Records and Information Privacy Act 2002 (No 71)* (NSW) ('*Health Records and Information Privacy Act*'); *State Records Act 1998* (NSW) ('*State Records Act* (NSW)'); *Criminal Records Act 1991 (No 8)* (NSW) ('*Criminal Records Act* (NSW)'); *Surveillance Devices Act 2007 (No 64)* (NSW) ('*Surveillance Devices Act* (NSW)'); *Workplace Surveillance Act 2005 (No 47)* (NSW) ('*Workplace Surveillance Act*'); *Telecommunications (Interception and Access) (New South Wales) Act 1987 (No 290)* (NSW) ('*Telecommunications Act* (NSW)'); *Crimes (Forensic Procedures) Act 2000 (No 59)* (NSW) ('*Crimes Act* (NSW)'); *Information Act 2002* (NT) ('*Information Act* (NT)'); *Criminal Records (Spent Convictions) Act 1992* (NT) ('*Spent Convictions Act* (NT)'); *Surveillance Devices Act 2007* (NT) ('*Surveillance Devices Act* (NT)'); *Telecommunications (Interception) Northern Territory Act 2001* (NT) ('*Telecommunications Act* (NT)'); *Information Privacy Act 2009* (Qld) ('*Information Privacy Act* (Qld)'); *Right to Information Act 2009* (Qld) ('*Right to Information Act* (Qld)'); *Public Records Act 2002* (Qld) ('*Public Records Act* (Qld)'); *Criminal Law (Rehabilitation of Offenders) Act 1986* (Qld) ('*Criminal Law Act* (Qld)'); *Invasion of Privacy Act 1971* (Qld) ('*Invasion of Privacy Act* (Qld)'); *Police Powers and Responsibilities Act 2000* (Qld) ('*Police Powers Act*'); *Private Employment Agents (Code of Conduct) Regulation 2015* (Qld) ('*Private Employment Agents Regulation*'); *Freedom of Information Act 1991* (SA) ('*FOI Act* (SA)'); *State Records Act 1997* (SA) ('*State Records Act* (SA)'); *Surveillance Devices Act 2016* (SA) ('*Surveillance Devices Act* (SA)'); *Telecommunications (Interception) Act 2012* (SA) ('*Telecommunications Act* (SA)'); *Personal Information Protection Act 2004* (Tas) ('*Personal Information Act* (Tas)'); *Right to Information Act 2009* (Tas) ('*Right to Information Act* (Tas)'); *Archives Act 1983* (Tas) ('*Archives Act*'); *Annulled Convictions Act 2003* (Tas) ('*Annulled Convictions Act*'); *Listening Devices Act 1991* (Tas) ('*Listening Devices Act* (Tas)'); *Telecommunications (Interception) Tasmania Act 1999* (Tas) ('*Telecommunications Act* (Tas)'); *Privacy and Data Protection Act 2014* (Vic) ('*Data Protection Act* (Vic)'); *Health Records Act 2001* (Vic) ('*Health Records Act* (Vic)'); *Freedom of Information Act 1982* (Vic) ('*FOI Act* (Vic)'); *Public Records Act 1973* (Vic) ('*Public Records Act* (Vic)'); *Surveillance Devices Act 1999* (Vic) ('*Surveillance Devices Act* (Vic)'); *Telecommunications (Interception) (State Provisions) Act 1988* (Vic) ('*Telecommunications Act* (Vic)'); *Freedom of Information Act 1992* (WA) ('*FOI Act* (WA)'); *Health and Disability Services (Complaints) Act 1995* (WA) ('*Health Complaints Act*'); *State Records Act 2000* (WA) ('*State Records Act* (WA)'); *Spent Convictions Act 1988* (WA) ('*Spent Convictions Act* (WA)'); *Surveillance Devices Act 1998* (WA) ('*Surveillance Devices Act* (WA)'); *Telecommunications (Interception and Access) Western Australia Act 1996* (WA) ('*Telecommunications Act* (WA)'). See also *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth) ('*Consequential Provisions Act*'); *Human Rights Act 2004* (ACT) ('*Human Rights Act*'); *Access to Neighbouring Land Act 2000 (No 2)* (NSW) ('*Neighbouring Land Act*'); *Charter of Human Rights and Responsibilities Act 2006* (Vic) ('*Charter*').

56 Arguably, following recent amendments, an amalgam of the *Privacy Act 1988* (n 11) and the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*Interception Act* (Cth)') now offers a partial definition of data privacy: *Interception Act* (Cth) (n 56) s 187LA(2); *Privacy Act 1988* (n 11) s 6(1) (definition of 'personal information'). The lack of statutory definition of privacy in Australia was said to be '[t]he result of legislative inaction' by Kirby P in *Australian Consolidated Press Ltd v Ettingshausen* (New South Wales Court of Appeal, Gleeson CJ, Kirby P and Clarke JA, 13 October 1993) 14.

57 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 226–7 [42]–[43] (Gleeson CJ).

58 See, eg, *WBM v Chief Commissioner of Police* (2012) 43 VR 446, 467 [89] (Warren CJ), citing *Charter* (n 55) s 13(a); ibid 226 [42] (Gleeson CJ).

Following the establishment of the ALRC in 1975,[59] the Commonwealth began to consider personal information privacy.[60]

The ALRC reported privacy was an issue in 1979,[61] and later broadened this to include information technology.[62] It noted that, while the Commonwealth has no enumerated power to make laws about privacy, the external affairs power could be used to make laws with respect to its obligations under international treaties.[63] With the signing of the *International Covenant on Civil and Political Rights* in 1980,[64] the Commonwealth recognised the right of individual citizens to privacy,[65] paving the way for federal privacy legislation.[66] Under the *Privacy Act 1988* (Cth) ('*Privacy Act*'), the Commonwealth introduced the National Privacy Principles,[67] which have now evolved into the more comprehensive Australian Privacy Principles ('APPs').[68]

The *Privacy Act* applies only to 'personal information' which is defined as:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.[69]

The APPs apply to personal information under the following numbered principles:

1. transparent management;
2. anonymity and pseudonymity;

59 The *Law Reform Commission Act 1973* (Cth) s 6(1)(a) established the Law Reform Commission to:
review laws to which this Act applies with a view to the systematic development and reform of the law, including, in particular—

> (i) the modernization of the law by bringing it into accord with current conditions;
> (ii) the elimination of defects in the law;
> (iii) the simplification of the law; and
> (iv) the adoption of new or more effective methods for the administration of the law and the dispensation of justice …

60 Law Reform Commission, *Privacy and the Census* (Report No 12, 1979).

61 Law Reform Commission, *Unfair Publication: Defamation and Privacy* (Report No 11, 1979) 3.

62 Law Reform Commission, *Privacy* (Report No 22, 1983) vol 1, xli.

63 *For Your Information* (n 10) vol 1, ch 2, 162 [2.3].

64 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

65 Ibid art 17.

66 *Privacy Act 1988* (n 11).

67 Ibid sch 1 ('Australian Privacy Principles').

68 The National Privacy Principles were amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch 1 cl 2.

69 *Privacy Act 1988* (n 11) s 6(1) (definition of 'personal information'). For an overview of the current law see also *Serious Invasions of Privacy in the Digital Era* (n 6) ch 3.

3. solicited;
4. unsolicited;
5. notification;
6. use or disclosure;
7. direct marketing;
8. cross-border disclosure;
9. government related identifiers;
10. quality;
11. security;
12. access; and
13. correction.[70]

However, the APPs only apply to Commonwealth government agencies, organisations with a turnover of more than $3 million,[71] or certain individuals.[72] Further, they only apply to information collected to be held in a record.[73] The Privacy Principles also 'apply to most state and territory government agencies',[74] in the form of Information Privacy Principles enacted under relevant state legislation.[75] The Commissioner has the power to provide advice, guidance and to monitor breaches of the APPs.[76]

Since the passing of the *Privacy Act*, Commonwealth, State and Territory

70 Australian Privacy Principles (n 67).

71 *Privacy Act 1988* (n 11) ss 6C(1), 6D; 'Regulatory Reforms' (n 6) 70.

72 *Privacy Act 1988* (n 11) s 6D.

73 Ibid ss 6(1) (definitions of 'holds' and 'collects'), 6A–6B, 6D, 6FB, 6P, 6U, 7, 7B–11, 28A, 55A, 66, 70, 86–7, sch 1.

74 'Regulatory Reforms' (n 6) 70.

