AHRC: Human Rights And Technology Issues Paper

July 2018

Submission:

Connected Autonomous Vehicles: Privacy Considerations and Legal Implications

Martha Browning, Megan Ellis and Kelly Yeoh

Submission prepared as part of Juris Doctor studies at Flinders University with

Tania Leiman

JD Topic Coordinator, Flinders University

1 October 2018

Introduction

Some estimates suggest connected autonomous vehicles (CAVs) will be in use on our roads by mid-2020s. Australian Transport Ministers have tasked the National Transport Commission to ensure an end-to-end regulatory framework is in place by 2020. CAVs offer potential benefits in terms of increased safety (more than 90% of road traffic crashes currently are caused by human error), and by increasing access to mobility for those who currently cannot use motor vehicles independently. They also offer additional social, economic and environmental benefits to the community.[1] Various Mobility as a Service (MaaS) offerings already exist (e.g. ride-sharing), with introduction of CAVs likely to grow these further. MaaS provides 'travelers with access to the full mobility ecosystem'[2] as well as 'personalised mobility solutions that make use of this wide range of mobility options'.[3] MaaS users access an online application for 'end-to-end trip planning, booking, electronic ticketing, and payment services across all modes of transportation, public or private.'[4]

CAVs also raise new concerns regarding privacy, confidentiality and use of data. CAVs and Connected Intelligent Transport systems (C-ITS) will generate, collect, store, access and use information about vehicle operation, route, infrastructure, CAV users, and potentially also other road users or those in the vicinity of those vehicles. CAVs will connect with other vehicles (V2V), with pedestrians (V2P), with businesses (V2B – particularly in the context of MaaS offerings) and with infrastructure and other connected devices (V2X). The digital footprint left by individuals using CAVs has the potential to reveal significant information about them including their interests, purchasing habits, online search history, health conditions, employment, political or

[1] Australian Driverless Vehicle Initiative, Driverless car benefits (2018) ADVI <https://advi.org.au/driverless-technology/driverless-car-benefits/>.
[2] MaaS Australia, *MaaS Australia* <http://maasaustralia.com/>.
[3] Ibid.
[4] Warwick Goodall et al, 'The rise of mobility as a service: Reshaping how urbanites get around' (2018) 20 *Deloitte Review* 111, 114.

religious associations. It may also include data generated by individuals outside the vehicles – pedestrians, bystanders or others whose data is accessed by C-ITS.

Even where the data comprising such footprint is de-identified or anonymized rapidly increasing computing capacity now allows for analysis of structured and unstructured big data, posing challenges to privacy that have not previously existed. This is particularly the case where vehicle users or others are at risk of adverse or discriminatory decisions or actions.

Location and route data may be used explicitly or implicitly to identify persons belonging to a particular minority group, or to denote or impute ethnicity, religious or cultural affiliations. Data demonstrating regular use of a vehicle to attend particular locations such as clinics, injecting rooms or brothels may indicate the vehicle user is at higher risk of serious health conditions such as HIV or other sexually transmitted disease. When aggregated with other information it may also impute sexual preference or gender identity, placing an individual at risk of discrimination on that basis. Monitoring CAV operation may be used to bully, harass, control or stalk individuals, including in the context of domestic violence.[5]

Other potential issues may include

1. Bias inherent in facial recognition software – for example law enforcement using recorded vehicle data to place a person in the vicinity of a crime, when in fact they were nowhere near the location but have essentially been racially profiled by a system that is unable to accurately tell the difference between persons of colour.[6]
2. Unauthorised access to location data of users (direct access to location data) and non-users (via facial recognition to develop a pattern of locations over time where the person has been seen by passing vehicles) for purposes such as stalking or casing for further crime such as robbery.

---

[5] Alison Branley and Rebecca Armitage, 'Perpetrators using drones to stalk victims in new age of technology fuelled harassment', ABC News 1 October 2018 http://www.abc.net.au/news/2018-10-01/drones-used-to-stalk-women-in-new-age-of-harassment/10297906

[6] Jieshu Wang, *What's in your face? Discrimination in Facial Recognition Technology* (2018, Georgetown University).

