DRIVING INTO NEW FRONTIERS? DATA AND DRIVERLESS CARS

BELINDA BENNETT,* JANE EVELYN** AND BRIDGET WEIR***

I INTRODUCTION

The prospect of driverless cars on Australian roads at some stage in the foreseeable future has led to a flurry of scholarly debate,[1] discussion of the safety and testing of vehicles,[2] and proposals for legislative reform.[3] Most of the debate both in Australia and overseas has centred around technical changes to road rules, driver licensing, and insurance to accommodate a vehicle that is 'driven' without a human driver,[4] requirements for safety and testing of vehicles,[5] and the ethics of the 'choices' that might be made by a driverless car in the event of an unavoidable

* Professor of Health Law and New Technologies, Faculty of Law, Queensland University of Technology ('QUT'). Work for this article was supported by the Institute for Future Environments at QUT. I wish to thank Elizabeth Dallaston for her research assistance and Mark Burdon, Des Butler and the anonymous reviewers for their helpful comments.

** Sessional Academic, School of Law, Faculty of Law, Queensland University of Technology.

*** Doctoral Candidate and Sessional Academic, School of Justice, Faculty of Law, Queensland University of Technology.

1 See, eg, Kieran Tranter, 'The Challenges of Autonomous Motor Vehicles for Queensland Road and Criminal Laws' (2016) 16(2) *Queensland University of Technology Law Review* 59; Lisa Collingwood, 'Privacy Implications and Liability Issues of Autonomous Vehicles' (2017) 26(1) *Information & Communications Technology Law* 32; Melinda Florina Lohmann, 'Liability Issues Concerning Self-Driving Vehicles' (2016) 7(2) *European Journal of Risk Regulation* 335; Mark Brady et al, 'Automated Vehicles and Australian Personal Injury Compensation Schemes' (2017) 24(1) *Torts Law Journal* 32; Michael Mattioli, 'Autonomy in the Age of Autonomous Vehicles' (2018) 24(2) *Boston University Journal of Science and Technology Law* 277.

2 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*'); David B Logan et al, 'Safety Benefits of Cooperative ITS and Automated Driving in Australia and New Zealand' (Research Report No AP-R551-17, Austroads, October 2017).

3 National Transport Commission Australia, 'Regulatory Options for Automated Vehicles' (Discussion Paper, May 2016) ('2016 Regulatory Options Discussion Paper').

4 Tranter (n 1); Mitchell L Cunningham, Michael A Regan and John Catchpole, 'Registration, Licensing and CTP Insurance Issues Associated with Automated Vehicles' (Research Report No AP-R540-17, Austroads, March 2017); National Transport Commission Australia, 'Clarifying Control of Automated Vehicles' (Policy Paper, November 2017); National Transport Commission Australia, 'Changing Driving Laws to Support Automated Vehicles' (Policy Paper, May 2018).

5 *Driverless Vehicles and Road Safety in NSW* (n 2); Logan et al (n 2). See also National Transport Commission Australia, 'Regulatory Options to Assure Automated Vehicle Safety in Australia' (Discussion Paper, June 2017).

crash.[6] More recently, there has been a growing debate over the role of data in automated vehicles and cooperative intelligent transport systems ('C-ITS'), and the potential privacy-related concerns that may arise in the context of driverless vehicles.[7]

This article analyses the legal and ethical issues that are raised by the use of data that will potentially be generated by driverless cars, comparing Australian approaches with those in overseas jurisdictions. Although current vehicle technology can also generate some data,[8] the focus of this article is on the data and privacy challenges posed by C-ITS and driverless cars. It will argue that the policy landscape for data and driverless cars is characterised by a series of intersections: between transport infrastructure and automated vehicles; between federal and state/territory privacy laws; and between access to data and privacy. The complexity of these intersections presents significant challenges for the development of Australian policy and regulation for driverless cars.

Part II provides an overview of the different types of data that will be used in the context of driverless vehicles, including the data that will be generated at an infrastructure level by connected transport systems, as well as the data that will be generated by individual driverless vehicles, which may or may not be part of a connected transport system. Part III analyses the issues that may arise in relation to transport infrastructure data within C-ITS. Part IV evaluates the question of access to data generated by driverless cars, including the question of accessibility to data by different parties, such as vehicle owners, law enforcement, manufacturers and others. Part V considers the possibility of adopting a 'privacy by design' approach to driverless cars before the conclusion in Part VI.

II DRILLING FOR THE 'NEW OIL'

With the emergence of 'smart cities' which rely on internet connectivity and data collection and analysis to tailor service delivery,[9] the connectivity of the

6 Noah J Goodall, 'From Trolleys to Risk: Models for Ethical Autonomous Driving' (2017) 107(4) *American Journal of Public Health* 496; Jan Gogoll and Julian F Müller, 'Autonomous Cars: In Favor of a Mandatory Ethics Setting' (2017) 23(3) *Science and Engineering Ethics* 681.

7 See, eg, National Transport Commission Australia, 'Regulating Government Access to C-ITS and Automated Vehicle Data' (Discussion Paper, September 2018) ('2018 Access to Data Discussion Paper'); National Transport Commission Australia, 'Regulating Government Access to C-ITS and Automated Vehicle Data' (Policy Paper, August 2019) ('2019 Access to Data Policy Paper'); 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); Angela Daly, 'Privacy in Automation: An Appraisal of the Emerging Australian Approach' (2017) 33(6) *Computer Law & Security Review* 836; Collingwood (n 1); Dorothy J Glancy, 'Privacy in Autonomous Vehicles' (2012) 52(4) *Santa Clara Law Review* 1171; Chassel Lee, 'Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars' (2017) 69(1) *Federal Communications Law Journal* 25.

