ENSURING LOCATION DATA PRIVACY IN CONNECTED AND AUTOMATED VEHICLES (CAVS)

AMY DUNPHY*

New privacy challenges will arise from the introduction of Connected and Automated Vehicle ('CAV') technology. CAVs are expected to 'drive' by a system that receives and shares data from sensorised infrastructure. CAV data will be constantly communicated wirelessly and bi-directionally, including with other CAVs which are operating within a vehicular network. Consequently, there will be a significant increase in the volume of data that will be generated by both CAVs and the operational infrastructure. This increase raises significant legal questions about whether CAV data is personal or sensitive information under the *Privacy Act 1988* (Cth). This is a threshold legal question because if CAV-related data does not fall into either of these categories, it may not be regulated by the *Privacy Act 1988* (Cth). One specific type of data that raises significant privacy concerns is CAV location data. This article examines the different jurisdictional approaches to classifying personal information in Australia, the European Union ('EU') and the United States ('US'). CAV-generated location data is used as a case study to examine potentially different framings of personal information in the CAV context. It applies the different jurisdictional notions of personal information under the *Privacy Act 1988* (Cth), the *General Data Protection Regulation* and the *Californian Consumer Privacy Act* to specified types of CAV-generated location data that are essential for operational purposes. Relevant jurisdictional case law, explanatory memoranda and policy guidance are used to formulate how different definitions would legally apply to the Australian CAV context. Following the application of different jurisdictional approaches, the article evaluates the additional protections that could be gained from an updated definition of personal information in the *Privacy Act 1988* (Cth) and undertakes a comparative analysis of the benefits of regulating CAV data (in particular, CAV location data) under a comprehensive framework or by adopting industry-specific law reform. In conclusion, the paper considers which law reform framework would best ensure that Australia remains at the forefront of regulating CAVs and addressing the privacy challenges they will create.

* Amy Dunphy (LLM, LLB(Hons), BA) is a graduate of the Australian National University and the University of Queensland. She is currently a PhD Candidate at the Queensland University of Technology and a senior lawyer at an international law firm with a focus on future automated transport and infrastructure.

I INTRODUCTION

High-level Connected and Automated Vehicles ('CAVs') have the potential to transform future mobility.[1] In these vehicles, the dynamic driving task (accelerating, steering, braking, assessing hazards and monitoring the environment) will be transferred from the human to the automated driving system ('ADS')[2] in specific environments, scenarios and locations. While CAVs are anticipated to deliver societal, economic and safety benefits, their deployment will not be without regulatory challenges.[3] From a privacy perspective, the range of personal and sensitive information that will aid the functionality of CAVs is important. A wealth of information will be gathered about CAVs and the people travelling within them.[4] A sophisticated cyber-controlled network of vehicles will share the positions of vehicles, velocities and observed traffic conditions, including precise geolocation data in real-time. The data collection may also extend to driver communications if mobile phones are linked to the computer system used by a high-level CAV.[5] Regardless, CAVs will generate an enormous amount of sensorised data.

A critical issue will thus be the regulation of the information privacy challenges arising from the public deployment of CAVs. Australian law does not currently have sector-specific legislation that would apply to CAVs. As such, the CAV information privacy challenges (for manufacturers and certain third-party suppliers) will be regulated by the *Privacy Act 1998* (Cth) ('*Privacy Act*'). However, suppose CAV data does not fall within the categories of personal information or sensitive information. In that case, CAV data may not be regulated by the *Privacy Act*, and CAV data may be able to be collected, used, disclosed and stored for any purpose, including marketing and commercial purposes.

This paper will examine whether location data will constitute 'personal information' under the *Privacy Act*. Location data was chosen because it raises novel challenges regarding CAVs' real-time and

---

[1] Society of Automotive Engineers International, 'Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_201806', (Web Page, 15 June 2018) <https://www.sae.org/standards/content/j3016_201806/>.

[2] National Transport Commission, 'Government Access to Vehicle Generated Data' (Discussion Paper, May 2020) https://www.ntc.gov.au/sites/default/files/assets/files/NTC%20Discussion%20Paper%20-%20Government%20access%20to%20vehicle-generated%20data_0.pdf 8 (NTC Government Data 2020 Discussion Paper).

[3] Greig Mordue, Anders Yeung and Fan Wu, 'The Looming Challenges of Regulating High Level Autonomous Vehicles' (2020) 132 *Transportation Research Part A: Policy and Practice* 174.

[4] Araz Taeihagh and Hazel Si Min Lim, 'Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks' (2019) 39(1) *Transport Reviews* 103, 113.

[5] Ivan Sucharski and Philip Fabinger, 'Privacy in the Age of Autonomous Vehicles' (2017) 73(2) *Washington and Lee Law Review* 724, 739.

historical tracking of users' routes and routines.[6] Further, the location data that CAVs rely upon has the potential to create novel information privacy risks that could be used improperly against the user's interests, such as the risk of stalking, discrimination, fraud, security incursions, data breaches or manipulation of a user's route or choices.[7] Moreover, the general regulation of location data under the *Privacy Act* is currently a controversial issue of law reform and one which is a significant issue of public concern.[8]

For example, the Australian Competition and Consumer Commission's ('ACCC') Digital Platforms Inquiry ('DPI') recommended modernising the definition of 'personal information' to reflect complex modern data collection and use.[9] Recently, the Attorney-General's review of the *Privacy Act* has proposed a number of measures to strengthen the definitions of personal information and sensitive information in Australia.[10] The proposed additional legal protections over location data included in both the DPI and Attorney-General's Review are designed in part to address the complexities introduced by the Full Federal Court's findings in *Privacy Commissioner v Telstra.*[11]

The proposed changes raise questions about whether comparable international developments should be introduced and whether the currently proposed reforms in Australia are sufficient to protect against CAV-related novel privacy issues. The *General Data Protection Regulation* ('*GDPR*')[12] has strengthened its privacy protections and is becoming an international best practice standard.[13] In the European Union ('EU'), the definition of 'personal data' under the *GDPR* specifically includes location

---

[6] Dasom Less and David Hess, 'Public Concerns and Connected and Automated Vehicles: Safety, Privacy and Data Security' (2022) 9(90) *Humanities and Social Sciences Communications* 1, 5.

[7] These risks are discussed in further detail at section II.A below.

[8] Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy' (Survey, 2020) 7: 'half (48%) of Australians consider location information to be one of the biggest privacy risks today, and only a quarter (24%) feel that their location information is well protected by law and Regulations'.

[9] ACCC, *Digital Platforms Inquiry* (Final Report, 25 June 2019) ('DPI').

[10] Attorney-General (Australia), 'Review of the Privacy Act 1988 (Cth)' (Issues Paper, 30 October 2020); Attorney-General (Australia), 'Privacy Act Review' (Discussion Paper, 25 October 2021) ('Attorney General's Discussion Paper'); Attorney-General (Australia), *Privacy Act Review* (Report, 16 February 2023) ('Attorney-General's Privacy Act Review Report').

[11] (2017) 249 FCR 24.

[12] *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 *('GDPR')*.

[13] Michelle Goddard, 'The EU General Data Protection Regulation (GDPR): European Regulation That Has a Global Impact' (2017) 59(6) *International Journal of Market Research* 703, 705.

data.[14] The potential incorporation of the *GDPR* approach into Australian regulation raises policy questions due to the international nature of CAV manufacturers, including those from the United States ('US'). As such, it is important to examine whether US information privacy laws should be primarily applied in the Australian context, as opposed to the *GDPR*. The recent adoption, on a state basis, of comprehensive privacy regulation in the US under the *California Consumer Privacy Act* ('*CCPA*')[15] will also be considered, as well as sector-specific approaches to CAVs within the US.

Section 2 of this paper will examine the CAV data environment and highlight the critical importance of location data to a CAV's operation. Section 3 will outline the policy and legislative background to 'personal information' in Australia under the *Privacy Act*. It will investigate the different jurisdictional approaches to classifying personal information (or personal data) under the comprehensive approach in the *GDPR*, the *CCPA* and the sectoral approach in the US. Section 4 will provide a comparative analysis of the different approaches to regulating personal information with a specific application and focus on CAV location data. Similarities, discrepancies and gaps between the Australian and international approaches will be identified, and the appropriateness of overseas models will be considered in the Australian regulatory context. It will discuss reframing the definition of personal information in the Australian context. Consideration will be given to appropriate law reform of the Australian information privacy system to prepare for the current and future technical development of CAVs and the impact of CAV location data. Section 5 will briefly conclude the paper and summarise the key research findings.

This article will seek to fill the gap left by Australian enquiries to date that have focused on government access to CAV, Cooperative Intelligent Transport Systems ('C-ITS') and vehicle-generated data and consider the issues of private company or third-party access to location data.[16] This is a significant gap in the current literature and a novel issue. It must be explored given the unprecedented levels of access to location data that CAVs will make available to numerous stakeholders within the CAV ecosystem and the related impact on the application of the definition of personal information.

---

[14] *GDPR* (n 12) art 4(1).

[15] *California Consumer Protection Act, 55* Cal Civil Code (West 2018) *('CCPA')*.

[16] National Transport Commission, *Regulating Government Access to C-ITS and Automated Vehicle Data* (Discussion Paper, September 2018) ('NTC Automated Vehicle Data 2018 Discussion Paper'); National Transport Commission, *Government Access to Vehicle-Generated Data* (Discussion Paper, May 2020) 27 ('NTC Vehicle Generated Data 2020 Discussion Paper').

II CAVS AND LOCATION DATA

A *Overview*

This article examines the location data that will be used, collected and stored by level 4, highly automated vehicles as defined by the Society of Automotive Engineers ('SAE').[17] In these vehicles, the ADS will assume control of the driving task and the monitoring of the environment, including by automatically bringing the vehicle to a stop.[18] While the term 'autonomous vehicle'[19] is often used interchangeably in the literature with 'automated vehicle', this article recognises that important differences in terminology arise. Compared to an automated vehicle, a fully 'autonomous vehicle' (or 'driverless vehicle') is one where the vehicle independently performs all aspects of the dynamic driving task in all environments and conditions on a full-time basis and without any human intervention[20] and is often recognised as SAE level 5. The main difference between levels 4 and 5 SAE is that level 4 will only be automated (or able to operate 'autonomously') in certain situations, and manual transition to the human driver may need to occur following the provision of sufficient warning.