3. Hacking of CAVs to cause accidents or distractions, or to follow people or keep tabs on people, for example celebrities or high-profile people or their families.
4. Surveillance by employers, insurers etc to determine the whereabouts of their employees, or whether vehicle use was work related or not. and be used to blackmail or fire them. T

Whenever the benefits of increased connectivity are used to make online shopping purchases, use online ride-sharing or banking services, social media, gaming and telecommunications channels, personal information is disclosed in order to do so. This also expose users to risk of consequences such as spam, scams, identity theft and fraud. These benefits and risks are set to expand with the introduction of CAVs.

This submission will review the efficacy of privacy law and other protections existing under Australian Law. It will explore the potential application of the recent United Nations Office of the High Commissioner for Human Rights (OHCHR) '*A Human Rights-Based Approach To Data*' Guidance Note, to guide protection of the personal privacy of AV users, the broader public, and fundamental human rights. It will also consider the impact of European Union's recent *General Data Protection Regulation* (GDPR), one of the most comprehensive attempts to regulate entities who are dealing with personal information, and a sound basis to argue for increased protections in Australia.[7]

Despite concerns regarding the potential impact of data security risks on the community, there is much to be gained from the introduction of autonomous vehicles, and it is not the intention of these submissions to suggest otherwise. Likewise, the potential benefits of CAVs to society may be enormous, and the data generated, collected and analysed may also be very useful in demonstrating deficiencies in

[7] GDPR.

services for vulnerable people and in otherwsaie supporting equitable access to those benefits. It is important to be mindful of risk versus benefit.

The final report provided by the Australian Law Reform Commission, in their discussion of serious invasions of privacy in the digital era,[8] and the requirements for law reform, expressly stated that 'the law should make appropriate provisions for people with disability or others who require assistance in obtaining access to justice'[9] and that 'statutory cause of action or other remedy for serious invasions of privacy should be accessible to people with limited means as well as to those who can more easily afford the high costs of litigation'.[10] It is evident that this discussion is integral for the introduction of autonomous vehicles for those who are vulnerable to minimise the risks of discrimination.

Regulatory frameworks: AV data, privacy and human rights

The United Nations Office of the High Commissioner for Human Rights ("OHCHR") recently released its '*A Human Rights-Based Approach To Data*' Guidance Note, identifying 6 key principles set out below. [11] The latter four principles will have particular relevance to the data generated by AVs.

1. Participation of the relevant population groups in data collection, including ensuring marginalized groups are adequately represented;
2. Data disaggregation, requiring more comprehensive data collection, to allow in-depth analysis of groups, including those that are discriminated based on ethnicity, gender, age, disability, sexual orientation, religion and income;

[8] Australian Law Reform Commission, *Serious invasions of privacy in the digital era*, Final Report No. 123 (2014).
[9] Ibid 38.
[10] Ibid.
[11] Office of the High Commissioner, *A human rights-based approach to data,* UN Doc A/RES/70/1 (2018).

3. Self-identification, including the option for individuals to withhold or disclose information to respect and protect personal identity;
4. Transparency of all information collecting entities in relation to the data they are collecting to be available to the public;
5. Privacy of the individual should be maintained and confidentiality ensured;
6. Accountability of the collectors of information must be held accountable for upholding human rights.

Auto-manufacturing is no longer carried out in Australia. Australia imports many vehicles made by European–based manufacturers either in Europe or elsewhere. Data from Navya driverless shuttles currently being tested in Australia is transmitted directly to its French manufacturer in Europe.[12] All of this means that the European Union's recent *General Data Protection Regulation* ("GDPR"), in force as of 25 May 2018, must be considered in the context of CAV use in Australia. Countries conducting trade with the European Union must adhere to these robust regulations. The GDPR seeks to safeguard human rights in the context of technology and ensure protection of personal information. The GDPR harmonises privacy laws across Europe. It includes stringent aspects in relation to consent when collecting and using data, penalties for organisations or companies that breach the conditions of the regulations, breach notification requirements, a right to access and a right to be forgotten amongst other aspects.