75 *Information Privacy Act 2014* (ACT); *PPIP Act* (n 55); *Health Records and Information Privacy Act* (n 55); *Information Act* (NT) (n 55); *Information Privacy Act* (Qld) (n 55); *Personal Information Act* (Tas) (n 55); *Data Protection Act* (Vic) (n 55). The South Australian Information Privacy Principles are contained in Department of the Premier and Cabinet (SA), *Information Privacy Principles (IPPs) Instruction* (Instruction No 1/89, 6 February 2017).

76 *Privacy Act 1988* (n 11) pt IV div 2.

governments have all introduced a variety of legislation relating to privacy.[77] This legislation is diverse, covering areas such as, inter alia, telecommunications interception, personal information, health, spent convictions, surveillance, money laundering, employment, and whistleblower protection.[78] The ALRC notes the fragmented nature of Australian privacy laws and calls for unified national reform.[79] Existing Australian legislation does not specifically cover automated vehicle data, largely because the technology has not yet been widely deployed.[80] The fundamental question is whether the data generated by automated vehicles is 'personal information' for the purposes of the *Privacy Act*.

1 *The Decision in* Telstra

In 2017, the Federal Court of Appeal narrowed the definition of 'personal information' in *Telstra*.[81] The Full Court in *Telstra* considered the earlier definition of personal information which was 'information or opinion … about [a person] and … from which his identity is apparent or could reasonably be ascertained'.[82] At the time of the hearing this definition had been repealed and replaced with the current version, which allows external information to be considered along with the data stream. This is because the current version defines 'personal information' as

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.[83]

77 Ibid; *Telecommunications Act* (Cth) (n 55); *Data-Matching Act* (n 55); *Anti-Money Laundering Act* (n 55); *Healthcare Identifiers Act* (n 55); *PCEHR Act* (n 55); *Consequential Provisions Act* (n 55); *Health Records (Privacy and Access) Act* (n 55); *Human Rights Act* (n 55); *FOI Act* (ACT) (n 55); *Territory Records Act* (n 55); *Spent Convictions Act* (ACT) (n 55); *Listening Devices Act* (ACT) (n 55); *PPIP Act* (n 55); *Health Records and Information Privacy Act* (n 55); *FOI Act* (NSW) (n 55); *State Records Act* (NSW) (n 55); *Criminal Records Act* (NSW) (n 55); *Surveillance Devices Act* (NSW) (n 55); *Workplace Surveillance Act* (n 55); *Neighbouring Land Act* (n 55); *Crimes Act* (NSW) (n 55); *Information Act* (NT) (n 55); *Spent Convictions Act* (NT) (n 55); *Surveillance Devices Act* (NT) (n 55); *Telecommunications Act* (NT) (n 55); *Information Privacy Act* (Qld) (n 55); *Right to Information Act* (Qld) (n 55); *Public Records Act* (Qld) (n 55); *Police Powers Act* (n 55); *Private Employment Agents Regulation* (n 55); *FOI Act* (SA) (n 55); *State Records Act* (SA) (n 55); *Surveillance Devices Act* (SA) (n 55); *Telecommunications Act* (SA) (n 55); *Personal Information Act* (Tas) (n 55); *Right to Information Act* (Tas) (n 55); *Annulled Convictions Act* (n 55); *Listening Devices Act* (Tas) (n 55); *Telecommunications Act* (Tas) (n 55); *Data Protection Act* (Vic) (n 55); *Health Records Act* (Vic) (n 55); *Charter* (n 55); *Surveillance Devices Act* (Vic) (n 55); *Telecommunications Act* (Vic) (n 55); *FOI Act* (WA) (n 55); *Health Complaints Act* (n 55); *State Records Act* (WA) (n 55); *Spent Convictions Act* (WA) (n 55); *Surveillance Devices Act* (WA) (n 55); *Telecommunications Act* (WA) (n 55).

78 See above n 55 and accompanying citations.

79 *For Your Information* (n 10) 189–90 [3.1].

80 'Regulatory Reforms' (n 6) 10.

81 *Telstra* (n 16).

82 Ibid 25 [3] (Dowsett J).

83 *Privacy Act 1988* (n 11) s 6(1) (definition of 'personal information'). For the purposes of this paper, 'about' is interpreted to have its plain and ordinary meaning: *Acts Interpretation Act 1901* (Cth) s 15AB(3)(a).

However, this has not been tested in court so remains subject to interpretation.[84] In *Telstra*, the Full Court affirmed the earlier decision in *Re Telstra Corp Ltd v Privacy Commissioner*,[85] which expressly rejected a broad interpretation of the definition of personal information, stating:

> [T]he questions that are asked must be framed in terms of the definition. They cannot be asked against a different frame of reference that has, as its starting point, the question: is it possible to use this information or opinion or to marry it with other information by using a computerised search engine or in some other way to ascertain the identity of an individual. The starting point must be whether the information or opinion is *about an individual*. If it is not, that is an end of the matter and it does not matter whether that information or opinion could be married with other information to identify a particular individual.[86]

This narrowed the interpretation of personal information so as to permit data produced by automated vehicles to be accessed if the data is not specifically about an individual as the subject of the information.[87] For automated vehicles, the Court's reasoning on the preposition 'about' allows information contained within the data stream to be compartmentalised because, according to the Court, information can have multiple subject matters:

> The words 'about an individual' direct attention to the need for the individual to be a subject matter of the information or opinion. This requirement might not be difficult to satisfy. Information and opinions can have multiple subject matters.[88]

Although the Court did not go on to define 'multiple subject matters' it could include information produced for several different purposes. The Court indicated that 'multiple subject matters' would require an evaluative conclusion to be drawn on a case by case basis.[89] Accordingly, for automated vehicles, this decision requires the court to treat each individual data stream separately to see if the subject matter is information about a person, and if identifiers that make the information about a person are contained within each specific data stream. It looks at the *purpose* of the data, for instance whether it is used to further the transmission of operational information, and not whether it is capable of identifying an individual when combined with other streams, even if those data streams emanate from the same vehicle (which would be the multiple subject matters). For automated vehicles,

84 The new definition of 'personal information' in the *Privacy Act 1988* (n 11) includes the following note that broadens the definition of personal information: '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': at s 6(1) (definition of 'personal information').

85 *Re Telstra Corp Ltd* (n 17).

86 Ibid 115 [95] (Forgie DP) (emphasis added).

87 Note that this does not mean that a court would be bound to find in the same manner under the current definition of personal information.

88 *Telstra* (n 16) 36 [63] (Kenny and Edelman JJ).

89 Ibid.

such an 'evaluative conclusion' would turn on whether the subject matter of the information stream was about the operation of the vehicle, or about the driver or occupant as would be the case in higher levels of automation.

Separating identification information from vehicle systems and traffic information is seen as one way to protect data produced by automated vehicles.[90] Dividing automated vehicle data into separate categories may help delineate the multiple subject matters and assist categorising which data requires protection. This would accord with the *Telstra* decision, by allowing operational data to be used by the system where necessary, as automated vehicle networks will be highly dependent on data sharing for the safe operation of the automated mass transport system. Notwithstanding this, information privacy appears to be an impediment to the broad implementation of automated vehicles by increasing the complexity of compliance.

This part has shown that, following the decision in *Telstra,* legislative provisions designed to protect information privacy will not adequately protect automated vehicles. Further, it highlighted the need for an examination of the current legislative frameworks surrounding information privacy and automated vehicles. Determining if the privacy framework protects automated vehicle data requires examination of legislation where the main entities intersect broadcast or stored data at each level of automation.

B *Stored Data and Privacy Legislation*

The four main entities that use stored data are: vehicle owners, manufacturers, government, and third party corporate interests. This section considers how the *Privacy Act*[91] impacts stored data and each of these entities. It examines the four main entities in turn, at each relevant level of automation, beginning with the individual owner of the vehicle.

1 *Individual Owner*

The individual owner of a motor vehicle in Australia is entitled to access and use any system in the vehicle unless expressly proscribed.[92] Legislative proscriptions

90 In a submission to the House of Representatives Standing Committee on Industry, Innovation, Science and Resources, the Federal Chamber of Automotive Industries recommended data generated by automated vehicles be divided into three categories: '[t]raffic information: currently collected and collated by infrastructure owners for traffic management'; '[v]ehicle owner/driver information: data created by use of the vehicle', eg position, location, velocity, etc; and '[v]ehicle systems operation: data contained within the vehicle management modules to control how the vehicle operates': Federal Chamber of Automotive Industries, Submission No 24 to House of Representatives Standing Committee on Industry, Innovation, Science and Resources, Parliament of Australia, *Inquiry into the Social Issues Relating to Land-Based Driverless Vehicles in Australia* (10 February 2017) 10.