A key limitation of CAV research is that the precise timeframe for deployment of CAVs and applicable level(s) of automation are unclear. Further, the implication of applying the SAE definition in descriptions of CAVs is that technological progress will move linearly through the various levels. In reality, competing trajectories and contingencies may occur and depend on a number of factors.[21] That said, recent policy research papers prepared in Australia by the National Transport Commission ('NTC') and international publications, such as the guidelines published by the European Data Protection Board ('EDPB'), have examined the processing of personal data in relation to level 4 vehicles.[22] Location data in

---

[17] Society of Automotive Engineers International (n 1).

[18] Jonathan Petit and Steven Shaldover, 'Potential Cyberattacks on Automated Vehicles' (2015) 16(2) *IEEE Transactions on Intelligent Transportation Systems* 546, 548.

[19] Dasom Lee and David Hess, 'Regulations for On-road Testing of Connected and Automated Vehicles: Assessing the Potential for Global Safety Harmonization' 136 *Transportation Research Part A* 86.

[20] Tess Bennett, *SAE Simplifies Explanation of Driverless Vehicle Levels to Show Who is in Control of the Car* (Web Page, 13 December 2018) <https://which-50.com/sae-simplifies-explanation-of-driverless-vehicle-levels-to-show-whos-in-control-of-the-car/>.

[21] Tom Cohen, Jack Stilgoe and Clemence Cavoli, 'Reframing the Governance of Automotive Automation: Insights from UK Stakeholder Workshops' (2018) 5(3) *Journal of Responsible Innovation* 257, 262.

[22] It is noted that the data driven technology that will power existing level 4 automated vehicles, which have typically operated in test environments or defined geolocations (such as universities), are expected to be different to publicly available level 4 CAVs. However, location data, and in particular the use of the Global Positioning System ('GPS') tracking, is expected to become an increasingly important and key feature of the public deployment of level 4 CAVs

level 4 CAVs enables assessment of proximity in relation to other CAVs, obstacles and traffic infrastructure by predominantly using the Global Positioning System ('GPS') and Radio Detection and Ranging ('radar').[23] CAVs that operate at high levels of autonomy for extended periods of time without a driver are an appropriate context for enquiry, as they are recognised as being technologically possible and imminent, although implementation timeframes may differ globally.[24]

CAV location data may yield a number of benefits for users, private companies and governments as a result of the ability to share information regarding traffic congestion and environmental and road conditions with other vehicles, infrastructure and entities. It may enable CAVs to adjust positioning, assume better, more efficient routes, and improve safety.[25] For governments, access to the location data could improve infrastructure development, road safety or maintenance outcomes. For original equipment manufacturers, the use of location data may be in the form of improvements in vehicle design and production and knowledge about how the car is used. Similarly, third-party suppliers may deliver vehicle-enhancing services, such as software updates or tailored insurance products. For the individual consumer, it can provide access to valuable information about vehicle use, which could, for example, be utilised for insurance policies (such as 'pay how you drive' insurance) or for routing of electric vehicle charging stations.[26] Location data may be linked with crash data for insurance purposes to identify, for example, who was in control of a vehicle at the time of an accident or whether the passenger responded in time (if the CAV is not operating at full automation).

However, these anticipated benefits are mixed in with new and novel privacy challenges and concerns. One of the challenges with location data is the difficulty in defining and regulating its scope.

---

as the identification of the precise position of a vehicle will be a critical feature. See, eg, Lijun Wei, Cindy Cappelle and Yassine Ruichek, 'Camera/Laser/GPS Fusion Method for Vehicle Positioning Under Extended NIS-Based Sensor Validation' (2013) 62(11) *IEEE Transactions on Instrumentation and Measurement* 3110, 3110–3122.

[23] Sankar P and Gayathri Voorandoori, 'Intelligent Transportation Systems and Its Necessity in Various Traffic Conditions in Indian Scenarios' in Nishu Gupta, Arun Prakash and Rajeev Tripathi (eds), *Internet of Vehicles and its Applications in Autonomous Driving* (Springer Cham, 2021) 13, 14.

[24] Felipe Jimenez et al, 'Communications and Driver Monitoring Aids for Fostering SAE Level 4 Road Vehicles Automation' (2018) 7 *Electronics* 228, 230.

[25] Ellie Burns, 'Why Location Data is the Driving Force Behind Autonomous Cars', *TechMonitor* (online, 7 November 2017) <https://techmonitor.ai/leadership/digital-transformation/location-data-driving-autonomous-cars>; Sankar P and Gayathri Voorandoori (n 23) 14–15.

[26] European Automobile Manufacturers Association, *Access to Vehicle Data for Third-Party Services* (Position Paper, December 2016) <https://www.acea.auto/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf>.

This issue stems from the ubiquity of modern connectivity that enables applications, platforms, operating system providers and other third parties to obtain information about the location of the device (and, consequently, its user).[27] The shift to smartphones and connected devices has increased the proliferation of tracking information from a device's IP address, GPS chips and Bluetooth signals (such as from wearable devices), as well as the proximity to cell towers and networks.[28]

In some ways, location data generated through high-level CAVs can be compared to data collected by mobile phones or currently available vehicles. Speed, location and other navigation and location data are already collected by GPS systems in cars and on mobile phones. Mobile phones can already connect to vehicles available on the market, and this may take place through multiple forms such as Wi-Fi, Bluetooth or infotainment systems. A study into connected vehicles' infotainment systems revealed that the infotainment system was recording location data even when GPS was not enacted.[29] Mobile phone application location data is already collected and used by ride-share and passenger services. This data may, for example, be used by transport agencies for traffic management and network optimisation.[30] From a rental car perspective, an expansion of information may be generated and processed by vehicles as they increasingly offer the ability to connect to mobile phones with the availability to download phone books to enable services such as connected phone calls, messages, internet browsing and media streaming.[31] If this data is not deleted from the vehicle or safeguarded, there is a risk that the stakeholders involved (i.e., fleet companies) or future users of the vehicle could access this information.[32] In this way, there are existing devices and capabilities in on-market vehicles that generate location data and present privacy challenges.[33]

---

[27] Jacek Chmielewski, 'Device-Independent Architecture for Ubiquitous Applications' (2014) 18 *Personal and Ubiquitous Computing* 481; Karen Lewis, 'Where's My Stuff? How Location and IoT Play Well Together', *IBM* (Blog Post, 21 October 2016) < https://www.iotone.com/guide/where-rsquo-s-my-stuff-how-location-and-iot-play-well-together/g247>.

[28] See, eg, Ke Wan Ching and Manmeet Mahinderjit Singh, 'Wearable Technology Devices Security and Privacy Vulnerability Analysis' (2016) 8(3) *International Journal of Network Security & Its Applications* 19.

[29] Jessie Lacroix, 'Vehicular Infotainment Forensics' (MSc Thesis, University of Ontario Institute of Technology, 2017).

[30] NTC Vehicle Generated Data 2020 Discussion Paper (n 16) 38.

[31] 'Connected Cars: What Happens to Our Data on Rental Cars', *Privacy International* (Web Page, December 2017) 2 <https://privacyinternational.org/sites/default/files/2017-12/cars_briefing.pdf>.

[32] Ibid 11.

[33] It is noted that such location data has a duality of being challenging from a privacy perspective but, if used correctly, having the ability to bring positive benefits such as improving network operational decisions and vehicle safety.

However, it is the widespread dissemination of more accurate location data over C-ITS that will create new and even more expansive privacy challenges in high-level CAVs by capturing and using more granular and timely location data. Privacy concerns arise because C-ITS has far more accurate and detailed data and because location data is physically applied to an object controlling a person's safety and mobility.[34] That is, CAVs will use location data (amongst other data) to 'drive' a passenger and likely tailor the service or transport route based on the individual's data. Further, mobile phones and other privately owned devices potentially give users opt-in capabilities. Highly automated CAVs are unlikely to be able to give notice of all the information that is required to be captured from the operating environment to make CAVs function. Mobile phones are also anticipated to play an ever-increasing role in the use of CAVs, with integrated mobile apps, infotainment, and telematics services available in vehicles. This increase in the quality and quantity of data and points of entry has significant implications for increased risk and probability of linking and cross-referencing information to identify an individual. As data sources increase, device identifiers (e.g., IP address or mobile phone serial number) may, in conjunction with vehicle location data, give greater context to identifying an individual.[35]

Critically, the matter of a CAV user's ability to consent to the collection and use of location data is tied to the risk of improper use. Notification and consent regimes play a fundamental role for individuals to manage their privacy risks and make informed choices.[36] Nevertheless, given the rapid nature of CAV data processing, it is anticipated to be impractical or impossible for a user to consent to the collection of personal or sensitive information or its disclosure for a secondary purpose as it changes along a CAV journey.[37] If asking for a CAV user's consent could, in fact, put the human driver turned passenger at a safety risk (for instance, due to distraction during the handover of the CAV to its autonomous system), then this is clearly undesirable.[38] Similarly, the method of notification about the range of potential secondary uses of the CAV location data is unresolved.[39]

---

[34] NTC Vehicle Generated Data 2020 Discussion Paper (n 16) 27.

[35] 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) 16 <https://www.ntc.gov.au/sites/default/files/assets/files/UNSW-report-privacy-and-data-protection-regulatory-framework-for-avs.pdf>.

[36] Relevantly, Australian Privacy Principle ('APP') 5.1 states that an APP entity must take *reasonable steps* either to notify an individual of the APP 5 matters or to ensure they are aware of the matters (emphasis added).

[37] Marcia Cristina Gaeta, 'Data protection and Self-Driving Cars: The Consent to the Processing of Personal Data in Compliance with GDPR' (2019) 24(1) *Communications Law Journal* 15, 17.

[38] See the existence of exemptions for consent for collection of sensitive information, eg, 'permitted health situation'.

[39] Vaile, Zalnieriute and Moses (n 35) 20, 35.