There is no right to privacy at common law in Australia. Instead a patchwork of federal and state frameworks apply to provide some protection. The federal *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs) listed in Schedule 1 impose obligations on 'APP entities' in relation to collection storage, access and use of information. 'APP entities' do not include small business operators with an annual turnover of $3,000,000 or less or State or territory authorities. This may mean that

[12] for example as part of Finders University's current FLEX trial using a Navya shuttle.

where C-ITS providers are state or territory authorities, *Privacy Act* and APP protections are unlikely to apply. This could result in a patchwork of privacy protections across Australia, mirroring the patchwork of provisions regarding liability of road authorities in state and territory civil liability legislation. This would seem to be problematic given the national cross jurisdictional nature of road transport.

Personal information

The GDPR broadly defines 'personal data' as 'any information relating to an identified or identifiable person.'[13] The GDPR classifies identifiers such as IP addresses, location and pseudonymous data as personal information, as it can be used to identify a person despite the data not directly naming an individual.[14] The GDPR seeks to protect personal information by regulating against the collection of unnecessary data,[15] unforeseen use of data[16] and biased algorithmic decisions. By doing so, the GDPR highlights the extent to which an individual's digital footprint is now intrinsically linked to their right to privacy.

The focus of the APPs is on protection of 'personal information', that is, 'information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.'[17] 'This also includes 'sensitive information' (includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information)'.[18] Everyday examples of personal information may include a person's

[13] Ibid.
[14] Ibid art 4(1).
[15] Ibid art 51(e).
[16] Ibid art 13, 14.

[17] *Privacy Act 1988* (Cth) s.6

[18] https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information

name, signature, address, telephone number, date of birth, medical records, banking details and commentary or opinion about a person. However, according to Australian case law, 'personal information' does not include data, that when linked to other data, may identify an individual.[19] APP entities that hold personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.[20]

The Federal Court held in *Privacy Commissioner v Telstra Corporation*

> The concept of "personal information" to which an organisation must provide an individual with access is very broad. It encompasses untrue information which is not recorded in any material form. It is, however, constrained by the requirements that: (i) it must be held by the organisation; (ii) it must be "about" the individual who requested access; and (iii) it must be about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[21]

The Court went on to note that

> In other words, if an individual's request included information in Telstra's control which was stored across any of 13 databases held by Telstra (ts 18) then in determining whether the individual's "identity is apparent", or can reasonably be ascertained, from the information requested, it would be necessary to consider all of the information in totality.[22]

and

> The words "about an individual" direct attention to the need for the individual to be a subject matter of the information or opinion. This requirement might not be difficult to satisfy. Information and opinions can have multiple subject matters. Further, on the assumption that the information refers to the totality of the information requested, then even if a single piece of information is not "about an individual" it might be about the individual when combined with other information. However, in every case it is necessary to consider whether each item of personal information requested, individually or in combination with other items, is about an individual. This will require an evaluative conclusion, depending upon the facts of any individual case, just as a determination of whether the identity can reasonably be ascertained will require an evaluative conclusion.[23]

---

[19] *Re Telstra Corporation Limited and Privacy Commissioner* (2015) 254 IR 83.
[20] *APP* 11.1.

[21] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 at paragraph 60

[22] Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 at paragraph 61

[23] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 at paragraph 63

Data generated by use of CAVs may be personal information, sensitive information and/or may include information that can be used to impute personal information and sensitive information. Even if that data is de-identified or anonymized and thus on its own cannot reasonably identify an individual, when big data analytics is applied to that and other large data sets it may be possible to re-identify individuals in ways that have not previously been possible.