8 '2018 Access to Data Discussion Paper' (n 7) 22–3; '2019 Access to Data Policy Paper' (n 7) 25–7.

9 Jesse W Woo, 'Smart Cities Pose Privacy Risks and Other Problems, but That Doesn't Mean We Shouldn't Build Them' (2017) 85(4) *University of Missouri-Kansas City Law Review* 953, 955; Sofia Ranchordás and Abram Klop, *Data-Driven Regulation and Governance in Smart Cities* (University of

transport system becomes one element in an integrated approach to urban planning. Smart cities, and the Internet of Things ('IoT'), of which connected vehicles may be one example, are built on connectivity and data.[10] In a 'big data' era, data increasingly has a commercial value. Indeed, such is this value that data has been described as 'the new oil'.[11] Yet access to data is becoming a contested space. Increasing connectivity and data collection has been accompanied by concerns about privacy and surveillance.[12] Privacy rights and consumer control of data are emerging as potential brakes on the ubiquity of data access.

In the context of transport, there is an emerging debate in Australia and elsewhere about the role of data in C-ITS and automated vehicles (driverless cars). Data is a central issue to these future transportation options.[13] With so much data likely to be generated by driverless cars, the privacy implications of that data, and the conditions upon which data may be shared and with whom, are emerging as important considerations for transportation law and policy.[14]

Glancy argues that there are three privacy interests related to autonomous vehicles: personal autonomy privacy interests, personal information privacy interests and surveillance privacy interests.[15] Personal autonomy interests relate to an individual's decision about whether to use an autonomous vehicle, and choice and control in relation to the operation of the vehicle, including where to go and how to get there.[16] The autonomy of the human operator may be delegated to some degree to the vehicle, with the human user retaining control over the goals of the transportation.[17] While the autonomy interests can be addressed through affirmative choice and informed consent, the complex technical nature of autonomous vehicles can present difficulties in terms of making information accessible to consumers so as to enable informed decision-making.[18] Autonomy interests may also be addressed by anonymity of data, although it may be difficult to achieve this within connected transport systems.[19] The data generated by autonomous vehicles will also generate personal information privacy interests around the collection and use of the data.[20] Finally, autonomous vehicles will raise

---

Groningen Faculty of Law Research Paper Series No 7/2018, February 2018) <https://ssrn.com/abstract=3126221>.

10 Woo (n 9); Ranchordás and Klop (n 9).

11 See, eg, 'The World's Most Valuable Resource Is No Longer Oil, but Data', *The Economist* (online, 6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>; Susie Gharib, 'Intel CEO Says Data is the New Oil', *Fortune* (online, 7 June 2018) <http://fortune.com/2018/06/07/intel-ceo-brian-krzanich-data/>; 'Data Is the New Oil', *The Australian* (online, 5 May 2017) <https://www.theaustralian.com.au/news/inquirer/the-new-oil-data-is-the-worlds-most-valuable-resource/news-story/f386217a9c63ac5ee6e1473413e9bda>; Perry Rotella, 'Is Data the New Oil?', *Forbes* (online, 2 April 2012) <https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#20d39e57db3d>.

12 Woo (n 9); Ranchordás and Klop (n 9).

13 Collingwood (n 1) 35.

14 Ibid; Daly (n 7).

15 Glancy (n 7) 1187–216, discussed in Collingwood (n 1) 35–6.

16 Glancy (n 7) 1188–95.

17 Ibid 1190–1.

18 Ibid 1195.

19 Ibid.

20 Ibid 1195–206.

surveillance privacy interests.[21] These interests 'respond to people's aversion to being constantly watched, tracked or monitored as they travel from place to place'.[22]

Part of the complexity of the debates about data and driverless cars is that they connect with our expectations of privacy in our vehicles.[23] Furthermore, debate about the regulatory implications of data, data sharing and privacy for driverless cars cannot be divorced from the broader debates within society about data and privacy and consequently are occurring within a rapidly changing social, ethical and regulatory environment around data and privacy more generally.

There are two broad areas in which data will potentially be generated by driverless cars and connected transport systems. The first relates to C-ITS which is essentially the road and traffic infrastructure and the 'smart' technologies that will allow vehicles to communicate with this infrastructure, known as Vehicle-to-Infrastructure ('V2I') communication.[24] It is in this sense that automated vehicles would also be connected vehicles, thus allowing for communication about matters such as traffic congestion.[25] However, within C-ITS, vehicles may also communicate with other vehicles ('V2V') and with other road users such as pedestrians and cyclists ('V2X').[26]

C-ITS have the potential to deliver improvements in road safety through collision avoidance and hazard detection, for example, by providing warning of potential hazards such as stationary vehicles ahead or approaching emergency vehicles, or warning of road works or reduced speed limits.[27] In addition, C-ITS may improve safety for vulnerable road users such as pedestrians, motorcyclists or cyclists by providing enhanced detection by motorists of these road users.[28] Drivers may also be provided with improved signage in their vehicles, providing them with information on speed zones, stop signs, changed road surfaces, or hazardous weather conditions.[29] Emergency response times to crashes could also be reduced by automatic emergency post-crash notification systems.[30]

The other area in which data may be generated is by the vehicle itself. While driverless cars are usually also connected vehicles, referred to as 'connected and autonomous vehicles' ('CAVs'), this is not necessarily the case. Driverless cars may simply allow for automated driving without relying on a connected transport