91 *Privacy Act 1988* (n 11).

92 This is based on the old English doctrine of *nulla poena sine lege* ('no penalty without a law'): see Jerome Hall, '*Nulla Poena Sine Lege*' (1937) 47(2) *Yale Law Journal* 165.

typically restrict interference with performance or safety systems, and apply only to vehicles driven on public roads.[93] Privacy legislation in this area is almost non-existent and the individual owner would only find difficulty in accessing the contents of an EDR where the unit was already withheld by the police in an investigation.[94] In a submission to the recent House of Representatives report,[95] it was recommended that access to data stored in the EDR should be streamlined to reduce protracted and complex litigation.[96] As data stored on the vehicle EDR forms part of the vehicle, it will be classed as private property, which includes any vehicle sub-system or componentry. However, individual ownership is likely to only be an issue at the lower levels of automation, typically SAE levels 1–3, as at higher levels the automated vehicle system may not resemble a private property model at all.[97] For the higher levels it is anticipated that manufacturers or third party entities will control and own the entire automated vehicle fleet.[98] At these levels of automation, typically levels 4 and 5, the occupant will likely be a third party having no rights over the EDR, or any other data management system. At present, information stored in an EDR is encrypted with operating systems and encryption codes subject to copyright protection.[99] Therefore, at SAE levels 1–3 it is likely that individual owners would be unable to access information stored in an EDR, even if able to prove ownership of the vehicle.

The Act sets out several APPs that may apply to the handling of data stored in an EDR.[100] Individuals have a general right to protection of data,[101] and to know how to find out what personal information is contained within the EDR.[102] As the EDR is only activated by a serious event,[103] it is often retrieved during the post-collision investigation.[104] At this point the stored data passes into the control of another entity, usually the vehicle or software manufacturer, for decoding.[105]

93 *Motor Vehicle Standards Act 1989* (Cth) s 5(1) (definition of 'road vehicle').

94 *Crimes Act* (Cth) (n 55) pt IAA div 2; *Crimes Act 1900* (ACT) pt 11; *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW) pt 5 div 2; *Police Administration Act 1978* (NT) pt VII div 2; *Police Powers Act* (n 55) ch 7; *Summary Offences Act 1953* (SA) s 80; *Criminal Investigation (Extraterritorial Offences) Act 1984* (SA) s 5; *Search Warrants Act 1997* (Tas) s 10; *Crimes Act 1958* (Vic) pt IIA; *Criminal Investigation Act 2006* (WA) pt 5.

95 *Social Issues Relating to Land-Based Automated Vehicles in Australia* (n 6).

96 Katie Minogue, Submission No 25 to House of Representatives Standing Committee on Industry, Innovation, Science and Resources, Parliament of Australia, *Inquiry into the Social Issues Relating to Land-Based Driverless Vehicles in Australia* (13 February 2017) 8.

97 European Commission, *Gear 2030: High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the European Union* (Final Report, October 2017) 19 ('*Gear 2030*').

98 Brady (n 5) 57.

99 See generally 'Types of IP', *IP Australia* (Web Page) <www.ipaustralia.gov.au/understanding-ip/getting-started-with-ip/types-of-ip>.

100 Australian Privacy Principles (n 67).

101 Ibid cl 12.

102 Ibid cl 1.4(d).

103 Kean (n 30) 2–3.

104 Gabler, Hampton and Hinch (n 31).

105 See generally Gabler et al (n 33).

Data management made by an entity in possession of the EDR must be 'open and transparent'[106] with specific policies in place to ensure procedural compliance for data handling.[107] The individual owner has the right to know what policy is in use,[108] and is entitled to know what use is made of the stored data.[109] Further, they have a right to know with whom their personal information is shared, and may in certain circumstances apply to correct information held about them.[110] Individual owners have a right under the Act to use information for their own personal affairs,[111] and have a right to request to be de-identified.[112] However, in an investigation post-collision,[113] this may not be possible where it is 'reasonably necessary'[114] for authorities to know the individual's identity.[115]

Where the EDR contains unsolicited information about an individual, no protection is afforded where it is recovered ancillary to an investigation,[116] with the only obligation being to notify a person, where practicable, that the recovered EDR contains information about them.[117] Where an entity transfers stored data to a third party,[118] there is limited protection if it is used to determine the functional parameters of a vehicle surrounding an accident,[119] and the only caveat is that it is noted in writing.[120] The exception is where information is transferred to a third party for the purposes of direct marketing,[121] which is unlikely in the circumstances. Transfer of the stored EDR data, to an extraterritorial entity, such as a parent company for decoding purposes, is also not protected where it is required for the accident investigation.[122] However, as Vaile, Zalnieriute and Moses argue, absent other information enabling cross-referencing, the probability of the EDR being misused to derive personal information is low.[123] Nevertheless, the Act provides only limited protection to the individual in relation to the privacy of stored data.

106 Australian Privacy Principles (n 67) cl 1.1.
107 Ibid cls 1.2–1.3.
108 Ibid cl 1.6.
109 Ibid cl 12.1.
110 Ibid cls 12–13.
111 *Privacy Act 1988* (n 11) s 16.
112 Australian Privacy Principles (n 67) cl 2.1.
113 Ibid cl 2.2.
114 Ibid cl 3.1.
115 Ibid cl 3.
116 Ibid cls 4.3–4.4.
117 Ibid cl 5.
118 Ibid cl 6.
119 Ibid cl 6.2(a).
120 Ibid cl 6.2(e).
121 Ibid cl 6.7(a).
122 Ibid cl 8.2(c).
123 Vaile, Zalnieriute and Moses (n 7) 20.

2 *Manufacturers*

The manufacturers of in-vehicle storage systems, including the EDR and other data manipulation software, have the capability to access data stored within the systems that they produce. At all levels of automation, from SAE levels 0–5, the manufacturers will be able to access and use the data stored within an automated vehicle for purposes relating to vehicle operation and safety. At the higher levels of automation, levels 4 and 5, the manufacturers will likely retain ownership of the automated vehicle fleet, with access being granted as part of a bundle of rights purchased by consumers using the system rather than the current model of ownership where a motor vehicle is treated as a chattel kept in a garage.[124] For manufacturers to access data within the EDR, or similar systems in an automated vehicle, they currently require close proximity,[125] or direct contact with the vehicle.[126] Issues of authority to access the data would turn on whether permission was given by the vehicle owner or allowed by legislation. The use of any information, from an EDR, or other storage device retrieved by a manufacturer, falls within the scope of the *Privacy Act*.[127]

The *Privacy Act* sets out what constitutes an interference with privacy.[128] A vehicle or software manufacturer would likely have a turnover of $3 million per year which would automatically enliven the Act.[129] As Australia no longer manufactures automobiles, the automated vehicle manufacturers will likely be extraterritorial entities.[130] The collection of personal information, being reasonably necessary to the determination of vehicle dynamics, is also allowed.[131] Further, a manufacturer may use stored data to further research into accident avoidance and safety enhancement,[132] which is the primary purpose of EDR use. The cross-border flow of data removed from an EDR, when sent to the parent company of the manufacturer, is also permitted under the Act as the extraterritorial entity[133] satisfies the related body corporate requirement.[134] A manufacturer may refuse access to personal information where a person is engaging in litigation against

124 Evidence to Joint Standing Committee on Road Safety, Parliament of New South Wales, Sydney, 20 June 2016, 15 (Mark Brady).

125 Data from EDRs may in future be broadcast and stored, locally or offshore, by manufacturers or service providers, or their agents.

126 See Hampton C Gabler et al (n 33).

127 *Privacy Act 1988* (n 11).

128 Ibid s 13.

129 Ibid ss 6C–6D.

130 Australian Privacy Principles (n 67) cl 8.

131 Ibid cl 3.

132 Ibid cl 6.2(a).

133 Ibid cl 8.

134 *Privacy Act 1988* (n 11) s 13B.

it,[135] which occurs in some product liability litigation after motor vehicle accidents.