CAV data may include:

- GPS positioning data of the vehicle, location and route tracking;
- Sensor array and LiDAR data, tracking locations and behaviour of other vehicles and non-vehicle obstacles (such as persons) nearby, together forming the main functionality to determine safe movement and expected behaviour of surrounding vehicles and persons;
- Camera data, similar to dash cams, used like dash cams to capture video and/or still images for finer tracking and processing of events and details such as traffic light colours, traffic signs, lights on other vehicles (such as indicators or brakes) etc. These are able to give highly detailed environmental information of the area surrounding the vehicle;
- Forms of voice control/recording of interactions inside of the car;
- Bluetooth or similar connection to phones or other devices, as is reasonably standard in many recent vehicles, and any data accessible therein.
- Sensor data, video or still image recording of behaviour inside the vehicle (particularly in fleet services such as Uber, or in the event of gesture control of vehicle functions, as might be required for passengers with no vocal capability such as non-verbal autistic persons). [24]

Mass collection of this type of data, even if it does not contain direct links to a person, may be capable of creating these links. Data not considered to be "personal

[24] Cara Bloom et al, *Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles* (July 2017) Usenix < https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bloom>.

information" may be able to be used to generate personal information.25 Once data assumed not to be personal is collected, consideration must be given to ensuring that, where it is used at some later time to generate personal information, that latter information is protected.

The GDPR's definition of personal data includes information that can be used to generate personal data. For example, the collection of a person's IP address plus web behaviour can lead to detailed knowledge about that person, including places of work, hobbies, schools or day care attended by children, times and locations of events that they attend, and far more, that can in turn be used to extract sufficient information to accurately pinpoint the identity of a person, without any requirement to link elsewhere to form the connection. The GDPR requires that personal data is subject to multiple rights given the person to whom it pertains, which includes most notably the right to erasure of all content pertaining to that individual.

Data collection

OHCHR principle 3 provides that 'individuals should have the option to disclose or withhold information about their personal characteristics.'

It is likely that the GDPR will treat AV image data collection analogous to CCTV data. Under the GDPR, persons under surveillance hold several rights regarding any collected data, including the rights to be informed of its collection, have access to any data about them, to correct or erase it, and to object to or restrict its collection or use.[26] These rights include the right to not be subject to any automated processing or profiling that may affect rights and freedoms.[27] Specific requirements apply to collection of

[25] Arvind Narayanan and Vitaly Shmatikov, 'Myths and Fallacies of "Personally Identifiable Information"' (June 2010) 53(6) *Communications of the ACM*, 24.
[26] GDPR ch 3.
[27] Ibid art 22.

"special categories of data", such as facial recognition data.[28] Companies collecting CCTV footage must demonstrate a lawful basis for collection and processing of such data,[29] subject to notification requirements.[30] Data subjects maintain their rights to be able to restrict what can be done with captured data, or to have it erased.[31] Law enforcement may override these rights.

The APPs provide that personal information (other than sensitive information) must not be collected unless the information is reasonably necessary for (or in the case of agencies, directly related to one or more of the entity's functions or activities.[32] Collection of sensitive information requires the individual's consent. CCTV surveillance by a business is covered by the *Privacy Act,* or by State and Territory law if carried out by an individual.[33]

We already volunteer much data willingly via existing separate technologies.[34] However, given the array of sensors and data recording devices required to successfully and safely navigate traffic, and ongoing focus on improving safety, in future much of the data collected by CAVs may be unsolicited and relating to uninformed and unknowing individuals.[35] The implications of storing and linking such vast quantities of data pose new challenges.

Building on the discussion above regarding the Telstra case, a significant limitation of the definition of "personal information" (or "personal data" as it is referred to

---

[28] Ibid art 9.
[29] Ibid art 6.
[30] Ibid art 13.
[31] GDPR art 17-8.