21 Ibid 1206.
22 Ibid.
23 Ibid 1216–25; Collingwood (n 1) 38–9.
24 As the NTC notes, 'C-ITS data is produced when components of the transport network (vehicles, roads and infrastructure) communicate and share real-time information (for example, information on vehicle movement, traffic signs and road conditions) through C-ITS devices': '2018 Access to Data Discussion Paper' (n 7) 1.
25 Logan et al (n 2) 2.
26 Ibid.
27 Ibid 4.
28 Ibid 7–8.
29 Ibid 8–9.
30 Ibid 9.

system.[31] Levels of driving automation for vehicles are generally categorised according to the Society of Automotive Engineers standard SAE J3016 which has six levels of automation.[32] At levels zero, one and two all or part of the driving tasks are performed by the driver. For example, at level zero the driver performs all of the dynamic driving task, while at level two there is partial driving automation. Parking assist functions where the vehicle parks while the driver remains in the car is an example of partial automation.[33] Most discussion about driverless cars refers to higher levels of automation. At level three (conditional driving automation), a driver may be required to intervene and take over the driving when requested to do so by the driving system. Heavy vehicle platooning is an example of conditional automation.[34] Level four (high driving automation) assumes that the driving task can be undertaken by the driving system even if the driver does not take over control when requested. An example of high automation would be an automated vehicle that drives on a pre-determined route, such as a shuttle service,[35] while level five (full driving automation) does not require any intervention by the human 'driver'.[36]

Some of the data generated by C-ITS or driverless cars will be of a similar kind to that already generated by vehicles. For example, current advanced driver assistance systems already use sensor units to detect obstacles, and electronic control units to provide information on journey distance and to warn of vehicle faults.[37] However developments in C-ITS and automated vehicle technology may generate new types of data. In-vehicle video recording, for example, may be used for driver recognition for security, or to set driver preferences.[38] These technologies may be extended to the whole of the interior of the vehicle cabin at higher levels of automation where there may be no 'driver seat'.[39] Other data that may be generated includes event data recorders to record data about crashes, including whether the driving system or the human driver were in control of the vehicle at the time of the crash, as well as V2V and V2I data.[40]

In its recent discussion paper on data and C-ITS and automated vehicles, the National Transport Commission ('NTC') stated:

---

31 '2018 Access to Data Discussion Paper' (n 7) 61–2; '2019 Access to Data Policy Paper' (n 7) 48. See also Glancy (n 7) 1176 (drawing a distinction between 'selfcontained autonomous vehicles' and 'interconnected autonomous vehicles').

32 '2016 Regulatory Options Discussion Paper' (n 3) 31.

33 Ibid 32.

34 Ibid 32: with platooning, 'except for the lead truck in the platoon, the system takes control of driving and monitoring the road environment on specific roads, and the driver monitors the automated driving system'.

35 Ibid 33.

36 Ibid.

37 '2018 Access to Data Discussion Paper' (n 7) 22; '2019 Access to Data Policy Paper' (n 7) 25.

38 '2018 Access to Data Discussion Paper' (n 7) 25; '2019 Access to Data Policy Paper' (n 7) 25.

39 '2018 Access to Data Discussion Paper' (n 7) 25–6; '2019 Access to Data Policy Paper' (n 7) 26.

40 '2018 Access to Data Discussion Paper' (n 7) 26–8; '2019 Access to Data Policy Paper' (n 7) 26.

> While only some types of C-ITS and automated vehicle technology (and the information generated by it) may raise new privacy challenges, the breadth and depth of information that will likely be generated may itself present a challenge.[41]

According to the NTC, these privacy challenges are likely to arise for several reasons: firstly, because automated vehicles will provide all or most of the driving task, they will require more inputs to operate than existing driving systems;[42] secondly, 'C-ITS and automated vehicle technology will collect (and broadcast) a greater amount of information relating to the safety of vehicle occupants and the road environment';[43] thirdly, navigation systems and event data recorders will become more widespread and their data may be stored for longer periods than is currently the case;[44] fourthly, 'external camera input units in automated vehicles will most likely move from real time feed to recording and storing';[45] and finally, there are greater opportunities for data linkage by governments.[46]

With the value of data gaining increasing recognition, the policy approaches to data management and data sharing are an important element in the policy and regulatory environment for the introduction of C-ITS and driverless cars, as is the application of privacy laws. Part III below will analyse the Australian approach to the use of data in relation to C-ITS, while Part IV will focus on the approaches to data generated by the vehicle itself.

III C-ITS DATA

Governments have an interest in being able to access C-ITS data for law enforcement purposes including crash investigations, for detection of traffic offences such as speeding, to manage traffic, to manage road safety from natural disasters or other hazards, and to assist with strategic planning for infrastructure.[47] However the connectivity of future transport systems potentially raises complex issues in terms of individual privacy. In its recent discussion paper on 'Regulating Government Access to C-ITS and Automated Vehicle Data'[48] the NTC concluded that location information generated by C-ITS would most likely constitute 'personal information' within the terms of the *Privacy Act 1988* (Cth) ('*Privacy Act*').[49] 'Personal information' is defined in section 6 as:

---

41 '2018 Access to Data Discussion Paper' (n 7) 30. See also '2019 Access to Data Policy Paper' (n 7) 36–8.

42 '2018 Access to Data Discussion Paper' (n 7) 30; '2019 Access to Data Policy Paper' (n 7) 39.

43 '2018 Access to Data Discussion Paper' (n 7) 30. See also '2019 Access to Data Policy Paper' (n 7) 39.

44 '2018 Access to Data Discussion Paper' (n 7) 30; '2019 Access to Data Policy Paper' (n 7) 39.

45 '2018 Access to Data Discussion Paper' (n 7) 31. See also '2019 Access to Data Policy Paper' (n 7) 39.

46 '2018 Access to Data Discussion Paper' (n 7) 31; '2019 Access to Data Policy Paper' (n 7) 39.