One of the most commercially valuable sets of CAV data will be travel patterns that identify whether a person frequently visits certain places of worship, a medical facility or lives in a high-value residential area. This logging of past routes could also be used to predict future routes and, for example, to manipulate a person's choices about where to shop or to suggest healthcare alternatives or other suppliers.[40] While these offerings may provide significant benefits to CAV users, there is a risk of improper use of this data. There is also the risk that Australian Privacy Principle ('APP') entities collecting or owning the data, or data brokers, could share or sell CAV location data with third parties (such as advertisers, marketers or political campaigns). If their data falls into the wrong hands, CAV users may subsequently be vulnerable to fraud, harassment, identity theft or discrimination based on their attributes. For example, users with an identified disability (such as a person with blindness) based on their location tracking (such as where the CAV drops them off) could be at risk of not being offered certain services. Alternatively, those routinely visiting a place of worship could be discriminated against, for example, by targeted advertising based on their perceived race or religion. Moreover, the protection of this personal information and data goes hand in hand with limits on the powers held by governments and private entities, as well as the trust that individuals place in third parties.[41] Even if governments or private organisations are currently trusted, as time passes, and as technology advances and more data is generated and collected, the risk that it may be misappropriated and misused by future (or foreign) governments or intelligence agencies increases.[42]

The increase in cyber-attacks[43] has revealed the vulnerability of cyber and cloud-based systems (such as those used by CAVs) to being compromised by dishonest actors.[44] The high mobility of CAVs makes them a vulnerable and valuable target for cyber-attacks with potentially serious consequences. If realised, location data incursions are anticipated to reduce public trust in CAVs, impede innovation

---

[40] 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) <https://nla.gov.au/nla.obj-3065138999/view>.

[41] Paul Bernal, 'Data Gathering, Surveillance and Human Rights: Recasting the Debate' (2016) 1(2) *Journal of Cyber Security* 243, 244.

[42] Kate Galloway, 'Big Data: A Case Study of Disruption and Government Power' (2017) 42(2) *Alternative Law Journal* 89.

[43] Albeit in other contexts.

[44] Eric Schoitsch, Christoph Schmittner, Zhendong Ma and Thomas Gruber, 'The Need for Safety and Cyber-Security Co-Engineering and Standardization for Highly Automated Automotive Vehicles' in Tim Schulze, Beate Muller and Gereon Meyer (eds) *Advanced Microsystems for Automotive Applications* (2015) 251, 255.

benefits and potentially put users at risk of physical and online harm. Moreover, if used improperly, the collected data could be used for sinister effects such as stereotyping, stalking or character profiling.

A significant additional layer of data concerns arises from the complexities of CAVs operating as a ride-share service. It will be necessary to ensure that no footprint could enable a future or fellow passenger to exploit the data of previous or shared occupants.[45]

The companies leading the development of CAVs have not been immune to data breaches involving location data and information. This suggests that the risk of future breaches in the CAV space is not improbable but one which must be carefully considered. The best possible protections must be put in place (which starts with ensuring that data is regulated by privacy legislation). For example, Uber was the subject of an investigation by the United States Federal Trade Commission regarding alleged breaches of Uber drivers' and consumers' personal information. The data breaches stated in the Complaint brought by the Federal Trade Commission allegedly involved, amongst other information, over 100,000 unencrypted names and driver's licences in 2014[46] and approximately 25.6 million names and email addresses of riders and drivers in 2016.[47] As part of the Federal Trade Commission's Decision and Order, Uber was mandated to implement a comprehensive privacy program designed to protect personal information (amongst other Orders).[48]

---

[45] Louis Bedigian, 'Connected Cars Both Best Friend and Worst Enemy, Warns BlackBerry', *TU Automotive* (Article, 24 May 2019) <https://www.tu-auto.com/connected-cars-both-best-friend-and-worst-enemy-warns-blackberry/?NL=TU-001&Issue=TU-001_20190528_TU-001_643&sfvc4enews=42&cl=article_1>;
Lisa Collingwood, 'Privacy Implications and Liability Issues of Autonomous Vehicles' (2017) 26(1) *Information & Communications Technology Journal* 32, 44.

[46] Joseph Simons, Noah Phillips, Rohit Chopra, Rebecca Slaughter and Christine Wilson, 'In the Matter of Uber Technologies, Inc., A Corporation: Revised Complaint Docket No. C-4662', United States Federal Trade Commission (Complaint No 152304, 25 October 2018) [21] <https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_complaint.pdf>.

[47] Ibid [24].

[48] Joseph Simons, Noah Phillips, Rohit Chopra, Rebecca Slaughter and Christine Wilson, 'In the Matter of Uber Technologies, Inc., A Corporation – Decision and Order Docket No. C-4662', United States Federal Trade Commission (Complaint No 1523053, 25 October 2018) II <https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf>.

While CAV data will not be homogenous at all levels of automation, data within the vehicle is anticipated to be stored, transmitted over the internet or broadcasted over telecommunication networks.[49] The effect on the way data is stored, broadcasted or shared can impact the various stakeholders within the CAV ecosystem in different ways. While most data concerning the operation of CAVs will be volatile, there will be certain operating data that will be recorded and stored, both to enable the monitoring of the vehicle for its operation and for product assurance.[50] By potentially providing private and public entities with unprecedented levels of access to personal and sensitive information, new privacy risks for owners, drivers and passengers will arise. Consequently, whether CAV-generated location data is personal or sensitive information and how it is managed are crucial questions to resolve.

B *Technology Underpinning CAV Location Data*

The issue of CAV location data is also borne out in the technology underpinning its collection and use. As CAV technology matures, it may result in imperfect vehicle positioning, mapping and location data collection or use. For CAVs, GPS will undeniably be a critical part of localising any vehicle.[51] Significant developments have been made in GPS accuracy, but errors can still occur. Some of these errors can be significant, impacting the accuracy of the assessed data by several metres.[52] This lack of accuracy can be an issue, particularly in built, inner-city environments, where office towers and urban sprawl can distort GPS signals.[53] Having a high degree of accuracy in the underlying maps is another challenge in developing a self-driving system.[54] Roadways typically contain numerous dynamic and temporary objects, so any localisation system will need to understand which objects are temporary to avoid and then use them as landmarks when localising both cars and pedestrians.[55] Other potential errors include changes in appearance (e.g., the differences between day and night) and any changes to the

---

[49] Mark Brady, 'Data Privacy and Automated Vehicles: Navigating the Privacy Continuum' (2020) 45(3) *Monash University Law Review* 589, 594.

[50] European Automobile Manufacturers Association, *ACEA Strategy Paper on Connectivity* (Strategy Paper, April 2016) <https://www.acea.auto/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf>.

[51] Amr Mohamed et al, 'Literature survey for Autonomous Vehicles: Sensor Fusion, Computer Vision, System Identification and Fault Tolerance' (2018) 12(4) *International Journal of Automation and Control* 555, 557.

[52] For example, errors and difficulties with using GPS may arise in circumstances of bad weather or where the signal is weaker (such as within city centres). See Mohamed et al (n 51) 557.

[53] James Anderson et al, *Autonomous Vehicle Technology: A Guide for Policy Makers* (Report, 2016) 63.

[54] Karl Rehrl and Simon Grochenig, 'Evaluating Localization Accuracy of Automated Driving Systems' (2021) 21(17) *Sensors (Basel)* 5855.

[55] Kichun Jo, Chansoo Kim and Myoungho Sunwoo, 'Simultaneous Localization and Map Change Update for the High Definition Map-Based Autonomous Driving Car' (2018) 18(9) *Sensors* 3145.

structure of the environment over time (e.g., new road works, new exits and the construction of new buildings).[56]

Significant work remains to be done in terms of developing the form of high-quality maps that CAVs can safely use. CAVs will need to rely upon a High Definition ('HD') map, which extends upon an enhanced digital map by recording a 3D representation of the world that is physically around the vehicle.[57] Such information will be generated using a variety of sensors, including Light Detection and Ranging ('LiDAR'), radar and cameras.[58]

One of the greatest challenges in using an HD map for CAVs is the localisation component.[59] As detailed position information is added to the digital map, it will be critical to know the exact position of the vehicle within the map.[60] Further, a localisation system needs to have the ability to identify temporary and dynamic objects and to avoid using them as landmarks. The technology that is currently available is considered to be insufficient to support fully autonomous operations.[61]

CAV mapping data will also involve complex data flows between a number of key parties, including government transport agencies and authorities, private HD map providers and CAVs (and companies that are related to them).[62] That is, HD map data will be a global shared state—being shared and updated by multiple CAVs and parties with ongoing real-time updates.[63] The ability to create HD maps with real-time accuracy for an entire city or country will depend on the installation of significant new digital infrastructure and communications technology across road networks and collaboration occurring

---

[56] Jun Wang et al, 'Safety of Autonomous Vehicles' (2020) *Journal of Advanced Transportation* 1, 4.

[57] Stephen Hausler and Michael Milford, 'Map Creation, Monitoring and Maintenance for Automated Driving: Literature Review' (Literature Review No P1-21, iMove Australia, 11 December 2020) 12, 13 <https://imoveaustralia.com/wp-content/uploads/2021/01/P1%E2%80%90021-Map-creation-monitoring-and-maintenance-for-automated-driving.pdf> ('iMove Map Literature Review').

[58] Ibid.

[59] Michael Milford, Sourav Garg and James Mount, 'How Automated Vehicles Will Interact with Road Infrastructure Now and in the Future' (Literature Review No P1-007, iMove Australia, January 2020) 17 <https://imoveaustralia.com/wp-content/uploads/2020/02/P1-007-Milestone-6-Final-Report-Second-Revision.pdf>.

[60] iMove Map Literature Review (n 57) 16.

[61] Ibid.

[62] For example, messages may be exchanged between the Government as the infrastructure provider to high-definition map providers and in turn to the CAVs.

[63] iMove Map Literature Review (n 57) 11.

between governments and private companies that operate within the CAV market.[64] The current state of international development of HD maps varies widely—from Japan, where the government is working with the private sector to develop HD maps for CAVs,[65] to the EU, where HD maps are under review in partnership with key private players such as TomTom.[66]

GPS is often associated with an inertial navigation system ('INS') to fill the information gaps, which continuously calculates the position of a vehicle using rotation sensors (gyroscopes) and motion sensors (accelerometers).[67] The collection of mapping data will be an enormous task. For example, the level 4 automated vehicle developed by Google's Waymo has reported collecting approximately 1GB of data every 20 seconds.[68] DeepMap has lodged a patent that specifies that the size of a country-wide HD map will be in the Petabyte size range.[69] This complex and rich tracking data that CAVs will generate will also raise further key points, such as data ownership issues between the private sector and governments, security of data issues, and personal privacy concerns.

III REGULATION OF PERSONAL INFORMATION

A *The Australian Privacy Act*

Australian information privacy law is governed at the federal level by the *Privacy Act*. The foundational framework for the *Privacy Act* is based on the principles for data collection, storage and use set out in the Organisation for Economic Co-operation and Development's ('OECD')[70] Guidelines on the Protection of Privacy and Transborder Flows of Personal Information ('OECD Guidelines').[71] The

---

[64] Tyler Duvall et al, 'A New Look at Autonomous-Vehicle Infrastructure' *McKinsey* (Blog Post, 22 May 2019) <https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/a-new-look-at-autonomous-vehicle-infrastructure>.