[32] APP 3
[33] Office of the Australian Information Commissioner, *Surveillance and monitoring* (accessed 21 September 2018), Australian Government <https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/what-can-i-do-about-my-neighbour-s-security-camera#what-rules-apply-to-businesses-using-cctv>.
[34] For example: reverse parking sensors, dash cam and cctv, google home and amazon alexa, playstation and xbox gesture controlled games, typical car/phone Bluetooth interface, etc.
[35] Melanie E. Bates, FDF and NADA Launch Guide to Consumer Privacy in the Connected Car (25 January 2017), Future of Privacy Forum <https://fpf.org/2017/01/25/fpf-and-nada-launch-guide-to-consumer-privacy-in-the-connected-car/>.

within the GDPR) is that mass collection of data, that does not contain direct links to a person, has been found to be capable in many cases of creating these links. Or, to rephrase, data that is not considered to be "personal information" can be used to generate personal information.[36] Furthermore, once we have given access to this data that we assume not to be personal, the Act does not specify ways and means of policing what is done with it, to ensure that no such personal information is generated.

While CAVs users may be provided with information about, and required to consent to data collection at the time of purchasing, booking or using the CAV, they are not likely to behave differently to users of digital technology currently. Most people ignore terms and conditions,[37] simply clicking 'I accept' to gain access to the relevant application or website without delay. Most people using MaaS or a CAV are unlikely to bother reading more than a few lines before agreeing in order to get their ride underway. Privacy settings on mobile devices and their applications change regularly, and even those CAV users who choose the highest privacy settings may not understand that metadata from their device may still be collected, especially if they have not taken the time to read any terms and conditions of use very carefully. Despite many privacy policies being made available on company websites, this is unlikely to demonstrate sufficient steps to making the policy available in such a form that is appropriate for a diverse user population.[38]

Services such as Uber currently have a list of terms and conditions available when registering to use the phone app, which comprises of privacy information and seems the most appropriate place to list such privacy concerns. However, companies or private individuals who own or operate the vehicles are not necessarily required to account for data collected by the manufacturers, and so it seems likely that some form of warning or acceptance should be made available within the vehicle prior to data collection. In the

[36] Arvind Narayanan and Vitaly Shmatikov, 'Myths and Fallacies of "Personally Identifiable Information"' (June 2010) 53(6) *Communications of the ACM*, 24.
[37] Caroline Cakebread, *You're not alone, no one reads the terms of service agreements* (Nov 15 2017), Business Insider Australia <https://www.businessinsider.com.au/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=US&IR=T>.
[38] *Privacy Act 1988* (Cth) sch 1 pt 1 cl 1.5.

case of acknowledgement once inside of the vehicle, it is likely that the vehicle already has a good deal of information about a person prior to any data entry, by way of recording devices inside of the cabin, or any information already parsed to the vehicle by the owner/operator (such as start and end location, date of travel, etc.).

CAV users or those near a CAV may be unaware that their data is being collected, of the extent of the data being collected, or when proximity to a CAV is sufficient to allow data collection to begin and end. Those without significant technological knowledge are unlikely to be aware that CAVs will have capacity to collect data about their personal information from the chips in their credit cards, metro cards, phones, laptops, or any electronic device being carried, or that data will be collected on trips made, occupants, and conversations carried out in the vehicle

CAVs may also collect data from outside the vehicle via cameras or sensors. This may mean collecting data or images of people in the vicinity of the CAV such as bystanders, pedestrians etc. It is unlikely these persons will have been notified that data was being collected or consented to it. Even requiring AVs to self identify with signage or lighting may not be sufficient to ensure that any data collected by them has been voluntarily provided. How will bystanders or pedestrians be notified that data is being collected or given any meaningful opportunity to withhold personal information?

This may mean that data collected will not be as part of a voluntary or self-defined process and without the knowledge of some of the participants. This presents a clear privacy risk to persons who cannot be notified and have not consented. This risk, and the potential for adverse impact or discrimination as a result, is increased for those with a disability, those with language barriers, those with no economic alternatives, and those with particular cultural, religious or political affiliations..

It may also magnify risks of bias inherent in facial recognition software. Law enforcement and security applications that use CAV data to place a person in the

vicinity of a crime will be unreliable if the method of collection of that data does not distinguish between facial features persons of colour,[39] or recognise them at all.