47 '2018 Access to Data Discussion Paper' (n 7) 39–40, app C; '2019 Access to Data Policy Paper' (n 7) 31–3.

48 '2018 Access to Data Discussion Paper' (n 7).

49 Ibid 33–5. See also '2019 Access to Data Policy Paper' (n 7) 42. For discussion of privacy laws see Vaile, Zalnieriute and Bennett Moses (n 7) 11–23.

> 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.

Furthermore, location information from C-ITS may reveal 'sensitive information' within the definitions of the *Privacy Act*.[50] The definition of 'sensitive information' includes information such as a person's race or ethnic origin, or religious beliefs, and that is also 'personal information' (ie, from which a person is 'reasonably identifiable'), as well as health information about an individual, 'genetic information about an individual that is not otherwise health information', 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification', or biometric templates.[51] The NTC concluded that location information within C-ITS may reveal sensitive information about an individual from the venues they visit.[52]

The intersections between C-ITS and privacy laws are made more challenging by the need to also consider the potential application of state and territory privacy laws.[53] The lack of harmonisation in Australian privacy laws adds to the complexities of the regulatory environment for data-related issues in the context of driverless cars. As Vaile, Zalnieriute and Bennett Moses have noted:

> Much of the collection or use of C-ITS & AV data will be done by state and territory instrumentalities. The privacy legislation, where it exists, is broadly similar but some jurisdictions do not have privacy statutes. … State and territory differences create potential inconsistency, complexity and uncertainty for citizens, regulators and industry.[54]

The challenge of determining whether particular forms of data, such as those generated by C-ITS, fall within the definitions of the *Privacy Act* or state and territory privacy legislation is significant. Of course, this is not simply a challenge for future transportation systems, but is one arising from the contemporary data environment more generally. As the Productivity Commission noted in its 2017 report on data:

---

50 '2018 Access to Data Discussion Paper' (n 7) 34–6; '2019 Access to Data Policy Paper' (n 7) 42; Vaile, Zalnieriute and Bennett Moses (n 7) 23–6. For discussion of the definitions of 'personal' and 'sensitive' information in Commonwealth, state and territory privacy legislation see Vaile, Zalnieriute and Bennett Moses (n 7) app B.

51 *Privacy Act 1988* (Cth) s 6. For discussion see '2018 Access to Data Discussion Paper' (n 7) 34; '2019 Access to Data Policy Paper' (n 7) 39; Vaile, Zalnieriute and Bennett Moses (n 7) 23–6.

52 '2018 Access to Data Discussion Paper' (n 7) 36; '2019 Access to Data Policy Paper' (n 7) 42. See also Vaile, Zalnieriute and Bennett Moses (n 7) 26.

53 Vaile, Zalnieriute and Bennett Moses (n 7) app B citing *Information Privacy Act 2014* (ACT); *Privacy and Personal Information Protection Act 1998* (NSW); *Information Act 2002* (NT); *Information Privacy Act 2009* (Qld); Department of the Premier and Cabinet, 'Cabinet Administrative Instruction 1/89, Also Known as the Information Privacy Principles (IPPS) Instruction, and Premier and Cabinet Circular 12, as Amended by Cabinet 6 February 2017' (Circular No 12, Government of South Australia, 6 February 2017); *Personal Information Protection Act 2004* (Tas); *Privacy and Data Protection Act 2014* (Vic); *Freedom of Information Act 1992* (WA).

54 Vaile, Zalnieriute and Bennett Moses (n 7) 68.

> The boundaries of personal information are constantly shifting in response to technological advances and new digital products, along with community expectations.
>
> The legal definition of personal information, contained in the *Privacy Act 1988* (Cth), has always had an element of uncertainty, and is managed by guidelines. In the face of rapid changes in sources and types of data, outcome-focused data definitions remain essential. But practical guidance (that data custodians and users can rely on) is required on what sorts of data are covered by the definitions.[55]

Internationally, the approach to the privacy issues related to automated vehicles has been mixed. While different approaches to privacy regulation are evident internationally,[56] recognition of the need to address privacy concerns associated with connected and automated vehicles is a common feature. In Canada the recommendations of a recent Senate Report included:

> Recommendation 9: The Government of Canada continue to assess the need for privacy regulations specific to the connected car.
>
> Recommendation 10: Transport Canada bring together relevant stakeholders – governments, automakers, and consumers – to develop a connected car framework, with privacy protection as one of its key drivers.[57]

In the United Kingdom, the approach taken by the House of Lords Select Committee Report on connected and autonomous vehicles reflects a need to balance privacy with use of data, noting:

> It is essential that any data gathered from CAV are used in accordance with data protection law. … However, the meaning of personal data is unclear in the context of CAV. It will be important to achieve privacy for individuals and communities, while using data to achieve efficiency and safety of CAV operations. Data relating to an individual's CAV in terms of position, speed and performance on the road cannot be regarded as entirely personal – such data is needed for public benefit if a CAV system is to operate as a whole. Good data governance will therefore be needed to secure appropriate protection of personal information while safely using and linking open and non-sensitive data. Distinctions will need to be made between commercially sensitive data owned by technology providers and open data.[58]

A 2017 German report on ethics and autonomous vehicles expressly recognised the 'autonomy and data sovereignty of road users':

> Permitted business models that avail themselves of the data that are generated by automated and connected driving and that are significant or insignificant to vehicle

---

55 Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, 31 March 2017) 137, finding 3.4.

56 For example, for discussion of the differences between approaches to privacy law in Europe and the United States see Vaile, Zalnieriute and Bennett Moses (n 7) 52–66; '2018 Access to Data Discussion Paper' (n 7) 16–18; '2019 Access to Data Policy Paper' (n 7) 67–9.