[65] Hiroshi Sakurai, 'Safer Traffic with Dynamic Map' *Public Relations Office, Government of Japan* (Web Page, January 2018) <https://www.gov-online.go.jp/eng/publicity/book/hlj/html/201801/201801_04_en.html>.

[66] Vincent Demuynck, 'How Do HD Maps Extend the Vision of Autonomous Vehicles?' *TomTom* (online, 16 January 2020) <https://www.tomtom.com/newsroom/product-focus/hd-maps-vision-autonomous-driving/>.

[67] Robert Christ and Robert Wernli, *The ROV Manual: A User Guide for Remotely Operated Vehicles* (Butterworth-Heinemann, 2nd ed, 2014).

[68] Andrew Hawkins, 'Waymo is Making Some of Its Self-Driving Car Data Available for Free to Researchers' *The Verge* (online, 21 August 2019) <https://www.theverge.com/2019/8/21/20822755/waymo-self-driving-car-data-set-free-research>.

[69] *US Patent No 10801845B2*, filed on 17 August 2019 (Granted on 13 October 2020).

[70] The OECD represents a unique collaboration between governments to address global challenges, such as privacy.

[71] OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD/LEGAL/0188, 11 July 2013)

Privacy Act develops 13 principles, collectively called the Australian Privacy Principles ('APPs'), in schedule 1 of the Act. The *Privacy Act* and APPs apply to Australian government agencies and organisations with an annual turnover of more than $3,000,000 and some smaller private sector organisations (for instance, private sector health providers) unless a limited exemption applies.[72] The APPs set out information privacy obligations for entities collecting data while affording individuals protection with privacy rights. The OECD Guidelines also form the basis for Australian state and territory-based privacy legislation, which regulates relevant government agencies under separate state and territory legislation.[73]

The *Privacy Act* does not seek to prescribe privacy rights to Australian persons but rather establishes a basis for a technology-neutral and principled approach to privacy regulation,[74] which is supplemented by other regulations as considered appropriate by regulators. As a principles-based regulation at its foundation, the *Privacy Act* is intended to provide an overarching information privacy framework and facilitate regulatory flexibility to adapt to new and changing situations.[75] This concept of principles-based regulation was later justified by the Australian Law Reform Commission ('ALRC'),[76] which argued that principles-based regulation offered greater flexibility and enabled the regime to respond to new issues as they arise without having to create new legal rules.[77] However, as technology has progressed and as the data collected becomes more expansive and complex, there are growing concerns that the *Privacy Act* is struggling to keep up.[78]

The focus of this article is on information privacy as regulated under the *Privacy Act*, as it is anticipated that most private organisations operating within the CAV chain (such as manufacturers and software developers) will fall within the scope of the *Privacy Act* and the APPs. One key issue is whether location data will be regulated by the *Privacy Act.* The reason for this is three-fold. First, CAV-related companies will satisfy the relevant monetary threshold. Second, they will likely be the APP entity

<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>.

[72] *Privacy Act 1988* (Cth) *('Privacy Act')* s 6D(4).

[73] *Privacy and Personal Information Protection Act 1998* (NSW); *Information Act 2002* (NT); *Information Privacy Act 2009* (Qld); *Information Privacy Act 2014* (SA); *Privacy and Data Protection Act 2014* (VIC).

[74] Mark Burdon, *Digital Data Collection and Information Privacy Law* (Cambridge University Press, 2020) 152.

[75] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 1, 235 ('ALRC Report').

[76] Ibid. See the discussion of the ALRC Report in *Jurecek v Director, Transport Safety Victoria* (2016) 260 IR 327 [60].

[77] ALRC Report (n 75).

[78] Ibid 421.

responsible for data collection and classification.[79] Third, from a privacy perspective, location data has important implications whether it is handled in accordance with the *Privacy Act* or not.

The definition of personal information is set out in s 6(1) of the *Privacy Act* to mean 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. Proposal 4.1 of the Privacy Act Review Report is to amend the reference to 'about' to 'relates to' to undo some of the uncertainty following the decision in *Privacy Commissioner v Telstra*[80] (discussed below).[81]

A further subset of personal information is sensitive information that includes information about, amongst other things, an individual's race, ethnicity, political or religious beliefs, sexual orientation and criminal record.[82]

Defining personal information has consistently been a bone of policymaker contention for the last two decades. For example, the Australian Law Reform Commission comprehensively reviewed the *Privacy Act* in 2008 and recommended an updated definition of personal information.[83] The *Privacy Act* was amended in 2014 to include this, as well as other significant changes.[84] However, the current application of the definition of personal information is uncertain, following the Federal Court's decision in *Privacy Commissioner v Telstra*.[85] In that case, the Federal Court found that certain technical data, namely certain types of telecommunications metadata, was not personal information because it was not 'about' an individual. The case history is informative as it highlights the way in which the issue is unresolved. Although the Federal Court's determination was made under an older definition under the *Privacy Act*, the definition of 'personal information' has not materially changed, and the impact of the Court's reasoning remains relevant.[86]

---

[79] It is noted that some additional obligations may still be imposed on private sector organisations in the relevant Australian state or territory with the consequence that, depending on the type of information, some organisations may have to comply with a wide range of regulatory regimes concurrently.

[80] *Privacy Commissioner v Telstra* (n 11).

[81] Attorney-General's Privacy Act Review Report (n 10) 24–25.

[82] *Privacy Act* (n 72) s 6(1).

[83] ALRC Report (n 75).

[84] *Privacy Amendment (Enhancing Privacy Protection) Act 2021* (Cth).

[85] *Privacy Commissioner v Telstra* (n 11).

[86] Relevantly, the parties in *Privacy Commissioner v Telstra* agreed that the relevant date for the applicable version of the *Privacy Act* was 1 July 2013 and that National Privacy Principle ('NPP') 6.1 in Schedule 3 applied to when an

In *Privacy Commissioner v Telstra,* an individual, Mr Ben Grubb, brought a claim that he had a right to access his metadata information stored by Telstra, including mobile phone network data recording IP, URL and cell phone tower information.[87] When Telstra refused access to this information, Mr Grubb made a complaint to the Privacy Commissioner, who upheld his action.[88] Deputy President Forgie in the Administrative Appeals Tribunal ('AAT') determined that before considering whether an individual could be identified from the metadata information, the threshold question of whether the information was 'about an individual' had first to be considered.[89] The AAT held that if the information or an opinion is not about an individual, then 'that is the end of the matter'.[90] However, if the information is about an individual, the second step is to question whether the identity of that individual 'is apparent or can reasonably be ascertained, from the information or opinion'.[91] Ultimately, the AAT determined that Telstra's mobile network data was not 'personal information' as it was not information 'about an individual' but rather about the way Telstra delivered their service, product, calls or messages.[92] The Privacy Commissioner then appealed the AAT decision to the Full Court of the Federal Court. Interestingly, the appeal brought by the Privacy Commissioner concerned a limited question of statutory interpretation that focussed on the meaning of the term 'about an individual' in the definition of personal information and did not specifically call into question the AAT's determination about whether metadata could be personal information.[93]

The Federal Court dismissed the Commissioner's appeal, but the decision is limited in its application. The Federal Court's decision was constrained to what it described as a 'very narrow question of statutory construction',[94] being whether the words 'about an individual' had a substantive meaning on their own.[95] Having found it in the affirmative, the Court upheld the AAT's factual finding and did not address the broader question of whether metadata would be about an individual.[96] The Federal Court

---

organisation must provide an individual with access to personal information it holds about the individual (unless an exemption applied). Since the 2014 amendments to the *Privacy Act,* NPP 6.1 was replaced with APP 12.1: *Privacy Commissioner v Telstra* (n 11); *Privacy Act* (n 72) sch 1 *('APPs').*

[87] *Privacy Commissioner v Telstra* (n 11).

[88] Ben Grubb and Telstra Corporation Limited [2015] AICmr 35 (1 May 2015).

[89] *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991 [89].

[90] Ibid [97].

[91] Ibid.

[92] Ibid [113].

[93] *Privacy Commissioner v Telstra* (n 11) [5].

[94] Ibid [63].

[95] Ibid [5].

[96] Except Dowsett J in obiter.

expanded upon the AAT's decision and, considering the totality of the information, favoured using an 'evaluative conclusion'.[97] Unfortunately, the Federal Court only provided limited guidance as to how this 'evaluative conclusion' was to be made and did not opine on whether the AAT's 'evaluative conclusion' was correct (it being outside the scope of appeal).[98] In the wake of the decision, the Australian Information Commissioner's guidance note further complicates the analysis by recognising that if the information reveals or conveys something about a person, it will be 'about' them, even if at first that person did not appear to be the subject matter of the information.[99]

A further example of the tension that exists in Australian privacy law,[100] specifically about location data (or travel data) constituting personal information, is the decision of *Transport for New South Wales v Waters (No 2)* [2019] NSWCATAP 96. Here, the Appeal Panel found that the Department's collection of travel data obtained through an individual 'tapping on and off' using the electronic ticketing system for public transport was personal information within the meaning of section 4 of the *Privacy and Personal Information Protection Act 1998* (NSW).[101] The Appeal Panel concluded, overturning the first instance decision,[102] that the travel data was collected for the lawful purpose of the Department's ticketing functions and activities and was reasonably necessary for the purpose.[103]

Because of this policy uncertainty, in 2019, the ACCC's DPI recommended that the definition of personal information needed to change to be in line with modern standards and technology, but it did not recommend a specific updated formulation.[104] As a result of the DPI, the Attorney-General's Department undertook a review of the *Privacy Act* as set out in its Issues Paper published in October 2020.[105] A key focus of the proposed reforms was the potential for updates to the definition of personal information. On 25 October 2021, the Attorney-General's Department delivered its Discussion Paper with a developed position on reform to change the definition of 'personal information'.[106] Following a further two-year extensive consultation and review process, on 16 February 2023, the Attorney General's

---

[97] *Privacy Commissioner v Telstra* (n 11) [63]–[64].
[98] Ibid [65].
[99] Office of the Australian Information Commissioner, 'What is Personal Information' *Privacy Guidance and Advice* (Web Page, 5 May 2017) <https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information>.
[100] Albeit under state based Australian privacy legislation.
[101] *Transport for New South Wales v Waters (No 2)* [2019] NSWCATAP 96, [9]–[12] *('Waters (No 2)')*.
[102] *Waters v Transport for New South Wales* [2018] NSWCATAD 40.
[103] *Waters (No 2)* (n 101) [35]–[36].
[104] DPI (n 9).
[105] Attorney-General's Discussion Paper (n 10).
[106] Ibid.