Location data relating to CAV users (via direct access to location data) and non-users (via facial recognition to develop a pattern of locations over time where the person has been seen by passing vehicles) may present particular safety risks in relation to stalking or for victims of family violence, or enable reconnoitring for further crimes such as robbery.

It may be very difficult to notify, or gain any form of authorisation from other road users of the road or persons near the road these people without using some kind of broadcast technology that informs all devices nearby that they are, essentially, under surveillance by a CAV operating in the area. At this point other privacy boundaries are potentially crossed, with notifications moving into spam territory.[40] Further, signage on the CAV itself, alerting bystanders that the vehicle was autonomous and would be potentially collecting data in the vicinity, could be difficult to view while the vehicle is in motion, potentially distracting for other drivers and generally not a reliable way to ensure people are aware.

Even where CAVs are privately owned by individuals, data may still be transmitted to, and so collected by the manufacturer.

Careful consideration is required to ensure AV users and the broader public understand the types of data collected by AV, and what rights they may have to consent to that collection or withhold information, and if the latter, how to do so effectively.

[39] Jieshu Wang, *What's in your face? Discrimination in Facial Recognition Technology* (2018, Georgetown University).
[40] `Australian Communications and Media Authority, Dealing with mobile spam (20 April 2018), Australian Government <https://www.acma.gov.au/Citizen/Phones/Mobile/Dealing-with-mobile-spam/spam-complaints-reports-and-enquiries>.

Transparency

OCHCR principle 4 provides that "Data collectors should provide clear, openly accessible information about their operations, including research design and data collection methodology. Data collected by State agencies should be openly accessible to the public".

The GDPR requires transparency as a matter of principle, in that all data shall be subject to "lawfulness, fairness, and transparency".[41] Transparency is required in all aspects of data collection and use, and in the ability for individuals to exercise their rights with relation to their data.[42] Individuals must be involved and/or informed, or able to be, with the entire process throughout the life of the project (commencing with data collection), including their own rights to refuse, add, retract, restrict and modify their own personal data.[43]

The APPs require open and transparent management of data, the notification of collection of personal information, requirements in relation to collecting solicited and unsolicited data, as well an ability for individuals to access the personal data in relation to them. APP 1 states that 'reasonable steps' should be taken to implement practices, procedures and systems that will ensure compliance with APPs, and that clearly expressed and up to date privacy policies should be available free of charge and in an appropriate form.[44] The recent Notifiable Data Breaches scheme,[45] increases transparency by requiring businesses to notify all affected persons in the event that personal information may have been compromised and in particular if the data breach could cause significant harm.

[41] Ibid art 5.
[42] Ibid art 12.
[43] Ibid ch 3.
[44] *Privacy Act 1988* (Cth) sch 1 pt 1 cl 1.
[45] Ibid pt IIIC.

APP entities that hold personal information about an individual can only use or disclose this information for the primary purpose for which an individual would expect such information was collected, unless an exception applies.[46] Such exceptions may include situations where an individual has consented to, or would reasonably expect, information to be used or disclosed for a secondary purpose.[47]

Successful development and adoption of CAVs will depend on effective use of the data they generate. Manufacturers, regulators, law enforcement agencies, road authorities, infrastructure and C-ITS providers, urban planners and adjacent industries (insurers, maintenance and repair service providers, mapping services, MaaS providers, in-car advertising, etc to name just a few) will collect and access AV data for a wide variety of purposes, some of which will be commercial–in-confidence. The data generated by individuals using AVs may have significant commercial value, increasing as AVs are introduced more widely. It may be very difficult to give individuals access to their personal information in these datasets, especially where it is held outside of Australia (e.g. by an overseas manufacturer).