In addition to the requirements to have readily accessible policies on the use and protection of data,[136] manufacturers must have a complaints,[137] and correction system available to persons whose data they are holding.[138] Data anonymity requirements are met as the EDR is encrypted,[139] and the collection of data whether solicited,[140] or unsolicited,[141] would be reasonably necessary to determine the behaviour of the vehicle in an accident.[142] Moreover, this information would be collected automatically with the original data on the EDR.[143] Notification would only be required where the information was personal and this only occurs once the contents of the EDR are combined with the vehicle owner's details held by the police, or the court, after the decoding process is finished and the data transferred to investigators.[144] The rights of manufacturers to stored data would also be proprietary in nature and protected as intellectual property.[145] Consequently, manufacturers dealing with stored data from an automated vehicle would not be liable under the *Privacy Act* unless transferring personal information to direct marketing entities, without permission.[146]

3 *Government or State Entities*

Information generated by automated vehicles will be of interest to various Commonwealth, state and territory entities, including such entities as the Australian state and federal police, main roads departments, insurance commissioners, the Australian security services, and the Department of Human Services (in order to track movements of Centrelink clients).[147] The uses made of the information will include policing, compliance, risk management, eligibility, security, infrastructure planning and behavioural control. At each level of automation, from SAE levels 0–5, the data relating to vehicular parameters stored within an automated vehicle EDR will be similar. Where permission to

135 This is where 'the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings': Australian Privacy Principles (n 67) cl 12.3(d).

136 Ibid cl 1.3.

137 Ibid cls 1.2, 1.4(e), 5.2(h), 12.9(b), 13.3(b).

138 Ibid cl 13.

139 Ibid cl 2.

140 Ibid cl 3.

141 Ibid cl 4.

142 *Privacy Act 1988* (n 11) s 16A; ibid cls 3.1–3.2, 3.3(a).

143 Australian Privacy Principles (n 67) cl 4.4.

144 Ibid cl 5.

145 For intellectual property of corporations see *IP Australia* (n 99).

146 Australian Privacy Principles (n 67) cl 7.

147 See generally Lyndal Sleep and Kieran Tranter, 'Social Media in Social Security Decision-Making in Australia: An Archive of Truth?' (2018) 22(4) *Media and Arts Law Review* 442.

use, transfer, or manipulate stored data is established, it is usually given with the authority of an entity of the state and only otherwise given by consent or under contract between parties. The *Privacy Act* binds the Crown,[148] while exempting the Crown from prosecution for any offence under the Act.[149] Nevertheless, the state has a duty 'to promote responsible and transparent handling of personal information'[150] under the *Privacy Act*,[151] and this affords some protection of stored data held in an in-vehicle EDR. The *Privacy Act* provides APP entities must comply with the APPs.[152] The *Privacy Act* defines an APP entity for the purposes of the Act to include an agency or an organisation.[153]

The *Privacy Act* defines 'agenc[ies]' to include most government departments,[154] and 'organisations' include everything from individuals to bodies corporate, whether private or statutory.[155] The *Privacy Act* sets out who is the principal executive of each agency.[156] The various entities of the state that may deal with stored data include: the courts, police services, the Australian Security Intelligence Organisation, or any other department, organisation, or APP entity, that the state deems responsible, or exempt from liability from time to time when dealing with personal information gathered from in-vehicle stored data.[157] The state is vicariously liable for the actions of its agents or employees.[158]

There are many provisions in the *Privacy Act* that regulate the behaviour of government or state entities in relation to the handling of stored data.[159] The state is able to determine what authority is given to whom and when it is applicable.[160] As the arbiter of who is authorised to use information and for what purpose, the state is unlikely to hold liability for the use of stored data in an EDR, as the use of the information[161] would fall within one of the exemptions under the *Privacy Act*.[162] State interest in stored data is ultimately limited by the greater quantities of information involved in broadcast data, which enable a more thorough pattern

148 *Privacy Act 1988* (n 11) s 4(1).

149 Ibid s 4(2).

150 Ibid s 2A(d).

151 Ibid ss 2A(d), 21B, 22A; Australian Privacy Principles (n 67) cl 1.1.

152 *Privacy Act 1988* (n 11) s 15.

153 Ibid s 6(1) (definition of 'APP entity').

154 Ibid s 6(1) (definition of 'agency').

155 Ibid s 6C.

156 Ibid s 37.

157 Ibid ss 6(1) (definitions of 'APP entity' and 'agency'), 6C(1), (3).

158 *Century Insurance Co Ltd v Northern Ireland Road Transport Board* [1942] AC 509, 519.

159 See generally *Privacy Act 1988* (n 11).

160 'Infosheet 20: The Australian System of Government', *Parliament of Australia* <www.aph.gov.au/About_Parliament/House_of_Representatives/Powers_practice_and_procedure/00_-_Infosheets/Infosheet_20_-_The_Australian_system_of_government>.

161 Usually the only time an EDR is examined is for the purposes of an investigation into a motor vehicle accident and the data stream lasts a very short time, typically less than one minute.

162 *Privacy Act 1988* (n 11) ss 7B, 7C, 26D, 34.

of behaviour to be gleaned from the data produced.

4 *Third Party Corporate Interests*

Third party corporate interests are corporations that may benefit from the use of data, particularly the high volumes of data set to be generated by automated vehicles. They may be information-centred entities such as motor vehicle insurance companies and software providers, or direct marketing companies, with a vested interest in the data contained within the EDR of automated vehicles. At each level of automation, from SAE levels 0–5, the data relating to vehicular parameters stored within an automated vehicle EDR will be similar. The fundamental question is whether the data generated by an automated vehicle is information 'about' a person for the purposes of the *Privacy Act*.[163] This is determined by assessing whether the data stored within the automated vehicle EDR contains information about an individual 'from which [their] identity is apparent or could reasonably be ascertained'.[164] The next question is whether the consent to use the information was given expressly or by implication. Further to this is whether the permission to use the information was validly made. Additionally, does the *Privacy Act* allow parties to avoid liability where consent was given impliedly? Finally, does the permission allow third party corporations to effectively contract out of the *Privacy Act*?

To determine these questions requires an examination of the ways consent is given in relation to each type of entity and how the information is used. These may be, for example, expressly contained in a signed insurance policy, or implied in an end user licence agreement to be found in electronic based media.[165] In an insurance policy there is often some form of written agreement,[166] which typically includes terms and conditions pertaining to the insurance company's privacy policy clarifying the use that may be made with information. The gathering of information is usually necessary for the purposes of an accident investigation following a collision that results in property damage or personal injury and the express permission would allow the insurance company to harvest the data stored in the EDR.

For an end user licence agreement as, for example, often found in a 'click-wrap' style software agreement, there is frequently a check box located on the screen

163 Ibid s 6(1) (definition of 'personal information').

164 See especially *Telstra* (n 16) 25 [3] (Dowsett J). See also ibid.

165 See John Adams, 'Digital Age Standard Form Contracts under Australian Law: "Wrap" Agreements, Exclusive Jurisdiction, and Binding Arbitration Clauses' (2004) 13(3) *Pacific Rim Law & Policy Journal* 503.

166 For validity of signature in contract see: *L'Estrange v F Graucob Ltd* [1934] 2 KB 394.

to signify agreement with the contract.[167] By checking the box,[168] the end user grants permission to the technology company allowing it to use and disseminate any information at its discretion to third parties for profit or other purposes.[169] Before proceeding to the check box stage, it is often required that the individual reads the privacy policy of the company before agreeing with the terms of the contract.[170] Once this is completed, and the check box is 'clicked', the rights over the information transfer to the company to use and share as they see fit within the agreement.[171] The effectiveness of any end user licence agreement depends on the ability of the company to enforce the agreement, usually a question of fact following a dispute between the parties to the agreement.[172] Where the agreement is held to be valid, the company is protected against any claim made against it in relation to the use of the client's information according to the agreement.