Department released its Privacy Act Review Report, which proposed a number of changes that would bring Australian privacy law into line with, or move it towards, the protections in the *GDPR*. In particular, proposal 4.2 of the Privacy Act Review Report is to include a non-exhaustive list of data, such as location data, in the definition of 'personal information'.[107] Further, proposal 4.10 recommended recognising that the collection, use, disclosure and storage of precise geolocation data was a practice that requires consent.[108] 'Geolocation tracking data' would be defined as 'personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time'.[109] However, including location data as a category of sensitive information was not recommended by the Attorney-General's Department.[110]

A critical question to resolve for broader Australian information privacy law, and as it applies to CAVs, is whether the relevant data (in this case, CAV data) falls into the categories of personal information or sensitive information under the *Privacy Act*. As noted above, if all of the information collected by, and in relation to, CAVs is not personal information, it may then fall outside the scope of the *Privacy Act*. It is clear that CAV technologies and the anticipated mode of operation of CAVs will test the practical effectiveness of the protections that have traditionally been provided to the Australian community by the *Privacy Act*.

Policy development for CAVs in Australia is spearheaded by the NTC. In 2018, the NTC released a discussion paper investigating the challenges and options to manage government access to C-ITS and automated vehicle data.[111] The NTC recommended a *GDPR*-type application of personal data to CAVs. However, in 2020, the NTC outlined a broader concept of 'vehicle generated data', moving away from a strict focus on the types of highly automated vehicles in its 2018 report, and examined the broader implications for the reform of information privacy legislation governing CAVs in Australia.[112] Consequently, the Australian policy consideration of what types of CAV-generated data should be classified as personal information is equally uncertain.

In Australia, without amendments to the *Privacy Act*, location data is currently likely to be too remote to, on its own, constitute personal information, although a different view is taken in Europe where

---

[107] Attorney-General's Privacy Act Review Report (n 10) 5.
[108] Ibid.
[109] Ibid.
[110] Ibid 46.
[111] NTC Automated Vehicle Data 2018 Discussion Paper (n 16).
[112] NTC Vehicle Generated Data 2020 Discussion Paper (n 16) 9.

such information will be treated as personal data. However, it is information of a kind that, when readily linked with other identifying data, can become both personal information and sensitive information (e.g., if it shows a person visiting a place of worship or a political association).[113] It is informative to draw upon statements by the United States Supreme Court in *United States v Jones* that location information '*generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.*'[114]

Relatedly, currently, only a limited number of collections, uses and disclosures of personal information require consent to be obtained under the *Privacy Act*,[115] but it is required for sensitive information.[116] Consent may be express or implied.[117] Relevantly, the Attorney General's Department proposed including new categories of consent (including voluntary, informed, current, specific and unambiguous).[118] However, the impact of the new categories of consent in the context of facial recognition or biometric technology where such consent may be inferred is not considered. This may be relevant for CAVs, which are anticipated to use these technologies. The data flows in the context of C-ITS and autonomous vehicle ('AV') technology are likely to be complex, and this presents challenges for obtaining genuine consent from individuals and dealing with data when the consent given is withdrawn.

B *The EU and US Context*

As outlined above, recent Australian law reform proposals about a new definition of personal information regard developments in other jurisdictions, most notably the EU and the US, in particular in relation to regulating location data. This presents an interesting starting point, given the different foundational bases for cultures of privacy in the EU compared to the US. While EU privacy laws are designed to protect human dignity and information self-determination,[119] the US model generally

[113] NTC Automated Vehicle Data 2018 Discussion Paper (n 16) 3.
[114] 132 S.Ct. 945, 955 (2012) citing *People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009).
[115] See, eg, under APP 6.1, APP entities may disclose personal information for the particular purpose for which it is collected (without consent) or a secondary purpose if an exception applies.
[116] *Privacy Act* (n 72) sch 1, APP 3.3, 3.4. See also at cl 3.6(a) which permits agencies to collect personal information indirectly on the basis of consent.
[117] Ibid s 6.
[118] Attorney-General's Privacy Act Review Report (n 10) proposal 11.1.
[119] *Charter of Fundamental Rights of the European Union* [2000] OJ C364/1, art 8.

protects freedom from incursion by the State within the sanctity of an individual's home.[120] Each point is addressed below.

C *European Union Information Privacy Law*

1 *Legislative Background to the GDPR*

1. Individuals in the EU reap the protection and benefits of an explicit right to informational privacy under Article 8 of the *European Convention on Human Rights* ('*ECHR*').[121] The *Charter of Fundamental Rights of the European Union* ('*EU Charter*') explicitly refers to the protection of personal data.[122]

2. The *GDPR*'s rights-based approach was explicitly preferred by the EU to a risks-based approach.[123] During negotiations of the *GDPR*, the Data Protection Working Party 29 ('WP29') indicated this preference: 'rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved'.[124] According to WP29, although a risks-based approach is evident in certain compliance requirements, the *GDPR*'s fundamental framework takes a rights-based approach.[125] *GDPR* regulatory bodies have maintained this position. For example, the European Data Protection Supervisor ('EDPS'), in their recommendations concerning the text of the *GDPR*, emphasised that 'the starting point is the dignity of the individual which transcends questions of mere legal compliance'.[126] More recently, the

---

[120] James Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113(6) *The Yale Law Journal* 1151.

[121] Article 8 of the *European Convention of Human Rights* ('*ECHR*') provides that 'everyone has the right to respect for [their] private and family life, his home and his correspondence': *European Convention of Human Rights*, signed 4 November 1950 213 UNTS 221 (entered into force 3 September 1953); Christopher Alexander, 'The General Data Protection Regulation and California Consumer Privacy Act: The Economic Impact and Future of Data Privacy Regulations' (2020) 32(2) *Loyola Consumer Law Review* 211.

[122] *Charter of Fundamental Rights of the European Union* (n 119).

[123] Article 29 Data Protection Working Party, *Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks* (Report, 14/EN WP 218, 30 May 2014) 2. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>.

[124] Ibid 3.

[125] Ibid 1–3.

[126] Giovanni Buttarelli, 'Europe's Big Opportunity: EDPS Recommendations on the EU's Options for Data Protection Reform, Opinion 3/2015' (9 October 2015) 5 (1) <https://edps.europa.eu/sites/default/files/publication/15-10-09_gdpr_with_addendum_en.pdf>.

European Data Protection Board ('EDPB')'s guidelines confirm that a risks-based approach is limited to a few articles only.[127] That being said, more recently, there has been some reconsideration of a risks-based approach under the *GDPR* in the context of artificial intelligence.[128]

3. The success of the *GDPR* in the EU can be tied to its reliance on a legislative mandate enjoining member countries in a prescriptive solution and homogenised legislation to ensure similar treatment of breaches regardless of where they occur.[129] The tight coupling of Member States enables a strong legislative response, which in turn facilitates a rights-based approach. The EU's composition of Member States, procedures and powers also allows it to implement a generalised (as opposed to sector-based) approach to privacy regulation. As the majority of the EU's legislation is enacted by the European Parliament with the Council of the EU (with representation from 28 Member States), it is designed to address broad issues conferred by treaties that member countries cannot sufficiently regulate themselves.[130] This includes the *GDPR,* which was enacted by the European Parliament and the Council of the EU.[131]

2 *Regulation of Personal Data*

Article 4(1) of the *GDPR* defines 'personal data' as any information 'relating to' an identified or identifiable person and provides a list of non-exhaustive identifiers.[132] Identifying factors are broadly defined and can be made directly or indirectly. 'Personal data' specifically includes location data (as well as other factors, including online identifiers or reference to a name or physical, genetic, social or economic identifiers).[133] The *GDPR* applies to data processing companies with establishments in the EU and

---

[127] European Data Protection Board, *Guidelines on Article 29 Data Protection by Design and by Default* (Guideline 4/2019, 13 November 2019) 7 (15).

[128] See Panel for the Future of Science and Technology, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (Study, PE 641.530, June 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf>.

[129] 'Two Approaches to Privacy – GDPR & CBPR', *Internet Commerce Australia* (Web Page, 24 July 2017) <http://www.inca.com.au/news/blog/two-approaches-to-privacy-gdpr-cbpr.html>.

[130] European Parliament Liaison Office in Washington DC, 'Composition, Powers and Functions' *European Parliament* (Web Page) <https://www.europarl.europa.eu/unitedstates/en/about-the-european-union-and-parliament/composition-powers-and-functions>.

[131] *Regulation (EU) 2016/679 of the European Parliament and of the Council* [2016] OJ L 119/1.

[132] *GDPR* (n 12) art 4(1).

[133] Ibid.

companies outside the EU where the processing activities relate to goods or services offered to individuals in the EU and monitor the behaviour of individuals in the EU.[134] Accordingly, the *GDPR* will apply to CAV companies (that may be both located inside and outside the EU) given that these vehicles will collect, process and share 'personal data'.

While location data is not defined in the *GDPR*, it is informative to have regard to the definition of 'location data' provided for in *The Privacy and Electronic Communications (EC Directive) Regulations 2003*:[135]

> any data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to—
>
> (f) the latitude, longitude or altitude of the terminal equipment;
>
> (g) the direction of travel of the user; or
>
> (h) the time the location information was recorded[136]

Further, location data may only be collected and processed for one of the six lawful bases identified in Article 6(1) of the *GDPR*. These include consent, performance of a contract to which the data subject is a party, compliance with a legal obligation, to protect the vital interests of the data subject or another natural person, to perform a task carried out in the public interest or exercise of official authority, or if processing is necessary for the legitimate interests of the controller or third party (except if the interests are overridden by the interests or rights or freedoms of the data subject, in particular concerning children). If consent is relied upon as the basis to obtain location data, presumably as CAV technology develops, every development and different use of CAV location data may arguably require a separate notice to receive consent.[137]

---

[134] *GDPR* (n 12) r 23.
[135] (UK) SI 2001/3495.
[136] Ibid r 2(1) (definition of 'location data').
[137] Erion Murati and Manjola Henkoja, 'Location Data Privacy on MAAS Under GDPR' (2019) 2 *European Journal of Privacy Law & Technologies* 131.