For CAV use to comply with APP 6, broad consents will be needed from users. CAV users and others will need to be provided clear information about how far such reasonable expectations might extend, probably much further than they initially envisage. It is not sufficient to assume that individuals should realise information will be used in a particular way that might breach their privacy, and context will be important in determining what can reasonably be expected.[48]

[46] APP 6.1.
[47] APP 6.1(a), 6.2(a).
[48] *'DK' and Telstra Corporation Limited* [2014] AICmr 118 (30 October 2014)

Privacy

Given the vast amount of data collected by AVs during operation, there is considerable scope for violation of individual's privacy if confidentiality is breached.

The OCHCR provides "Data disclosed to data collectors should be protected and kept private, and confidentiality of individuals' responses and personal information should be maintained." The GDPR responds to the need for privacy with multiple requirements designed to allocate responsibility for data security,[49] to ensure that it is accounted for in every step of the projects,[50] that it is subject to critical assessment and audit,[51] and that there are penalties in place for failure to comply with any such requirements.[52]

APP 2 requires that individuals must have the option of being anonymous of having a pseudonym when dealing with an APP entity. APP 11 provides for the security of personal information requiring an APP entity to take 'reasonable steps' to protect personal information it holds from misuse, interference, and loss, as well as unauthorised access, modification or disclosure.

While collection of a variety of data types that can be collected may be common practice in a standalone or security environment,[53] CAVs present new risks and opportunities. CAVs collect a wide variety of data types and transmitting this to various C-ITS providers, road authorities, regulators, etc, thus potentially acting as a mass mobile surveillance system. The greater the number of CAVs in use on the road, the

[49] GDPR art 24.
[50] Ibid 25.
[51] Ibid art 37-19 and ch 6.
[52] Ibid ch 8.
[53] Australian Institute of Criminology, *Using CCTV to reduce antisocial behaviour* (3 November 2017) Australian Government <https://aic.gov.au/publications/crm/crm080>.

greater the data collection capacity will be. It is likely to be very difficult to effectively use MaaS, CAVs etc anonymously or via pseudonym.

Where individuals are concerned that their privacy has been breached, they can make a complaint to the Office of Australian Information Commissioner. However such a complaint relies on the individual becoming aware that their privacy has b unlikely that individuals will become aware of privacy breaches. Persons with disability, elderly persons or children particularly may be less likely to be aware a breach has occurred and be less likely to be able to navigate the complaints process.

Data Storage

The UN Special Rapporteur on the right to privacy's address to the Human Rights Council in 2016[54] asserted that it is necessary to find a balance between storing enough information to assist when need to learn about a person's past and the notion that where information is stored for a prolonged period of time or in too high detail, individuals may be continually confronted by his or her past, and not be able to develop a future.

CAV data may be used to inform insurers and in allocating fault in the event of a collision. It may be necessary to retain this information for considerable periods of time given limitations periods for civil claims, particularly those involving children, or in relation to law enforcement and imposition of criminal liability.

Proceedings commenced in the US in March 2018 and still underway, *Zellmer v Facebook, Inc*., allege that Facebook is acting in violation of the Illinois *Biometric Information Privacy Act* ("BIPA") by capturing, possessing, collecting, storing, receiving

[54]Mr Joseph Canatacci, 'Statement by Special Rapporteur on the right to privacy' (Speech delivered at the 31st Session of the Human Rights Council, 9 March 2016).

through trade, obtaining, and using the biometric identifiers and biometric information of Mr Zellmer and other individuals, without their informed written consent. he *BIPA* provides that private entities must not store biometric data and must also publicly publish the timing of retention and termination of data storage. Although proceedings are still underway, and no decision has been made, the complaint highlights that the storage of biometric data directly increases an individual's risk of identity theft.

The Australian Government introduced into parliament the *Identity-matching Services Bill* 2018, seeking to provide the Commonwealth and state and territory governments with the authority to use and disclose personal information retrieved via identity-matching technology. In comparison with the GDPR and the BIPA, Australia's approach to data storage and the protection of privacy rights may be weaker than its international counterparts. In response to the introduction of the Bill, the Law Council of Australia ("LCA") highlighted the risk that the identity-matching services could result in excessive interference and oversight of the private lives of Australians. LCA further argues that the bill requires amendments before it can satisfactorily ensure identity-matching services uphold privacy rights and the government can guarantee transparency and accountability in relation to data-sharing practices.