It is at the point of examination that the check box style of agreement may falter,[173] where the agreement might be found to be invalid and therefore unenforceable.[174] Here the *Privacy Act* provides some protection in relation to the use or misuse that has been made of the information. A closer examination of the contract and the amount of attention drawn to the terms of the agreement is necessary,[175] on a case by case basis, to see whether the use of the data was validly made under the contract.[176] The most important consideration is whether the parties have contracted out of the *Privacy Act*, and if not, whether the Act protects the information that is the subject of the agreement. Under the *Privacy Act*, the consent given to use information is sufficient to protect the party using it for the agreed purpose.[177] This means it is possible to contract out of the *Privacy Act* with a valid agreement. A party cannot contract out of the *Privacy Act* when consent is absent.[178] Here the APPs prohibit the use by third parties of information, for the purposes of direct marketing, without consent.[179]

167 Adam Gatt, 'Electronic Commerce: Click-Wrap Agreements' (2002) 18(6) *Computer Law & Security Report* 404, 405.

168 For enforceability of online agreements see: *Smythe v Thomas* (2007) 71 NSWLR 537, 546–7 [35]–[38].

169 Adams (n 165) 510–11.

170 See generally ibid. See also David Bolton, 'Shrink-Wrap and Click-Wrap Contracts' [2009] (95) *Precedent* 10.

171 See generally Gatt (n 167) 408.

172 Gordon Hughes and Andrew Sutherland, 'Enforcement Problems with Online Contracts: An Uber Case Study', *Davies Collison Cave* (Web Article, 5 October 2016) <dcc.com/services/trade-marks/domain-name-protection-disputes/enforcement-problems-with-online-contacts-an-uber-case-study/>.

173 Ibid.

174 Adams (n 165) 503.

175 *Thornton v Shoe Lane Parking Ltd* [1971] 2 QB 163, 170.

176 *Peekay Intermark Ltd v Australia & New Zealand Banking Group Ltd* [2006] EWCA Civ 386, [40].

177 *Privacy Act 1988* (n 11) ss 6(1) (definition of 'consent'), 6D(7)–(8), 16A–16C, 80Q; Australian Privacy Principles (n 67) cl 3.3.

178 Australian Privacy Principles (n 67) cls 4–5, 7.

179 Ibid cl 7.3(b).

Corporate interests may use data, for purposes other than direct marketing, under the *Privacy Act* where it is not passed to third parties. Information technology companies exist in an area where personal information obtained by the questionable method of click-wrap style consent is relatively unregulated.[180] Information may then be onsold to third parties who use the information as they see fit.[181] This becomes a serious problem if the check box style of consent is given for the use of personal information obtained from automated vehicles. Once permission is given, and unless it is later withdrawn, the recipient third party may use all future data at will. At this point, the *Privacy Act* offers no protection to the privacy of individual personal data stored in the EDR of automated vehicles.

This section has shown that where consent is absent, the *Privacy Act* offers some protection of the data contained within an EDR of an automated vehicle. For the individual owner of the vehicle, the *Privacy Act* sets out how the data may be handled and used. For government and manufacturers the *Privacy Act* sets out their responsibilities in handling personal information. Third party corporate interests are covered under an all or nothing approach. Absent consent they are prohibited from using the data, but with consent they may do as they see fit with personal information if within the terms of the agreement. Information taken from an EDR or intercepted between short-range inter-vehicle communications from connected vehicles may allow third parties to develop a pattern of behaviour of a person, though not as easily as with broadcast data.[182] With broadcast data, the situation is different due to both the greater volumes of data involved, and how that data may be used.

C *Broadcast Data and Privacy Legislation*

Broadcast data is quantitatively on another level than stored data. Broadcast data is continuously transmitted between the vehicle, third parties, and infrastructure. This 'conversation' between the automated vehicle and other systems is ongoing and constantly mediated whenever the vehicle is operational. The subject matter of broadcast data and the type of data produced changes with the level of automation.[183] Further, the quantity of data generated by this process is huge compared with stored data which typically only records for around less than a minute.[184] The number of nodes where this data intersects is constantly changing as the vehicle moves, and the potential for security breaches in broadcast data is exponentially greater than with stored data. This section argues that the

180 See generally Gatt (n 167).

181 Ibid 408.

182 Both generally require close proximity to the vehicle in order to retrieve data and an EDR only records data for a few seconds: 'Event Data Recorder' (n 29).

183 Brady (n 5) 49.

184 Ibid.

information privacy frameworks are ineffective at protecting broadcast data. It examines where the privacy law intersects each of the four main entities: vehicle owners, manufacturers, government, and third party corporate interests. This part shows how the privacy of broadcast data is limited under the *Privacy Act*.

1 *Individual Owner*

The individual owner of a vehicle has a basic right of ownership over the vehicle and its systems.[185] However, it is highly probable that the proprietary nature of the communication between the automated vehicle and the internet would be the intellectual property of the manufacturer, or fleet operator, and outside the individual owner's realm of control in a similar way to the operating system in a personal computer.[186] The *Privacy Act* affords some protection to the individual owner, where the information broadcast can be used to identify them, or their personal information.[187] This protection is limited with the caveat, 'unless the information is reasonably necessary for … one or more of the [receiving] entity's functions or activities'.[188] This is likely to be the case with automated vehicles as accessing the vehicular data stream would be 'reasonably necessary' for the network to function.[189] The use that is made of broadcast information is restricted under the *Privacy Act*, here the recipient of the information is required to follow specific policy[190] in relation to that use.[191] Further, there must be procedures in place to allow the individual owner to access,[192] dispute,[193] and alter data held by the recipient.[194]

At SAE levels 1–3, data will likely not be broadcast unless it becomes prescribed as a requirement for all road vehicles as part of the automated and connected vehicle infrastructure.[195] If this situation occurs, then at levels 1–2, the data broadcast will primarily be about vehicle dynamics such as location, velocity, vector and delta-V. This information will be used by other vehicles and infrastructure in the CITS and automated vehicle system to make the infrastructure safer during the transition phase. At SAE level 3, this will also include information about the

185 See generally BJ Edgeworth et al, *Sackville and Neave: Australian Property Law* (LexisNexis Butterworths, 8th ed, 2008) 57–75.

186 See *IP Australia* (n 99).

187 Australian Privacy Principles (n 67) cls 3, 4, 6, 11.

188 Ibid cls 3.1–3.2. See also at cls 3.3–3.4.

189 Ibid cls 3.1–3.4.

190 *Privacy Act 1988* (n 11) pt IIIB.

191 Australian Privacy Principles (n 67) cl 1.2.

192 Ibid cl 12.

193 *Privacy Act 1988* (n 11) ss 36, 40.

194 Australian Privacy Principles (n 67) cl 13.

195 Lucas Mearian, 'Why Your Car Will Be Connected to the Internet by 2020', *Computerworld* (Online Article, 8 April 2015) <www.computerworld.com/article/2907540/why-your-car-will-be-connected-to-the-internet-by-2020.html>.

driver and their behaviour in response to warnings given by the vehicle about system failures, or to retake control of the vehicle.

At SAE level 4, in addition to what will be broadcast at the lower levels of automation, the subject matters widen to include a variety of data sets, such as images broadcast from external cameras about the vehicle surroundings,[196] infrastructure, and traffic for the purposes of maintaining an operational real time infrastructure modelling. Internal cameras may monitor the occupants in a similar way that public transport observes the behaviour of occupants to minimise noncompliance with societal norms.[197] Other information may also be broadcast regarding the occupants, such as identity, destination, media access, biometric data and, where permission is given, marketing preferences.[198] At level 4 these data streams may be separated or transmitted together on the same bandwidth. As the rollout of higher level automated vehicles progresses, this will become clearer.

At SAE level 5 the multiple data streams may be largely separate and will likely be encrypted in a rolling pseudonym.[199] One data stream would contain all the dynamic operational information for the vehicle and any internal functional parameters. Information will also be sent to infrastructure to build a comprehensive environmental model in real-time for all vehicles using the transport network. Information about the occupants will be contained within a separate data stream and will largely be based around their journey, their starting and finishing locations, and their integrated cellular and internet access, as well as for behavioural compliance.[200] It will also contain detailed personal information including biometrics, social and interactive media, marketing preferences (which may be the price of entry to the system).[201]

A major problem arising is the inability to identify who is in receipt of the broadcast data.[202] Without identification of the recipient, there is no possibility of enforcing rights under the *Privacy Act*. This leaves the individual owner with limited protection and renders the *Privacy Act* impractical in relation to broadcast data. Additionally, the quantity of data being monitored may be so large that

196 Zak Doffman, 'Smarter Cities: Will Autonomous AI Surveillance and IoT Now Automate Law Enforcement?', *Forbes* (Online Article, 15 December 2018) <www.forbes.com/sites/zakdoffman/2018/12/15/smarter-cities-will-autonomous-ai-surveillance-and-iot-now-automate-law-enforcement/#37e60bf21d55>.