The *GDPR* also introduces 'the right to erasure'[138] and 'the right to object'[139]. Equivalent rights for data subjects to object to data processing or to seek erasure of personal data are not currently provided for under the *Privacy Act* in Australia. Proposals 18.2 and 18.3 of the Privacy Review Report set out a recommendation to introduce these as new rights,[140] and proposal 11.3 is for the ability to withdraw consent to be expressly recognised.[141]

In addition to the *GDPR*, the Directive 2002/58/EC on Privacy and Electronic Communications (as amended) ('E-privacy Directive')[142] will impact the collection and use of personal data, including location data, by entities in the CAV ecosystem. These directives establish that personal information should be used fairly and lawfully and in a relevant manner, not excessively and for a specified purpose. Personal data should be limited to a strict minimum.[143]

The EDPB adopted Guidelines 1/2020 on 9 March 2021 on processing personal data in the context of connected vehicles and mobility-related applications ('Guidelines').[144] The Guidelines focus on personal data in the context of non-professional use of CAVs, such as personal data processed inside the vehicle, exchanged between the vehicle and personal devices (such as smartphones), collected locally within the vehicle and exported to external third entities (such as vehicle manufacturers or insurers).[145] Falling within the scope of the Guidelines will be GPS navigation systems. However, applications that use location data to, for example, recommend other businesses (such as restaurants and location attractions) will fall outside the scope of the Guidelines.

The Guidelines specifically address concerns that the location technologies used by CAVs are a type of data requiring special attention as they raise the risk of surveillance of individuals which would impact personal data. The EDPB notes that most of the data generated by a CAV will constitute personal data, being information that is identified or identifiable about a person.[146] Focussing on location data, the

---

[138] GDPR (n 12) art 17.
[139] Ibid art 21.
[140] Attorney-General's Privacy Act Review Report (n 10) 11.
[141] Ibid 8.
[142] *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 *('E-privacy Directive')*.
[143] Ibid art 30.
[144] European Data Protection Board, *Guidelines on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications* (Guideline 1/2020, 28 January 2020).
[145] Ibid 8 [1.3].
[146] Ibid 7 [1.3.28].

Guidelines give the example that there is a risk that details of journeys made or vehicle uses could be connected with a person.

Accordingly, the Guidelines recommend that CAV stakeholders be particularly vigilant in not collecting location data without a necessary purpose for doing so.[147] The Guidelines also give an example of the processing involved in the vehicle's movement. The Guidelines suggest that the gyroscope is adequate to complete the function of detecting a CAV's motion without the collection of location data.[148]

Finally, the Guidelines set forward principles in relation to collecting location data. The EDPB's guidance is that the activation of geolocation data should not occur by default, even if the user has provided consent, or be continuously processed while the CAV is in operation. Instead, the EDPB recommends that geolocation data should only be activated if a function of the CAV requires it for operation, and even then, the user should have the option to deactivate it at any time.

3 *Sector-Specific Regulation of CAV Data in the EU*

Although the *GDPR* creates broad, wide-ranging privacy protections and rights that apply to CAVs, a trend has emerged in countries within the EU with a strong interest in establishing CAV-specific legislation to address their legal issues. These stand-alone sector-specific regulations also cover data and, in turn, have privacy implications relating to CAVs.

In Germany, since 2017, revisions have been introduced to the *Road Traffic Act* (Strassenverkehrsgesetz, StVG)[149] to first enable cars with automated driving systems (up to SAE level 3) to be driven on public roads. The initial legal framework required that these vehicles must be equipped with a black box to help allocate fault and liability in the event of an accident (similar to an aircraft black box).

In the absence of EU or international legislation, on 28 July 2021, further amendments were introduced to the German *Road Traffic Act* and the German *Compulsory Insurance Act—Autonomous Driving Act*.[150] These establish a legal regime for CAVs up to SAE level 4 on public roads in defined areas.

---

[147] Ibid 12 [2.1.1.60].

[148] Ibid 13 [2.1.3.64].

[149] *Strassenverkehrsgesetz* [Road Traffic Act] (Germany) 29 December 2022, BGBI I, 2022, 2606 ('StVG').

[150] Act amending the Road Traffic Act and the Compulsory Insurance Act–Act on Autonomous Driving, BGBl. 2021 I, 3108 ff. Regulated in section 1d–l Road Traffic Act; for the classification as level 4, cf. *Bundesregierung*,

There are broad obligations on the registered vehicle keeper regarding the collection, storage and transmission of data resulting from CAVs. The amendments require the registered vehicle keeper to save extensive data about the vehicle, including position data, activation and deactivation of autonomous functions, operational data (such as speed, acceleration and direction), system monitoring data, vehicle identification number and commands.[151] The vehicle keeper is also required, to the extent necessary, to transmit certain information and data externally to the Federal Motor Transport Authority and other authorities upon request, who may use it for monitoring the CAV. Further, if the CAV data is appropriately depersonalised, these entities may use the data for research into traffic and road accidents or purposes related to traffic-related public interest.[152]

In turn, obligations exist on the vehicle manufacturer to inform the vehicle keeper about the privacy settings and data processing by the CAV in a way that is precise, clear and in plain language, enabling the vehicle keeper to make appropriate changes to the settings.[153] In creating these obligations, the StVG, in part, captures the principles of privacy-by-design and privacy-by-default under the *GDPR* but in the CAV-specific context. Where the legislation is silent is in relation to the manufacturer's access and use of the CAV information.

Further, the *Automated and Electric Vehicles Act 2018* (UK), enacted by the United Kingdom to address liability and insurance issues related to CAVs, exemplifies government strategies to enact reformist legislation which specifically responds to CAV risks. On 25 April 2022, a new section in the Highway Code entitled 'Self-driving vehicles' was proposed before both Houses of Parliament. This amendment will enable the driver to hand over control of the driving task to the vehicle and divert their attention to other tasks (for instance, infotainment).[154] However, humans must be ready and able to take back control safely if a warning is given by the vehicle.[155] The Department for Transport recognised that

---

Draft of an Act to amend the Road Traffic Act and the Compulsory Insurance Act–Act on Autonomous Driving, BT-Drs. 19/27439, 9.3.2021, 15 f.

[151] Ibid s 1g(1).

[152] Ibid s 1g(5)–(6).

[153] Ibid s 1g(3).

[154] 'Rules on the Safe Use of Automated Vehicles: Summary of Responses and Government Response', *Department for Transport* (UK) (Web Page, 25 April 2022) <https://www.gov.uk/government/consultations/safe-use-rules-for-automated-vehicles-av/outcome/rules-on-the-safe-use-of-automated-vehicles-summary-of-responses-and-government-response#draft-amendment-to-the-highway-code--a-new-section-for-self-driving-vehicles>.

[155] Ibid.

the new section is required 'to clearly articulate the expectations for users of vehicles with automated, or self-driving, capability'.[156]

D *California Consumer Privacy Act 2018*

1 *Legislative Background to US Privacy Law*

US data protection laws take a different approach to the *GDPR* and Australian *Privacy Act* by instead implementing sector-specific privacy and data protection regulations and state-based legislation.[157] The differences between the US and EU approaches tie back to the historical development of the relevant privacy models. As noted, in the US, the government is typically taken to be the potential source of invasion of privacy, whereas in the EU, the government is regarded as the guardian of privacy.[158]

The sectoral approach in the US is typically considered to be a more 'laissez-faire' approach to privacy, with different levels of protection applying to various economic sectors through specific legislation in a way that is not universally applicable (or even co-ordinated). By way of example, stand-alone privacy statutes exist in industries that cover healthcare,[159] education, financial services[160] and communications.[161] Separately, the regulation may impose privacy obligations on specific types of data, such as the online collection of personal information in relation to children[162] or the use of video rental information.[163]

A number of industries may not be specifically regulated by privacy statutes at all at a federal level (although state-based legislation such as the *CCPA* may apply). As a result, the US legal framework governing data protection consists of a patchwork of state and federal statutes, regulations, binding guidelines and court rulings, and the legislation often permits entities to contract out of their privacy obligations.[164] There currently exists no national framework that regulates public and private sector privacy

---

[156] Ibid.

[157] Burdon (n 74) 152–53.

[158] Lisa Zivkovic, 'Reconciling the European and American Approaches to Privacy Law: A Historical and Legal Analysis of Privacy Law and Data Communications Technology in the United States and Europe, 1970 – 2018' (PhD Thesis, New York University, 2018) 228.

[159] *Health Insurance Portability and Accountability Act of 1996* 45 C.F.R. §§ 160, 162, 164 (1996).

[160] *Financial Services Modernization Act of 1999* 15 U.S.C. §§ 6801–6809 (1999).

[161] *Electronic Communications Privacy Act of 1986* 18 U.S.C. § 2510 (1986).

[162] *Children's Online Privacy Protection Act of 1998* 15 U.S.C. § 6501–6506 (1998).

[163] *Video Privacy Protection Act of 1988* 18 U.S.C. § 2710 (1988).

[164] Carol Li 'A Repeated Call for Omnibus Federal Cybersecurity Law' (2019) 94(5) *Notre Dame Law Review* I.

obligations in the US. As a consequence, in the US, there is no official national regulator overseeing the enforcement of privacy protections.

The US example can be compared to the Information Commissioner's Office in the UK, which is an independent authority tasked with enforcing compliance with the *GDPR*,[165] or the Australian Information Commissioner in Australia.[166] However, several federal laws in the US create privacy protections, and both state and federal regulations exist that serve to protect personal data. At a federal level, the *Federal Trade Commission Act of 1914*[167] provides protection against unfair privacy and data security practices under the umbrella of general unfair or deceptive trade practices.[168] Consequently, the Federal Trade Commission is commonly viewed as the de facto privacy and data protection authority.[169] Further, the USA Attorney-General and state Attorney-Generals are imbued with powers to enforce privacy statutes, such as civil actions under the *Health Information Privacy and Security Rules*.[170] As an additional overlay, led by the introduction of the *CCPA*, a number of US states have introduced comprehensive privacy statutes or proposed bills to do so (although variances between the states exist).[171] Further, sectoral approaches to regulating privacy continue to exist between different states. For example, in 2021, seven states passed legislation introducing privacy protections regarding consumer genetic information. This includes California, where a comprehensive privacy regime under the *CCPA* exists.[172]

---

[165] 'About the ICO', *Information Commissioner's Office* (Web Page, 2022) <https://ico.org.uk/about-the-ico/>.
[166] 'About Us', *Office of the Australian Information Commissioner* (Web Page, 2022) <https://www.oaic.gov.au/about-us>.
[167] 15 U.S.C. §§ 41–58 (1914).
[168] Daniel Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114 *Columbia Law Review* 583, 585.
[169] Steven Hetcher, 'The De Facto Federal Privacy Commission' (2000) 19(1) *J Marshall Journal of Computer & Information Law* 109, 131.
[170] *American Recovery and Reinvestment Act of 2009*, Pub L No 111-5 title XIII ('*The Health Information Technology for Clinical and Economic Health (HITECH) Act*').
[171] '2021 Consumer Data Privacy Legislation', *National Conference of State Legislatures* (Web Page, 27 December 2021).
<https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx>
[172] Ibid.