57 Standing Senate Committee on Transport and Communications, Senate of Canda, *Driving Change: Technology and the Future of the Automated Vehicle* (Final Report, January 2018) 58.

58 Science and Technology Select Committee, House of Lords, *Connected and Autonomous Vehicles: The Future?* (House of Lords Paper No 115, Session 2016–17) 43 [169–70].

> control come up against their limitations in the autonomy and data sovereignty of road users. It is the vehicle keepers and vehicle users who decide whether their vehicle data that are generated are to be forwarded and used.[59]

In relation to the connectivity of transport infrastructure, the German report cautioned that '[a]utomated and connected driving could result in the total surveillance of all road users … Autonomous driving would be at the expense of autonomous everyday action'.[60] Drawing on the 'principles of data minimization and data avoidance, which are enshrined in European and German law',[61] the report states that '[i]n keeping with the data law principle of privacy by default, vehicles should, upon delivery, already have privacy-friendly factory settings' to ensure that data that is not 'safety-critical' is not collected unless the collection features are activated by the driver.[62]

The approach in the German report is consistent with the 'privacy by default' approach in current European law. The *General Data Protection Regulation* ('*GDPR*') requires a 'privacy by design' and 'privacy by default' approach for technologies that collect data.[63] Earlier work by the European Commission Article 29 Data Protection Working Party ('Working Party') concluded that data generated by C-ITS could be personal data.[64] The Working Party recognised the benefits that could be delivered by C-ITS but sounded a cautionary note on the privacy risks stating:

> that the large scale deployment of this new technology, which will entail the collection and processing of unprecedented amounts of location data of individuals in Europe, poses new challenges to the fundamental rights and to the protection of personal data and privacy both of users and of other individuals that will possibly be affected.[65]

In 2017 a working group of the European Commission's C-ITS Platform concluded that 'the balance between privacy, data protection and road safety should be thoroughly further assessed'.[66]

---

59 Federal Ministry of Transport and Digital Infrastructure, *Ethics Commission: Automated and Connected Driving* (Report, June 2017) 12 ('*Ethics Commission: Automated and Connected Driving*'). For discussion of the German report see Christoph Luetge, 'The German Ethics Code for Automated and Connected Driving' (2017) 30(4) *Philosophy and Technology* 547.

60 *Ethics Commission: Automated and Connected Driving* (n 59) 24.

61 Ibid.

62 Ibid 25.

63 '2018 Access to Data Discussion Paper' (n 7) 16–17; '2019 Access to Data Policy Paper' (n 7) 68; Vaile, Zalnieriute and Bennett Moses (n 7) 56.

64 European Commission Article 29 Data Protection Working Party, 'Opinion 03/2017 on Processing Personal Data in the Context of Cooperative Intelligent Transport Systems (C-ITS)' (Working Paper No 252, October 2017). For discussion see Vaile, Zalnieriute and Bennett Moses (n 7) 54–5, 115. With the introduction of the *GDPR* in Europe in May 2018, the Article 29 Working Party has now been replaced by the European Data Protection Board: 'Article 29 Working Party', *European Data Protection Board* (Web Page) <http://www.edpb.europa.eu/our-work-tools/article-29-working-party_en>.

65 European Commission Article 29 Data Protection Working Party (n 64) 8.

66 C-ITS Platform Phase II, *Cooperative Intelligent Transport Systems Towards Cooperative, Connected and Automated Mobility* (Final Report Phase II, European Commission, September 2017) 31. For discussion see Vaile, Zalnieriute and Bennett Moses (n 7) 54–5.

As is clear from the above, there is recognition of the need to consider the privacy implications of C-ITS. Internationally, jurisdictions are grappling with the significance of privacy laws for C-ITS data. As Part IV argues, additional privacy-related concerns are also raised by automated vehicles themselves.

IV KNOWING MY CAR, KNOWING ME?

There are two aspects to the data-related issues for driverless cars: first, whether the data comes within the scope of privacy laws, and second, who can access the data from driverless cars. For the most part, C-ITS and driverless cars are discussed together. There is good reason for this as many of the proposed benefits of driverless vehicle technology, such as easing traffic congestion, will only be realised when automated vehicles are also connected vehicles within a C-ITS. Yet driverless cars are not necessarily part of C-ITS.[67] Furthermore, there are differences between C-ITS and automated vehicles in terms of access to data, with governments able to collect data from C-ITS directly, while government collection of data from automated vehicles will need to rely on third parties such as the automated driving system entity ('ADSE') for access to data.[68] Driverless cars are also more likely than C-ITS to generate sensitive data, for example from in-cabin video recordings and health sensors.[69]

The data that automated vehicles may generate might be 'personal information' within the *Privacy Act*.[70] As noted by the NTC, '[d]ata from in-cabin cameras is highly likely to be personal information in all circumstances because it can identify the driver and vehicle occupants'.[71] Data from biological, biometric or health sensors may be used to monitor driver alertness and behaviour or to identify drivers in order to customise the driving experience.[72] Such data may be 'personal information' depending on the ability of the entity holding the data to analyse it and link it to other data for identification purposes.[73] The NTC noted that

> government entities such as road operators and law enforcement are likely to have a wider range of data and capacity to analyse the data than other entities may have.

67 '2018 Access to Data Discussion Paper' (n 7) 61–2; '2019 Access to Data Policy Paper' (n 7) 48. See also '2019 Access to Data Policy Paper' (n 7) 49: '[a]t this early stage of regulatory framework development, the NTC considers it is possible to have a broadly similar approach for both technologies'.