197 Brian Cooley, 'In-Car Monitoring: Surveillance Tech Will Make Your Car Less Private: Everything You Do in Your Car May Soon Be Noticed', *CNET* (Online Article, 12 March 2019) <www.cnet.com/roadshow/news/in-car-monitoring-surveillance-technology-privacy/>.

198 See generally Lee (n 3); 'Automated Vehicle Data' (n 6) 34–5.

199 'Automated Vehicle Data' (n 6) 21–35.

200 See Doffman (n 196).

201 'Automated Vehicle Data' (n 6) 21–35; Lee (n 3) 29, 33–4.

202 See generally Alana Maurushat, 'Australia's Accession to the *Cybercrime Convention*: Is the *Convention* Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?' (2010) 33(2) *University of New South Wales Law Journal* 431, 433–5; Russell G Smith, *Impediments to the Successful Investigation of Transnational High Tech Crime* (Publication No 285, October 2004).

it overwhelms any individual seeking to extract some meaningful information from it without using data mining techniques. The data transmitted is likely to include both vehicle telemetry and encrypted two-way communication between the vehicle and infrastructure precluding access by the individual. Further, the *Privacy Act* makes contracted service providers, in the provision of a service under a Commonwealth contract (the likely controller of transport infrastructure contracts), exempt from breaching the APPs.[203]

2 *Manufacturers*

The manufacturers of automated vehicles look set to have a greater ongoing commitment to the operation and monitoring of these vehicles as the liability arising from their use will likely be greater.[204] This will include using two-way telemetry and monitoring and collecting broadcast data produced by automated vehicles. It is predicted that manufacturers will be heavily involved in the operation of the automated vehicle fleet throughout the operational life of these vehicles.

At SAE levels 3 and 4, the manufacturer may receive mission-critical data for automated vehicles and will be in receipt of data about the occupants for the purposes of heeding warnings and establishing liability where necessary. At higher levels of automation, SAE levels 4 and 5, the manufacturer will also likely be the owner of the vehicle and the data about the occupant becomes proprietary in nature and the occupant may also be a party to the contract of service (transport) or they may be merely a third party using the system. Again, the provision of personal data to the manufacturer (or fleet operator) may by then be the ubiquitous cost of access to the system. Where the manufacturer stores information about the occupant, the *Privacy Act* will provide some protection.

The *Privacy Act* applies to the use and control of broadcast data collected by manufacturers because the manufacturers are APP entities[205] for the purposes of the Act.[206] Where the manufacturers are situated in another country but have an ongoing two-way interaction with the vehicles, questions arise as to whether the *Privacy Act* still applies to them. This is particularly relevant where the broadcast data is collected and sent to a subsidiary company or parent company, which are deemed to be related under the *Privacy Act* and therefore exempt.[207] As set out in Part III(B)(2), all the same requirements for storage and access to data under

203 *Privacy Act 1988* (n 11) s 6A(2).

204 See generally Mark Brady et al, 'Automated Vehicles and Australian Personal Injury Compensation Schemes' (2017) 24(1) *Torts Law Journal* 32.

205 *Privacy Act 1988* (n 11) s 6(1) (definition of 'APP entity').

206 Ibid s 6C(1)(b).

207 Ibid s 13B.

the *Privacy Act* still apply.[208] The public interest in having a safer global mass transport system will pave the way for the manufacturers to avoid breaching the APPs in the future but the *Privacy Act* will nevertheless require modification to specifically deal with automated vehicles.

3 *Government or State Entities*

Commonwealth, state and territory entities will have an interest in information broadcast by automated vehicles for such diverse purposes as policing, compliance, risk management, eligibility, security, traffic, infrastructure development and behavioural control. There are many provisions in the *Privacy Act* regulating behaviour of government or state entities in relation to the handling of broadcast data.[209] At all SAE levels of automation the responsibilities of the state remain the same. The state has a duty to 'promote responsible and transparent handling of personal information' under the *Privacy Act*,[210] and this affords some protection of broadcast data received by a government or state entity. APP entities are responsible under the *Privacy Act* for the handling and management of information that comes into their possession.[211] As with stored data, the *Privacy Act* defines an APP entity to include an agency or an organisation.[212] Agencies are further defined to include most government departments,[213] and organisations include everything from individuals to bodies corporate whether private or statutory.[214] The *Privacy Act* stipulates that APP entities must comply with APPs,[215] and sets out the principal executive of each agency.[216] Once again the state is unlikely to hold liability for the use of broadcast data as its use of the information would fall within one of the exemptions under the *Privacy Act*.[217]

4 *Third Party Corporate Interests*

The third party interest in automated vehicles will be large and wide ranging. It is likely that the future automated vehicle fleet will be populated with multiple overlapping interests, many of a proprietary nature, that function to create an operational automated vehicle. Third party interests will include various stakeholders, including telecommunications providers, software developers, programmers, hardware manufacturers, encryption coding entities, control

208 See above Part III(B)(2).

209 See above Part III(B)(3).

210 *Privacy Act 1988* (n 11) s 2A(d). See also at ss 21B, 22A; Australian Privacy Principles (n 67) cl 1.1.

211 See above Part III(B).

212 *Privacy Act 1988* (n 11) s 6(1) (definition of 'APP entity').

213 Ibid (definition of 'agency').

214 Ibid s 6C.

215 Ibid s 15.

216 Ibid s 37.

217 Ibid ss 7B, 7C, 26D, 34.

system operators, infrastructure providers, and those who seek to profit from advertising and data mining.[218] These participants will be involved to varying degrees in the creation and operation of the vehicle. As with stored data, liability vanishes where permission to use and disseminate the data is granted.[219] Third party corporate liability under the *Privacy Act* in relation to broadcast data will turn on how they use the data. If the use is wholly within the corporate control of the third party entity then it is unlikely to be subject to the Act.

At SAE levels 1–2, data will only be broadcast in relation to the dynamic operation of the vehicle in relation to infrastructure and other vehicles. At SAE level 3, this information will also include information regarding the identity of the driver and whether they have heeded any warnings in the event of a malfunction or emergency. At SAE levels 4–5, the data may be separable into dynamic vehicular information and personal information about the occupant as well as to monitor behaviour within the vehicle for compliance with societal norms.[220] The vehicular information will be of interest to those stakeholders in the automated and connected vehicle operation and infrastructure. The information about the occupant will be of specific interest to marketing companies.

Under the current framework, the primary question is whether the broadcast data, retained by third party corporate interests, is considered information 'about' a person', for the purposes of the *Privacy Act*.[221] The next consideration is the third party's use of the information. Where one may require information about the general operation of a vehicle, or for the taking of safety precautions,[222] risk assessment,[223] or to determine liability in motor vehicle accidents,[224] another may seek to understand individual or group proclivities and/or vulnerabilities[225] in order to profit from impulse purchasing.[226] Again, the recent *Telstra* decision[227] offers limited protection against data mining,[228] and there are growing concerns

218 See Lee (n 3).

219 See Hughes and Sutherland (n 172); Adams (n 165); Gatt (n 167) 405. See also provisions relating to stored data as set out in Part II(B)(1).

220 See above n 51.

221 *Privacy Act 1988* (n 11) s 6(1) (definition of a 'personal information').

222 DJ Gabauer and HC Gabler, 'Comparison of Delta-V and Occupant Impact Velocity Crash Severity Metrics Using Event Data Recorders' (2006) 50 *Annual Proceedings Association for the Advancement of Automotive Medicine* 57.

223 Mike Batty et al, 'Predictive Modeling for Life Insurance: Ways Life Insurers Can Participate in the Business Analytics Revolution' (Paper, Deloitte, April 2010) <www.soa.org/globalassets/assets/files/research/projects/research-pred-mod-life-batty.pdf>.

224 Gabler, Hampton and Hinch (n 31).

225 Nathan Newman, 'How Big Data Enables Economic Harm to Low-Income Consumers', *HuffPost* (online, 15 November 2014) <www.huffpost.com/entry/how-big-data-enables-econ_b_5820202>.

226 Joseph H Malley, 'Using State Motor Vehicle Records for Direct Marketing: An Industry's Dirty Little Secret Exposed (Part 1)' (Online Article, 20 September 2016) <www.linkedin.com/pulse/using-state-motor-vehicle-records-direct-marketing-an-malley>.

227 *Telstra* (n 16) 35–7 [57]–[65] (Kenny and Edelman JJ).