APP's 12 and 13 deal with access to[55] and correction of[56] personal information, allowing individuals to know what personal information held by an entity says about them, and provides the ability for them to correct the record if necessary. Given the amount of information generatedb y the use of CAVs and the number of potential entities holding that data, it is likely to be very difficult for an individual to exercise these rights.

[55] *Privacy Act 1988* (Cth) sch 1 pt 5 cl 12.
[56] Ibid 13.

Accountability

This OCHCR principle states “Data collectors are accountable for upholding human rights in their operations, and data should be used to hold States and other actors to account on human rights issues.” The GDPR makes companies collecting and processing data that may be considered to be personal responsible and accountable for the handling of that data. They are expected to ‘implement appropriate technical and organizational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed”. hey are also required to employ a data protection officer, and are answerable to independent supervisory authorities. Deterrents are in place to ensure that companies do better in ensuring human rights of data subjects.

The Australian Information Commissioner can request privacy impact assessments,[57] or conduct an assessment,[58] although it is unclear what events might trigger such action. Individuals may file complaints to the commissioner regarding data concerns after they have attempted to seek recourse via the company holding the data, at which time an investigation may be ordered. Accountability within Australia has minimal recourse, and none where data is not considered to be personal enough. Serious and repeated interferences with privacy attract a civil penalty.[59]

The complaint scheme under the Office of the Australian Information Commission (“OAIC”) requires an individual to be aware of or understand their rights in relation to privacy, and subsequently requires the knowledge and/or resources to navigate this system in order to receive an investigation of an alleged breach. The addition of privacy concerns in relation to autonomous vehicles also adds a layer of complexity for vulnerable people in trying to understand their legal privacy rights and is likely to result

[57] *Privacy Act 1988* (Cth) s 33C.
[58] Ibid s 33D.
[59] *Privacy Act 1988* (Cth) s 13G.

in greater reliance on advocacy services. Subsequently, this will require capacity building of the advocacy services workforce.

Recommendations

CAVs offer significant potential benefits in terms of increased safety, increased access to mobility and other additional social, economic and environmental benefits. CAVs also raise new concerns regarding privacy, confidentiality and use of data. These concerns must be identified and addressed to ensure that the benefits of this new technology do not come at the cost of decreased protections for privacy or human rights.

While the enactment of the Notifiable Data Breaches Scheme goes some way towards improving accountability and transparency of those dealing with personal information, more needs to be done in Australia in order to protect individuals human right to privacy with the widespread introduction of autonomous vehicles. This includes, *inter alia*:

- Refining privacy legislation to be more in-line with OHCHR guidelines and GDPR, giving more explicit rights to the data subject;
- clarifying the meaning of “personal data” to include any data that can be used to link to or generate identifying data. This would be more in line with the GDPR in the European Union;
- Require specific ethics and auditing requirements for data collected by anything that could be classed as, or considered to be, a mass surveillance system, or mobile surveillance device;

Consideration should be given as to how to encourage wider community and industry discussion of these issues including:

- ethical review of all projects working with personal (or potentially personal) data, such as IEEE (Institute of Electrical and Electronics Engineers) robotics and ethics compliance standards etc.,
- recommending autonomous vehicles legislation requires ethical compliance and agreement to auditing/monitoring of data stores prior to authorization for any product or service to be allowable within the country.

This submission has outlined the general commitment of the international community, to providing individuals with increased protections against entities who collect, store and use their personal information, as evidenced by the human rights-based approach within the GDPR and the OHCHR guidelines for data collection.

This submission recommends that these international frameworks inform review of Australia's privacy law regime, to ensure that the Australian Government satisfies its obligations under the UDHR when autonomous vehicles are introduced on our roads.