68 '2018 Access to Data Discussion Paper' (n 7) 62; '2019 Access to Data Policy Paper' (n 7) 48. The automated driving system entity ('ADSE') is the 'legal entity responsible for the ADS' (automated driving system): National Transport Commission Australia, 'Safety Assurance for Automated Driving Systems: Decision Regulation Impact Statement' (Regulation Impact Statement, November 2018) 16 ('2018 Safety Assurance for Automated Driving Systems').

69 '2018 Access to Data Discussion Paper' (n 7) 62; '2019 Access to Data Policy Paper' (n 7) 48.

70 '2018 Access to Data Discussion Paper' (n 7) 34–5; '2019 Access to Data Policy Paper' (n 7) 41–2. See also Vaile, Zalnieriute and Bennett Moses (n 7) 6–23.

71 '2018 Access to Data Discussion Paper' (n 7) 34; '2019 Access to Data Policy Paper' (n 7) 41.

72 '2018 Access to Data Discussion Paper' (n 7) 23; '2019 Access to Data Policy Paper' (n 7) 26.

73 '2018 Access to Data Discussion Paper' (n 7) 35; '2019 Access to Data Policy Paper' (n 7) 41–2.

> In their hands, data from biometric, biological or health sensors is therefore more likely to be personal information.[74]

While some of the data generated by driverless cars, such as event data recorders or sensor input units, may have limited value on their own, the ability to combine this data with other vehicle and C-ITS data such as from in-vehicle or external cameras and microphones may reveal personal information.[75] Data from in-vehicle cameras and sensors may also reveal sensitive information as it may be possible to deduce a person's race, ethnic origin, religious affiliation, or sexual orientation,[76] all of which are within the *Privacy Act's* definition of 'sensitive information'. Furthermore, data from sensors may reveal health information, which also falls within the definition of 'sensitive information'.[77] As noted by the NTC, the ability to combine data from C-ITS and automated vehicle technology could reveal sensitive information:

> A person who parks their car near a place of worship may do so because they intend to visit. This could reveal information about their religious affiliation. However, the person could just be visiting another venue in the same vicinity. If this information is combined with a video from in-cabin cameras that shows the person wearing religious clothing, then a person's religious affiliation may be clearer.[78]

Access to such data from driverless cars may enable profiles of vehicle operators to be developed.[79] Lee has argued that although data from driverless cars 'may enable a range of attractive consumer features, it is only steps away from surreptitious surveillance and untoward influence of consumer behavior, especially by companies looking to profit from such valuable information'.[80]

A further issue is that of who can access the data from driverless cars. Parties likely to be interested in accessing the data include the public sector (eg, law enforcement and transport departments to assist with infrastructure management and planning),[81] and the private sector (eg, insurers, vehicle manufacturers, and fleet managers), as well as those injured[82] or for those who have suffered property damage in the event of a crash. At levels below full automation, vehicles may sometimes be controlled by the human driver and at other times by the automated driving system. It will be important for police to be able to identify whether the human driver or the automated driving system were in control of the vehicle at the

---

74 '2018 Access to Data Discussion Paper' (n 7) 35. See also '2019 Access to Data Policy Paper' (n 7) 41.

75 '2018 Access to Data Discussion Paper' (n 7) 35–6; '2019 Access to Data Policy Paper' (n 7) 42.

76 '2018 Access to Data Discussion Paper' (n 7) 36. See also '2019 Access to Data Policy Paper' (n 7) 41; Vaile, Zalnieriute and Bennett Moses (n 7) 23–6.

77 '2018 Access to Data Discussion Paper' (n 7) 36; '2019 Access to Data Policy Paper' (n 7) 42; Vaile, Zalnieriute and Bennett Moses (n 7) 8, 23–6.

78 '2018 Access to Data Discussion Paper' (n 7) 36; '2019 Access to Data Policy Paper' (n 7) 42. See also Vaile, Zalnieriute and Bennett Moses (n 7) 26.

79 Lee (n 7) 33.

80 Ibid 34.

81 '2018 Access to Data Discussion Paper' (n 7) 39–40; '2019 Access to Data Policy Paper' (n 7) 31–3.

82 National Transport Commission Australia, 'Motor Accident Injury Insurance and Automated Vehicles' (Discussion Paper, October 2018) 66 ('2018 Motor Accident Injury Insurance and Automated Vehicles'); National Transport Commission Australia, 'Motor Accident Injury Insurance and Automated Vehicles' (Policy Paper, August 2019) 40–1 ('2019 Motor Accident Injury Insurance and Automated Vehicles').

time of a crash or a traffic offence such as speeding.[83] The NTC concluded that '[t]o ensure the effective administration of road safety laws, enforcement agencies, regulators and the courts should, in the future, be able to identify who is responsible for a vehicle at a point in time'.[84]

The NTC concluded that 'Australia's information access framework does not sufficiently address the new privacy challenges of government collection and use of C-ITS and automated vehicle technology'.[85] Furthermore, the use of C-ITS and automated vehicle data for law enforcement purposes 'may result in increased surveillance opportunities'.[86] As the NTC noted:

> Law enforcement is exempt from complying with many collection, use and disclosure privacy principles where such noncompliance is reasonably necessary for the performance of law enforcement functions. While the NTC recognises that these exceptions apply on a case-by-case basis, the argument that noncompliance is reasonably necessary could be made in many law enforcement contexts.[87]

In the private sector, the degree to which manufacturers who operate the ADSE are required to share data about crashes or other events is also important. Such data may play an important role in the continuous improvement of automated driving systems, as well as for government safety assurance of automated vehicles.[88]