228 Ibid 36 [62]–[63].

post-*Telstra* that 'personal information' is too narrowly defined,[229] and personal information identifiable by cross-referencing data streams is unprotected.[230] Although there are provisions under the *Privacy Act* covering direct marketing,[231] the definition of 'personal information' under the Act sets the threshold too high to be an effective protection against abuse as it fails to recognise broadcast data that individually cannot reasonably identify a person.[232] However, when this information is combined with other information or data streams it makes identification of a person in minute detail possible.[233]

This section has shown that, like stored data, absent valid consent the *Privacy Act* protects data broadcast by an automated vehicle to a very limited degree.[234] The *Privacy Act* sets out vehicle owners' rights and how data may be handled and used,[235] although post-*Telstra* the threshold definition of 'personal information' is too narrow to offer any effective protection. For government and manufacturers the *Privacy Act* sets out their obligations in handling personal information,[236] but is again let down by the narrow interpretation by the Court. Third party corporate interests, absent consent, are prohibited from using the data, but with consent are virtually unrestricted in how to use the information.[237] The next consideration is whether data broadcast and received by an automated vehicle receives any protection under Australian telecommunications legislation.[238]

D *Broadcast Data and the Telecommunications Acts*

Broadcast data receives some protection under Australia's telecommunications legislation. The *Privacy Act* is enlivened under the *Telecommunications Act 1997* (Cth) ('*Telecommunications Act*') where data is defined as a 'communication',[239] and potentially falls under the purview of the *Telecommunications Act*.[240] It is likely that this would apply where the automated vehicle is communicating with the infrastructure. The *Telecommunications (Interception and Access) Act 1979*

229 *Review of Privacy* (n 6) 107–8 [3.23]–[3.30]; Goldenfein (n 7); James North, 'Metadata: It's Not about You After All' (2016) 68(2) *Governance Directions* 96.

230 Thakur and Mann (n 2) 471; Goldenfein (n 7). See generally *Serious Invasions of Privacy in the Digital Era* (n 6).

231 Australian Privacy Principles (n 67) cl 7.

232 *Privacy Act 1988* (n 11) s 6(1) (definition of 'personal information'). See especially *Telstra* (n 16).

233 See Vaile, Zalnieriute and Moses (n 7) 16–19.

234 See *Review of Privacy* (n 6) 107–8 [3.23]–[3.30]; *Serious Invasions of Privacy in the Digital Era* (n 6); *Telstra* (n 16).

235 Australian Privacy Principles (n 67).

236 Ibid.

237 Ibid cl 7.

238 *Telecommunications Act* (Cth) (n 55); *Interception Act* (Cth) (n 56); *Telecommunications (Interception) Amendment Act 2006* (Cth).

239 *Telecommunications Act* (Cth) (n 55) s 7 (definition of 'communications').

240 *Telecommunications Act* (Cth) (n 55).

(Cth) ('*Interception Act*') makes it an offence to intercept any telecommunication[241] without lawful excuse.[242] The *Interception Act* requires service providers to retain information[243] in particular circumstances[244] for two years.[245]

The *Interception Act* provides express application of the *Privacy Act* where data is retained by the service provider.[246] It further defines retained personal information to be

> information about an individual if the information relates to:
>
> (a) the individual; or
>
> (b) a communication to which the individual is a party.[247]

These protections only apply to data *retained* by the service providers, bringing them under the obligations set out in the *Privacy Act*.[248] Recent amendments to the *Telecommunications Act* only require carriage service providers to 'do their best' to prevent their services being used to commit crime.[249] This may yet prove to be wholly inadequate as the automated vehicle fleet increases in size and complexity. The recent Federal Chamber of Automotive Industries' submission to the House of Representatives recommends the division of automated vehicle data into three categories: traffic data, driver/owner data, and vehicle systems data.[250] This may make regulating broadcast data more efficient by separating pertinent information from the data stream. Additionally, the automated vehicle artificial intelligence cannot fall under the telecommunications legislation for the purposes of protecting personal information in a communication between individuals.[251] As automated vehicles develop it may be useful to recognise the automated vehicle artificial intelligence[252] as having a separate legal personality to inter alia protect automated vehicle communications.[253]

241 *Interception Act* (Cth) (n 56) s 7.

242 Ibid ss 7(2)–(8).

243 Ibid s 187A.

244 Ibid s 187AA.

245 Ibid s 187C(1).

246 Ibid s 187LA(1).

247 Ibid sub-s (2).

248 Ibid s 187LA.

249 *Telecommunications and Other Legislation Amendment Act 2017* (Cth) sch 1 cl 1.

250 Federal Chamber of Automotive Industries (n 90) 10.

251 *Interception Act* (n 56) s 187LA(2).

252 For a discussion on the 'operating system' as the 'driver' of an automated vehicle, see Brady et al (n 204).

253 This development would contrast historical notions of 'robotic' as denying agency: Lynden Griggs, 'A Radical Solution for Solving the Liability Conundrum of Autonomous Vehicles' (2017) 25(2) *Competition & Consumer Law Journal* 151, 154–61; Chris Holder et al, 'Robotics and Law: Key Legal and Regulatory Implications of the Robotics Age (Part I of II)' (2016) 32(3) *Computer Law & Security Review* 383; Ryan Calo, 'Robots as Legal Metaphors' (2016) 30(1) *Harvard Journal of Law & Technology* 209, 237.

This section showed that the ability of Australian information privacy legislation to protect personal information contained in data produced by automated vehicles is limited following the *Telstra* decision. Part III(A) evaluated the decision in *Telstra* showing how it negatively impacts information privacy in Australia. It argued that protection under the information privacy framework turns on whether the data can be construed as information about a person and that the interpretation of information about a person is now too narrow. Part III(B) highlighted gaps in the ability of the privacy framework to protect stored data. Part III(C) argued that existing privacy legislation provides insufficient protection where it intersects broadcast data and the four main categories of data-using entities in Australia. Part III(D) argued that Commonwealth telecommunications legislation provides only limited protection to broadcast data produced by automated vehicles. Accordingly, legislative reform is necessary to better protect the privacy of personal information produced by automated vehicles.

IV AUTOMATED VEHICLES AND LEGAL REFORM

The path toward safeguarding the future automated vehicle fleet requires understanding how the privacy of personal information, produced by automated vehicles, may be better protected. To accommodate the introduction of automated vehicles, Australia's information privacy framework requires reform. These reforms range from defining 'information privacy', setting a 'reasonable expectation of privacy'[254] test in the *Privacy Act*, or making the communications from automated vehicles 'restricted' under the *Telecommunications Act* to creating a national overarching legislation for the regulation and protection of automated vehicles. Legislative reform is ultimately necessary to promote the better protection of automated vehicle data in future. Part A responds to various Australian law reform recommendations regarding possible reform of the existing privacy framework and looks at the different approach to the regulation of privacy in Europe where individual privacy, although protected, is balanced against the greater social good. It argues that post-*Telstra*, the *Privacy Act* allows an interpretation inconsistent with the protection of information contained within large data streams. Part B suggests possible reforms that may be implemented in Australia to better protect the privacy of personal information produced by automated vehicles.

254 Also used in the *United States Constitution* amend XIV.

A *Privacy Frameworks*

1 *Australia*

There are differing opinions in Australia as to whether or to what degree privacy is in need of reform. Although the Australian National Transport Commission considers motor vehicles sufficiently regulated under existing legislation,[255] they have a roadmap for reform covering many aspects of automated vehicle technology over the coming years.[256] The ALRC claims further investigation into data privacy is necessary.[257] Significantly, the ALRC argues that convergent technology requires further review of both the *Privacy Act* and Australia's telecommunications legislation.[258] The New South Wales Joint Standing Committee on Road Safety recommend '[a]n examination of the security of the data systems which underpin [automated vehicle] technology, including the development of protocols to facilitate data sharing and address privacy issues'.[259]

The recent House of Representatives report recommends 'the Commonwealth Government further investigates the issue of data rights for consumers, vehicle manufacturers and third parties such as insurers and relevant government agencies'.[260] Additionally, the House of Representatives report suggests formation of a body to inter alia examine '[t]he ownership, use and security frameworks applicable to the data generated by automated vehicles'.[261] Notwithstanding the differing recommendations, most law reform organisations agree that there needs to be legislative reform of privacy in Australia.