Against this backdrop of a multifaceted legal response to privacy, the function of the sectoral approach in the US has been called into question.[173] High-profile individuals[174] and companies[175] have sought the enactment of a comprehensive or omnibus privacy law in the US that would harmonise regulation of the private sector[176] on the basis that uniform standards would create certainty and potentially minimise international conflicts in privacy regulation.[177] Further, the introduction of the *GDPR* and its increasing adoption as the international standard has highlighted the divergence between the EU system and the US system of privacy law.[178] The movement to introduce a comprehensive regime in the US at a federal level calls into question complex issues about the different underpinning foundational approaches and their impact on existing rules and regulations.[179] In response to these complex matters, the American Law Institute ('ALI') developed a project aimed at guiding the development of US data privacy law, titled the 'Principles of Law, Data Privacy ('Principles'). Writing on the Principles, two of America's most prominent privacy scholars, Solove and Schwartz (2022)[180] (Reporters on the Principles), contend that it is possible to bridge the gap between the US and EU data privacy law. They propose that the starting point is to revitalise the application of the Fair Information Practice Principles (FIPPs) in US privacy law, as set out in the Principles, rather than to abandon them in favour of a completely new regime (noting that the *GDPR* includes regulations founded on the FIPPs principles).[181] Solov and Schwartz acknowledge the strength and utility of the *GDPR* but assert that seeking to transpose the *GDPR* into US law simply would be impractical due to the tension it would introduce with existing laws and incompatibility with core privacy values in US law and the First Amendment. However, Solov and Schwartz advocate for

---

[173] See, eg, 'U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Federal Privacy Law', *United States Chamber of Commerce* (Web Page, 13 February 2019) <https://www.uschamber.com/technology/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law>.

[174] See, eg, Bill Gates has advocated for a comprehensive federal privacy law: Anne Broache, 'Gates Urges Federal Data Privacy Law', *ZDNET* (Web Page, 7 March 2007) <https://www.zdnet.com/article/gates-urges-federal-data-privacy-law/>.

[175] Nicole Lindsey, 'Top CEOs Now Pushing for Federal Privacy Legislation' *CPO Magazine* (Web Page, 23 September 2019) <Top CEOs Now Pushing For Federal Privacy Legislation - CPO Magazine>.

[176] Paul Schwartz, 'Pre-emption and Privacy' (2009) 118 *The Yale Law Journal* 902, 904.

[177] Ibid. These states included Arizona (2021 AZ H 2069), California (CA A.B. 825) and (CA S.B. 41), Florida (FL H 833 (2021)), Maryland (MD H.B. 240), (MD S.B. 187), Montana (MT H.B. 602), South Dakota (SD S.B. 178), and Utah (UT S.B. 227).

[178] Daniel Solove and Paul Schwartz, 'ALI Data Privacy: Overview and Black Letter Text' (2022) 68 *UCLA Law Review* 1252, 1258.

[179] Ibid 1257.

[180] Ibid.

[181] Ibid 1263.

incorporating certain key aspects of the *GDPR*, modified to fit the US system, in a way that provides flexibility for future change that will significantly advance US privacy law.[182] An important initial step change reflected in the Principles is to adopt the privacy terminology used in the *GDPR* (and across privacy regimes around the world) in the US. The Principles propose adopting key *GDPR* terminology, such as data subjects, data controllers and data processors.[183] Although similar concepts already exist, at least in part, in US privacy regulation, there currently exists a lack of consistent terminology, internal divergence and gaps in the relevant statutes. For example, the definitions typically used in US legislation are 'personal information' or 'personally identifiable information'.[184] Introducing a concept of personal data that aligns with the *GDPR* approach to include an identified or identifiable individual[185] and is uniform in US privacy statutes and regulations (where currently different approaches apply across various statutes) is advocated as an important underlying reform principle.[186]

A significant change has recently been proposed in the US. On 20 July 2022, the House Committee on Energy and Commerce approved the *American Data Privacy and Protection Act* ('*ADPPA*'),[187] which will now move to a vote in the full House of Representatives and, if passed, to the Senate. The *ADPPA* represents a potential landmark step change in federal privacy regulations in the US. The *ADPPA* would apply to 'covered entities', being those subject to the *Federal Trade Commission Act* (but not including governmental entities), and therefore be enforced by the Federal Trade Commission and state Attorney-Generals.[188] It would provide privacy protections to consumers in relation to 'covered data'. Covered data is defined as information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device but is subject to specified exclusions such as de-identified data, employee data or publicly available data.[189] Relevantly for CAVs, additional privacy protections would apply to 'sensitive covered data' and explicitly capture past or present

[182] Ibid 1260–1261.
[183] Ibid 1266.
[184] Paul Schwartz and Daniel Solove, 'Reconciling Personal Information in the United States and European Union' (2014) 102(4) *California Law Review* 887, 889.
[185] Ibid.
[186] Solove and Schwartz (n 178) 1267.
[187] *American Data Privacy and Protection Act,* HR 8152, 117th Congress (2022).
[188] Ibid § 2(9).
[189] Ibid § 2(8).

precise geolocation data.[190] While there has been some bipartisan support in favour of the *ADPPA,*[191] there remain a number of significant hurdles and issues that need to be resolved before a federal US privacy bill can be considered a potential reality. A key issue to resolve will be the application of exemptions to pre-emption and whether state-based comprehensive privacy statutes, such as the *CCPA* (discussed further below), will continue to take precedence.

2 *Regulation of Personal Data*

At a state level, California has introduced the *CCPA*, which was recently amended by the *California Privacy Rights Act of 2020* ('*CPRA*').[192] The *CCPA* sets a new benchmark in privacy protection in the US, with several states following (or planning to follow) with their own legislation (although there may be varying degrees of similarities or differences).[193]

Relevantly for the CAV space, the *CCPA* includes 'geolocation data' within the definition of 'personal information' as well as inferences drawn from this data about a consumer. Accordingly, geolocation data under the *CCPA* will also fall under the purview of the notice and transparency requirements and rights of access, deletion and opt-out held by consumers. Further, the *CCPA* defines 'sensitive personal information' to include a consumer's 'precise geolocation data',[194] which is further defined to mean 'any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations'.[195]

---

[190] Ibid § 2(24).

[191] 'The American Data Privacy and Protection Act', *American Bar Association* (Web Page, 30 August 2022) <https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl/>.

[192] *California Privacy Rights Act of 2020–Proposition 24* as passed by ballot on 3 November 2020 <https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf>.

[193] Gary Kibel and Justin Lee, 'States Proposing Their Own CCPA-Like Privacy Laws', *JDSUPRA* (Web Page, 13 February 2020) <https://www.jdsupra.com/legalnews/states-are-proposing-their-own-ccpa-55449/#:~:text=CCPA%20was%20just%20the%20tipping%20point%20of%20comprehensive,there%20have%20been%20further%20developments%20in%20New%20York>.

[194] *CCPA* (n 15) § 1798.140(ae).

[195] Ibid § 1798.140(w).

The *CCPA* applies to businesses with gross annual revenue over $25,000,000, or that alone or in combination receive, sell or share the personal information of over 100,000 consumers.[196] Accordingly, the *CCPA* will likely apply to most automotive companies within California as they are anticipated to meet these statutory thresholds. The territorial reach of the *CCPA* applies to organisations that do 'business in the State of California'.[197] Accordingly, a business based outside the State (even in another country) could be caught by the *CCPA* if they are nevertheless doing business within the State. An exception to this is that the data must pertain to California residents. Therefore, if personal information about a California resident is not collected, it will fall outside the scope of the *CCPA*. The importance of the *CCPA* is that, much like the *GDPR*, it is becoming a de-facto standard of privacy regulation within major US cities[198] and to which international regulators have regard.

As noted, the *CPRA* amended the *CCPA* commencing on 1 January 2023. Under the *CCPA*, as amended, consumers are given more control over how their sensitive personal information (which includes precise geolocation data) is collected, used and disclosed by having the ability to request limits on its use and disclosure.[199] According to the amendments to the *California Consumer Privacy Act Regulations* ('*CCPA Regulations*'),[200] there is a narrow set of purposes for which a business may use or disclose sensitive personal information without giving consumers a right to limit the data. By way of example, the *CCPA Regulations* provide that a consumer's precise geolocation data may be used by a mobile application that provides consumers with directions to a specific location. However, this precise geolocation information could not be used by a gaming application, given that the average consumer would not expect this application to require precise geolocation information.[201]

Further, a business' collection, use, retention or sharing of a consumer's personal information must be reasonably necessary and proportionate to the purpose for which it was collected or processed.[202]

---

[196] Ibid § 1798.140.
[197] Ibid § 1798.140(d).
[198] For example, comprehensive consumer data privacy laws also exist in Colorado *(Colorado Privacy Act, Pub L No 21-190, Stat § 6-1-1301 (2021))*, Connecticut (*An act concerning personal data privacy and online monitoring,* S Res 6 (2022)), Utah *(Consumer Privacy Act, S Res 227 (2022))*, Virginia *(Consumer Data Protection Act S Res 1392 (2022))*.
[199] *California Consumer Privacy Act Regulations,* 11 Cal Reg Code §§ 7000–7304 (Barclays, 2023) *('CCPA Regulations')* amending *California Consumer Privacy Act Regulations of 2020* 11 Cal Reg Code §§ 7000–7304 (Barclays, 2020).
[200] Ibid.
[201] Ibid reg 7027(m)(1).
[202] Ibid reg 7002(a)(1).

The *CCPA Regulations* also specify that it is manipulative to bundle choices when requesting consent so as to subvert the consumer's choice. It gives the example of a location-based mobile service not being entitled to bundle other consent for other uses of the consumer's geolocation data.[203]

The *CCPA* also introduces several obligations on companies, such as enabling residents to opt out of the sale of personal information, allowing minors aged between 13 and 16 to opt in and requiring parental consent for children under 13 years old.[204] Given that an anticipated benefit of CAVs is to expand the type and kind of passengers,[205] potentially enabling minors to travel unaccompanied (and others who would not currently hold a licence), an automated driving system entity ('ADSE') will likely be faced with the challenge of how to obtain the relevant consent.