The NTC has noted that 'vehicle data relevant to determining liability in an ADS [automated driving system] crash is most likely to be considered personal information for the purposes of Australia's privacy laws'.[89] The NTC concluded that in determining who should have access to data it was necessary to balance the privacy interests of owners, occupants and drivers, with the proprietary interests of the ADSE or manufacturer in the data, as well as the costs associated with storing the data and making it available in the future.[90] The NTC noted, '[i]n the context of automated vehicle data for personal injury insurance, a balance needs to be struck so that only the minimum vehicle data necessary to determine liability is required to be made, recorded and stored'.[91] In its 2019 policy paper on motor accident insurance the NTC indicated that it 'will coordinate a national approach to a data access framework for insurers to determine liability as part of the NTC's automated vehicle reform program'.[92]

---

83 The NTC has issued guidance on enforcement in relation to automated vehicles: National Transport Commission Australia, 'National Enforcement Guidelines for Automated Vehicles' (Guidelines, November 2017).

84 National Transport Commission Australia, 'Regulatory Reforms for Automated Road Vehicles' (Policy Paper, November 2016) 66 ('2016 Regulatory Reforms Policy Paper').

85 '2018 Access to Data Discussion Paper' (n 7) 60. See also '2019 Access to Data Policy Paper' (n 7) 43.

86 '2018 Access to Data Discussion Paper' (n 7) 61. See also '2019 Access to Data Policy Paper' (n 7) 44.

87 '2018 Access to Data Discussion Paper' (n 7) 61.

88 '2018 Safety Assurance for Automated Driving Systems' (n 68) 147–8. See also '2019 Access to Data Policy Paper' (n 7) 32.

89 '2018 Motor Accident Injury Insurance and Automated Vehicles' (n 82) 66. See also '2019 Motor Accident Injury Insurance and Automated Vehicles' (n 82) 42.

90 '2018 Motor Accident Injury Insurance and Automated Vehicles' (n 82) 67.

91 Ibid.

92 '2019 Motor Accident Injury Insurance and Automated Vehicles' (n 82) 44.

The issue of data has also been considered by the NTC in the context of assessing the requirements for safety assurance for connected and automated vehicles. However, while the NTC acknowledged that 'privacy is an important consideration' it also considered 'that it falls outside the scope of the criteria for the Statement of Compliance' recommended by the NTC as a pre-market safety requirement for automated vehicles in Australia.[93] The NTC recommended 11 safety criteria for ADSEs to demonstrate their management of safety risks and recommended a further three obligations for ADSEs to assist with assigning liability in the event of a crash or a breach of the traffic laws, with one of these obligations relating to 'data recording and sharing'.[94] Data would be recorded to enable enforcement of traffic laws and safe vehicle operation, including data related to crashes. There would be a requirement for the recorded data to be made available by the ADSE to insurers, police, consumers and other relevant parties and in accordance with the provisions of the *Privacy Act*.[95]

The NTC has also published a consultation regulation impact statement ('RIS') on in-service safety for automated vehicles, that is, for service after the vehicles are on Australian roads.[96] Among the proposed safety criteria and obligations are obligations related to data recording and sharing which require that '[t]he applicant must outline the ADS data it will record and how it will provide the data to relevant parties'.[97] The RIS also notes that '[i]n responding to this criterion, the applicant should note that the *Privacy Act 1988* (Cth) places limitations on the collection, use and disclosure of personal information, which may limit the data the applicant can record and share'.[98]

Other legal developments in Australia will also help to shape the regulatory landscape relating to data.[99] For example, the Consumer Data Right will give consumers rights to facilitate access to and control of their data to assist consumer choice and the benefits of competition.[100] As the NTC has noted: '[t]he Commonwealth government's policy development highlights a move to improved data sharing. … the NTC is considering reform options for data sharing between government agencies to cover the new privacy challenges of C-ITS and automated vehicle technology'.[101]

---

93 '2018 Safety Assurance for Automated Driving Systems' (n 68) 74.

94 Ibid 134.

95 Ibid 147.

96 National Transport Commission Australia, 'In-Service Safety for Automated Vehicles' (Consultation Regulation Impact Statement, July 2019).

97 Ibid 137.

98 Ibid 138.

99 '2018 Access to Data Discussion Paper' (n 7) 75–7; '2019 Access to Data Policy Paper' (n 7) 64–6.

100 '2018 Access to Data Discussion Paper' (n 7) 75; '2019 Access to Data Policy Paper' (n 7) 64. See *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth).

101 '2018 Access to Data Discussion Paper' (n 7) 75. See also '2019 Access to Data Policy Paper' (n 7) 64.

V BUILDING PRIVACY INTO THE DRIVERLESS FUTURE

The NTC has proposed policy options for automated vehicle and C-ITS data.[102] The NTC has also developed a set of draft design principles for government access to C-ITS and autonomous vehicle data.[103]

In an analysis of privacy and data in relation to driverless cars, while a distinction can be drawn between data generated within C-ITS and the vehicles themselves, practical challenges may arise in the maintenance of this distinction. Many of the purported benefits of driverless cars, including those related to traffic congestion, will only arise when driverless cars are part of C-ITS. Once automated vehicles become connected vehicles and part of C-ITS, the ability to maintain a distinction between the categories of data and the source of the data (vehicle or C-ITS) is unclear. Furthermore, with one Australian survey of devices and products within the IoT finding that many did not have privacy policies and notices that adequately explained the collection, use and disclosure of personal information,[104] the connected nature of driverless cars may present privacy dilemmas for regulators, drivers, and others.