When the National Transport Commission recommended 'at this time no changes are necessary to privacy laws governing automated vehicles and the transmission of personal information',[262] it did not consider the post-*Telstra* understanding of 'personal information'.[263] Use of the qualifying term 'reasonably' situates identifiable information on a trajectory moving outside the scope of the *Privacy Act* by narrowing the available criteria for identifiability.[264] Moreover, in relation to health data, the term 'reasonably necessary' has been held to be on a continuum

255 'Regulatory Reforms' (n 6) 73.

256 See generally 'Automated Vehicle Program', *National Transport Commission* (Web Document, October 2019) <www.ntc.gov.au/sites/default/files/assets/files/NTC%20Automated%20Vehicle%20Reform%20Program%20Approach%20%28October%202019%29%20-%20Public%20version.pdf >.

257 See generally *Serious Invasions of Privacy in the Digital Era* (n 6).

258 See generally ibid.

259 *Driverless Vehicles and Road Safety in NSW* (n 6) 2 recommendation 1(e).

260 *Social Issues Relating to Land-Based Automated Vehicles in Australia* (n 6) iii recommendation 4.

261 Ibid v recommendation 10.

262 'Regulatory Reforms' (n 6) 73.

263 *Privacy Act 1988* (n 11) s 6(1) (definition of 'personal information'); *Telstra* (n 16).

264 *Privacy Act 1988* (n 11) s 6(1) (definition of 'personal information').

itself, where '[w]hat may be seen as "reasonably necessary" falls towards the higher end of a continuum that might be seen as having "of some relevance" at one end and "essential" at the other end'.[265] Further, there is no reason to believe that data generated by automated vehicles will be any more 'private' than health data. This comes at a time when, with the introduction of automated vehicles, more data is set to be streamed than ever before.[266]

The situation in Australia is that data streams partially containing personal information, and therefore the streams associated with automated vehicles, will not fall under protection of the *Privacy Act*. Additionally, the lack of a legislative definition of privacy, or data privacy, or what the 'expectation' of data privacy may mean, leaves future data streams vulnerable to unregulated use and allows data to be mined with only minimal protection against interception.[267] To understand some possible privacy reform in Australia this paper briefly considers some privacy legislation in the European Union.

2 *Europe*

Unlike Australia, Europe favours a rights-based approach to privacy. In Europe, privacy regulation offers some protection against data mining, in circumstances where a person may be identified by the use of additional information.[268] In 2016, the European Parliament passed a regulation on the *General Data Protection Regulation* ('*Regulation*').[269] The *Regulation* defines 'personal data' as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person …[270]

This definition affords a broader interpretation than available under 'personal information' in the Australian *Privacy Act* and would yield a determination in contrast to that decided in *Telstra*. Notably, the *Regulation* also offers no protection

265 *ALZ v WorkCover NSW* [2015] NSWCATAP 138, [51], discussing *Health Records and Information Privacy Act* (n 55).

266 Patrick Nelson, 'Just One Autonomous Car Will Use 4,000 GB of Data/Day', *Network World* (Online Article, 7 December 2016) <www.networkworld.com/article/3147892/internet/one-autonomous-car-will-use-4000-gb-of-dataday.html>.

267 Prohibition against interception is to be found in the *Interception Act* (Cth) (n 56) s 7.

268 *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)* [2016] OJ L 119/1, 5 [26] ('*General Data Protection Regulation*').

269 Ibid.

270 Ibid art 4(1).

where such techniques are unable to identify a person,[271] as it specifically protects the 'natural person',[272] but not deceased persons,[273] or corporations.[274] However, in 2002, the European Parliament passed the *Directive on Privacy and Electronic Communications*[275] ('*Directive*') which sets out standards for the processing of personal data.[276] The *Directive* covered areas of standardisation,[277] data interception,[278] location data,[279] and traffic data (which includes everything in a data stream necessary for the conveyance of a communication) between two entities,[280] and defined 'communication' to be between any finite group of *legal persons*.[281]

The *Directive* also recommended that manufacturers of electronic communications equipment incorporate safeguards during their manufacturing process to protect personal data privacy in a technologically neutral way.[282] Significantly, while the *Directive* considers privacy of natural persons, it also includes the 'legitimate interests of … *legal persons*'[283] paving the way for the protection of artificial intelligence legal entities which may include automated vehicles in future. In Europe, the right to protection of personal data is not absolute,[284] 'it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality'.[285] Europe, therefore, while favouring a rights-based approach to privacy, understands privacy as a continuum which balances the benefits to society against individual privacy in relation to stored or broadcast data.[286]

B *Recommended Privacy Reforms*

It has been shown that there are gaps in the current Australian privacy framework which fail to protect personal information contained in data streams, and privacy

271 Ibid art 2.

272 Ibid art 1.

273 Ibid 5 [27].

274 Ibid 3 [14].

275 *Directive on Privacy and Electronic Communications* (n 6).

276 Ibid arts 1–15.

277 Ibid art 14.

278 Ibid art 5.

279 Ibid art 9.

280 Ibid arts 2(b), 6.

281 Ibid art 2(d).

282 Ibid 42 [46].

283 Ibid art 1(2) (emphasis added).

284 *General Data Protection Regulation* (n 268) 2 [4].

285 Ibid.

286 For further automated vehicle legislative and policy developments in other countries: see National Transport Commission, *In-Service Safety for Automated Vehicles* (Consultation Regulation Impact Statement, July 2019) app D <www.ntc.gov.au/Media/Reports/(D748D1D0-7D93-C79D-CE5F-77A1D50111D3).pdf>.

is regulated differently in Australia than in Europe. Additionally, there will be a marked increase in the quantity of data produced with the introduction of automated vehicles which will intensify the potential impact of future data privacy problems. To protect personal information produced by automated vehicles the current privacy framework is in need of reform. The following reforms are recommended:

1. Create a national legislation for the regulation and protection of automated vehicles which includes specific provisions on the privacy, use, and security of data. This will enable the standardised regulation of automated vehicles in Australia in relation to every facet of their use, testing and integration into society, including protecting the privacy of personal information generated by automated vehicles.

   Define 'information privacy' in Australian legislation, or, in the alternative, set a 'reasonable expectation of privacy' test,[287] as recommended by the ALRC.[288] Defining privacy will enable certainty in legal decisions as it removes doubt as to whether an action is 'private' for the purposes of the *Privacy Act* and will increase protection for interferences with information privacy.[289]

2. Amend the telecommunications Acts to include automated vehicles as a separate category of 'restricted' telecommunication requiring specific protection. This will enable the information streams emanating from automated vehicles to be identified as 'restricted' for the purposes of the telecommunications Acts and make the interference or mishandling of such data a strict liability offence. This will deter potential actors from accessing such data for their own gain which is, since the decision in *Telstra*,[290] unprotected.

The Australian information privacy framework can be strengthened by the adoption of these reforms, and should be amended, augmented, or replaced before the introduction of automated vehicles on Australian roads.

V CONCLUSION

As society's interdependence on increasingly advanced technology grows there will be ever larger quantities of data exchanged between automated vehicle technologies. This cumulative flood of information, has limited protection under Australia's privacy framework, which fails to cover data generated by automated

287 As also used in the *United States Constitution* amend XIV.

288 *Serious Invasions of Privacy in the Digital Era* (n 6) 92 recommendation 6.1.

289 *Privacy Act 1988* (n 11).

290 *Telstra* (n 16).

vehicles. The definition of 'personal information' in the *Privacy Act* is too narrow and requires amendment to cope with the future automated vehicle fleet.[291] Australia needs a legislative definition of privacy, or the reasonable expectation of privacy, and this must include data generated by automated vehicles. Australia will benefit from a national overarching automated vehicle regulation, or at the very least specific legislation protecting the privacy of data produced by automated vehicles.

This article considered the historical development of legal frameworks surrounding information privacy and personal information in Australia. It has considered foreign jurisdictions and recommended reforms. When automated land vehicles arrive on our roads, Australia must be prepared to protect automated vehicle data on every level. A failure to understand the significance of automated vehicles in relation to data privacy may in future yield a problem the likes of which cannot yet now be imagined. Protecting data privacy may require regulating transmission and reception of data, amending the definitions of 'personal information', and 'communication' or redefining 'privacy' in the legislative frameworks, to creating a separate legal personality for automated vehicles. Ultimately, data privacy exists on a continuum, with individual autonomy at one end balanced against benefits to society at the other. Understanding where automated vehicles fit into that continuum will be crucial to navigating an appropriate legislative solution to data privacy.

291 *Privacy Act 1988* (n 11) s 6(1) (definition of 'personal information').