3 *Sector-Specific Regulation of CAV Data in the US*

The hybrid nature of regulation in the US exists in relation to CAVs with the existing or planned sector-specific regulation. In addition to the overarching privacy obligations under the *CCPA*, California has introduced state-based regulations about the deployment of autonomous vehicles on public roads in California.[206] Specifically, section 228.24 of the *California AV Regulations* requires manufacturers of autonomous vehicles to provide written disclosure to passengers of the CAV describing the personal information collected by the CAV that is not necessary for the safe operation of the vehicle and how it will be used. Data that is not used for the safe operation of a vehicle must be anonymised by the manufacturer. If a CAV is sold or leased to a customer, equivalent written approval must be collected by the registered owner or lessee of an autonomous vehicle.

It is anticipated that future regulatory advances in the US in the context of CAVs will adopt the trend of introducing targeted, industry-specific legislation instead of relying on a general, principles-based privacy law. At a federal level, legislation to regulate CAVs, such as the *Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act of 2017* ('*SELF DRIVE Act*'),[207] have been put forward in the US

---

[203] Ibid reg 7004(a)(4)(B).
[204] *CCPA* (n 15) 1798.120(c).
[205] Compared to vehicles currently in public use.
[206] 'California Autonomous Vehicle Regulations–Article 3.7 Testing of Autonomous Vehicles', *State of California Department of Motor Vehicles* (Web Page, 13 April 2022) <https://www.dmv.ca.gov/portal/file/adopted-regulatory-text-pdf/> *('California AV Regulations')*.
[207] Pub L No 115-294, 163 Stat 6667. A separate bill, the *American Vison for Safer Transportation Through Advancement of Revolutionary Technologies Act of 2017* Pub L No 115-187, 163 Stat 7360 *('AV START Act')* was reported from a Senate Committee.

but have failed to be enacted. Data ownership and consumer privacy are identified gaps in the US regulatory landscape, with no current laws in existence to prevent vehicle manufacturers and software providers from reselling information obtained about vehicle users (or drivers).[208] With the renewed focus on the introduction of a comprehensive federal privacy regime in the US while continuing to pursue separate sector-specific regulation for CAVs, it suggests that a hybrid approach may still, in part, be pursued. If so, careful consideration of the cohesion between the various pieces of legislation and those existing under state laws would need to occur.

IV COMPARATIVE ANALYSIS OF INFORMATION PRIVACY LAW

Current law reform considerations about changing the definition of personal information represent important developments in Australian information privacy law.

The scope of the reform in Australia is in part complicated by the fact that while international regimes such as the *GDPR* and *CCPA* have similarities in terms of how they regulate location data, there are several areas where they do not intersect. For example, a key difference arises between who is regulated by the legislation. The *CCPA* applies to for-profit businesses within the geographical limit of California. In contrast, the *GDPR* has a broader territorial scope, capturing organisations outside the EU with data processing activities that offer goods or services to data subjects situated within the EU or monitor the behaviour of those subjects. Further, the *GDPR* applies more broadly to data controllers, which may be any private or public entity (for-profit or not-for-profit) and natural or legal persons, regardless of size.

Given that Australia is not anticipated to be a manufacturer of CAVs but rather an importer, it is important that any regulation is in step with international approaches and that Australia does not introduce regulations that could create a barrier to the entry and deployment of CAVs in the Australian market. In this author's view, the appropriate first step is to define 'personal information' in Australian information privacy law to recognise location data as a factor by which a person may be identified (directly or indirectly). The recent proposals by the Attorney-General's Department in this respect are a welcome step change. Location data has demonstrably crossed the threshold to qualify as personal information

[208] For example, this is an identified gap in the Alliance for Automotive Innovation, 'Privacy Principles for Vehicle Technologies and Services', *Consumer Privacy Protection Principles* (Web Page, 12 November 2014) <https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf>.

and, therefore, ought to be subject to similar protections that exist in the *GDPR*, some of which are not currently present within Australian information privacy law. As a starting proposition, it remains important that location data is only used for its primary purpose and a restriction on the secondary use of the data exists, such as the offering of other services or advertisements, without notice and consent being sought from the CAV subject, such as exists under *GDPR* article 5. Australian information privacy law should introduce protections that ensure consumers or users of CAVs are provided with a readily understandable and meaningful notification of how their personal information is being collected, used and shared and to enhance the practice of informed consent. The Attorney-General's Department did not recommend expanding the circumstances in which consent must be obtained but strengthening other reforms regarding the handling of personal information.[209] Proposal 11.2 of the *Privacy Review Report* is for the OAIC to introduce guidance on the use of layouts, wording or icons when obtaining consent. Given that CAVs are anticipated to expand solo travel in vehicles to the elderly, young children and the sick,[210] this notice will need to be designed in a way that is readily digestible and age-appropriate. This context ought to be considered when formulating the relevant guidance.

It is generally accepted that in order for manufacturers and suppliers of CAVs to supply the services that will enhance CAV usage, they will need access to location data (along with other information about the vehicle). Relatedly, CAV users should also have the ability to decide which connected services to opt in to, update their preferences and unsubscribe to services over time.[211]

Further, the concrete data protections that exist under the *GDPR* to enshrine the principle of privacy by design (article 25) are appropriate to introduce into the *Privacy Act*. This inclusion would mean that manufacturers of CAVs and related software and technology developers need to build CAVs in a way that seeks to achieve data minimisation, including in relation to location data. Stakeholders would need to design systems to create physical and digital security, such as encrypting data and installing firewalls and authentication processes for a user to gain access to the CAV and related systems, particularly as regards CAV location data. The concepts of privacy-by-design and -default are not new, but mandating them

[209] Attorney-General's Privacy Act Review Report (n 10) 103.

[210] Ashley Halsey III, 'Driverless Cars Promise Far Greater Mobility for the Elderly and People with Disabilities', *The Washington Post* (online, 23 November 2017) <https://www.washingtonpost.com/local/trafficandcommuting/driverless-cars-promise-far-greater-mobility-for-the-elderly-and-people-with-disabilities/2017/11/23/6994469c-c4a3-11e7-84bc-5e285c7f4512_story.html>.

[211] See generally, *Privacy Act* (n 72) sch 1; *GDPR* (n 12).

under the law in the GDPR is a significant change.[212] That said, the practical application of a privacy-by-design framework still brings with it challenges and questions about its scope. By way of example, a strict application of principle two, 'privacy as the default', could require an opt-in protocol for every IT system, business practice, digital service, app, website, etc, that a user wanted to access. It is left unanswered as to whether explicit consent is required in each instance or if each relevant entity should be left to decide the data that is necessary for each specific purpose.[213]

Currently, location data is not treated as a special category of sensitive information under the *GDPR* unless combined with other data to identify sensitive information. Importantly, the *CPPA* introduces a new category of precise geolocation data. It is posited that including a similar new category of precise geolocation data in Australian information privacy law (under APP 3) would offer specific protections for this higher-risk category of data. Precise location data will be highly informative for a few stakeholders involved with CAVs, such as enabling traffic forecasting and manipulation of routes to avoid hazards. However, in doing so, it could identify a closely identified pattern of traffic for an individual, including other aspects of sensitive information such as attendance at a hospital or place of worship.

The comprehensive approach to regulating information privacy law adopted by the EU and OECD countries, such as Australia, remains favourable to establishing information privacy rights by individuals (including consumers of CAVs) and establishing obligations on organisations captured by the *Privacy Act*, regardless of industry or sector. Further, it is clear that even where currently higher standards of overarching privacy laws apply in the EU and California, additional sector-specific regulation of CAVs fills an important gap in CAV areas. Similarly, it is posited that an equivalent approach in Australia would ensure appropriate information privacy protections for CAV users. Doing so would retain the flexibility to amend CAV-specific regulations in step with technological developments more readily compared to making amendments to the *Privacy Act*.

Separate regulations that address CAV data would be appropriate to focus on the collection and storage of such data and any supplementary provisions for compliance by ADSE and the enforcement of

---

[212] Belinda Bennett, Jane Evelyn and Bridget Weir, 'Driving Into New Frontiers? Data and Driverless Cars' (2019) 8 *University of New South Wales Law Journal Forum* 1, 15. See also Attorney-General's Privacy Act Review Report (n 10) proposal 11.4 recommending that online privacy settings should reflect the privacy by default framework of the *Privacy Act* (n 72).

[213] Marja Boskovic Batarelo, 'Privacy as a Default Setting Under the GDPR', *Batarelo Dvojkovic Vuchetich Law Firm* (Web Page, 14 June 2018) <https://www.bdvlegal.com/privacy-as-a-default-setting-under-the-gdpr/?cookie-state-change=1582513558329>.

these actions. The overarching rights and rules regarding consumers regarding the subject of the location data are appropriate for continuing to be regulated at a high level under the *Privacy Act*. The sheer depth and breadth of the location data generated by CAVs are staggering and unique in their volume. However, the type of data is not so exceptional that it wholly diverges from the information privacy challenges resulting from the increased use of other forms of automated transport or increased use of mobile phones and other Bluetooth and tracking devices.

Instead, supplementary CAV-specific legislation will be appropriate to develop, as is the case in the UK and Germany, and to do so in a way that does not detract from the *Privacy Act* but provides rights and remedies for specific issues that warrant addressing. For example, notice and consent regarding the collection of personal information associated with CAVs will be imperative to ensure that proper safeguards are in place about how location information is gathered. Further, in the context of location data, stand-alone regulation of CAVs should address the question of whether CAVs should record location data and, if so, how it is to be dealt with (i.e., the time period it is stored for) and with whom it may be shared. It is believed that it will be necessary to record location data within the CAV to establish liability in the event of an accident or incident, and, in appropriate circumstances, it will be necessary to share the data with insurers and traffic enforcement bodies while remaining compatible with data protection principles.

V CONCLUSION

The definition of 'personal information' in the *Privacy Act* requires an amendment to address the risk of pervasive surveillance and collation of data tracking movement or behaviour that may be associated with the introduction of CAVs. Australia's privacy laws should be brought into line with more progressive laws, such as the *GDPR* and *CCPA*, to specifically recognise location data as being capable of personal information. Further, precise location data is highly sensitive and should be treated as such. The benefits that CAVs will derive from the collection, use, and sharing of location data are numerous and varied. However, as the value, complexity, quality and depth of location data increase, so do its vulnerabilities. Having a clear path to protect this data is anticipated to not only build trust amongst CAV users but also provide certainty for CAV manufacturers and stakeholders when developing the vehicles and the related operational systems.