Adequate privacy protections will be an important part of fostering public trust in autonomous vehicles.[105] Privacy by design has been suggested as one way of implementing privacy protections in the development stage of new technologies.[106] Described as 'the next generation of privacy protection'[107] privacy by design is premised on 'building in privacy right up front, directly into the design specifications and architecture of new systems and processes'.[108] Seven foundational principles have been articulated for privacy by design:[109]

1. 'Proactive not Reactive; Preventative not Remedial' in which events that intrude on privacy are anticipated in advance, with the aim of preventing them;
2. 'Privacy as the Default' 'by ensuring that personal data are automatically protected in any given IT system or business practice';
3. 'Privacy Embedded into Design' meaning that 'privacy becomes an essential component of the core functionality being delivered';
4. 'Full Functionality – Positive-Sum, not Zero-Sum' in which all legitimate interests and objectives are accommodated;

---

102 '2018 Access to Data Discussion Paper' (n 7) 61–2; '2019 Access to Data Policy Paper' (n 7) 48–56. See also (n 67).

103 '2019 Access to Data Policy Paper' (n 7) 58–61.

104 Office of the Australian Information Commissioner, 'Privacy Commissioners Reveal the Hidden Risks of the Internet of Things' (Media Release, 23 September 2016) <https://www.oaic.gov.au/updates/news-and-media/privacy-commissioners-reveal-the-hidden-risks-of-the-internet-of-things/>.

105 Glancy (n 7) 1225; Daly (n 7) 844; '2016 Regulatory Reforms Policy Paper' (n 84) 17.

106 Glancy (n 7) 1226. See also Ira S Rubinstein, 'Regulating Privacy by Design' (2011) 26(3) *Berkeley Technology Law Journal* 1409.

107 Ann Cavoukian, 'Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-Makers and Policy-Makers' (White Paper, August 2011) 10, 27.

108 Ibid 10.

109 Ibid 28–9.

5. 'End-to-end Lifecycle Protection' where privacy 'extends securely throughout the entire lifecycle of the data involved, from start to finish';
6. 'Visibility and Transparency' of all parts and operations; and
7. 'Respect for User Privacy' with the interests of the individual kept uppermost through 'such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options'.

A privacy by design approach would allow for proactive management of the privacy-related issues for driverless cars.[110] The German report on automated vehicles discussed above advocates a privacy by default approach in which 'users take a decision of their own volition on the use of their data'.[111] One possible suggestion, outlined in the German report, is for the licensing of automated and connected driving functions:

> It would then only be possible for the vehicle to drive in automated mode if it is ensured that it obtains certain certificates, and when in operation, exchanges sufficiently pseudonymized condition data with other vehicles and the infrastructure.[112]

In Australia, in 2013 the Standing Council on Transport and Infrastructure agreed a recommendation 'that Austroads adopt privacy by design principles, including the undertaking of a privacy impact assessment, in the development of the C-ITS operational framework'.[113] In its discussion paper on data, the NTC noted that two of its reform

> options focus on limiting the collection, use and disclosure of C-ITS information to specific purposes and explicitly incorporating privacy by design elements where government directly collects C-ITS information.[114]

While privacy by design began as a concept, it has now been incorporated into the *GDPR*, converting it 'from a theoretical concept to a legal obligation and an essential principle of data protection that every controller and processor must respect'.[115] While the *GDPR* may be relevant to some Australian businesses, '[i]t does not however generally extend to processing of EU citizens' personal data in Australia, or processing of [their] personal data by law enforcement and other government agencies in Australia'.[116] However, by formalising the requirement for privacy by design through the *GDPR*, it is likely that European law will provide opportunities for considering how to put privacy by design into practice, including for C-ITS and automated vehicles.[117] Although privacy by design is just one aspect of broader privacy protections governed by privacy laws and regulation that may

---

110 Joshua Schoonmaker, 'Proactive Privacy for a Driverless Age' (2016) 25(2) *Information & Communications Technology Law* 96.

111 *Ethics Commission: Automated and Connected Driving* (n 59) 25.

112 Ibid.

113 '2018 Access to Data Discussion Paper' (n 7) 62.

114 Ibid 69.

115 Anna Romanou, 'The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise' (2018) 34(1) *Computer Law & Security Review* 99, 102. See also Vaile, Zalnieriute and Bennett Moses (n 7) 56.

116 Vaile, Zalnieriute and Bennett Moses (n 7) 53.

117 Daly (n 7) 837.

be relevant for new automation technologies, the concept provides a framework for articulating the co-design of new technologies and privacy protection.

VI CONCLUSION

Public trust will be an important element in the successful introduction of driverless cars in Australia and elsewhere. Concerns about data access and privacy have the potential to deter consumer trust in driverless vehicle technology, including C-ITS.[118] With the introduction of driverless cars at high levels of autonomy still in the future, there is now a window of opportunity in which to address these concerns. However the intersections between driverless cars and C-ITS, between federal, state and territory privacy laws, and between access to data and privacy, combine to form a challenging regulatory environment for transport-related data generated by driverless cars and C-ITS that will challenge the likelihood of providing clarity for consumers and motorists in this area. Yet regulatory clarity around the collection, use and sharing of data will be key to enabling innovations in transportation and to engaging public trust to support the adoption of driverless cars. While some of the challenges relating to data and driverless cars may be overtaken by broader regulatory reforms in Australia through proposed new federal data sharing legislation[119] and the introduction of a Consumer Data Right, whether these will prove sufficient in providing the necessary clarity for the driverless future remains to be seen.

118 Glancy (n 7) 1225–6; Daly (n 7) 844; '2016 Regulatory Reforms Policy Paper' (n 84) 17.

119 Department of the Prime Minister and Cabinet, 'New Australian Government Data Sharing and Release Legislation: Issues Paper for Consultation' (Issues Paper, Australian Government, 4 July 2018).