Privacy in automation: an appraisal of the emerging Australian approach[i]

Angela Daly

PRE-PRINT VERSION, FORTHCOMING IN COMPUTER LAW & SECURITY REVIEW (2017)

ABSTRACT

This article presents an initial appraisal of the emerging Australian approach to applying privacy and data protection laws to automated technologies. These laws and the general context in which they operate will be explained, with appropriate comparisons made to the European Union frameworks. In order to examine their specific application vis-à-vis automated technologies, three case studies - Automated facial recognition technologies (AFRT), unmanned aerial vehicles (UAVs – better known as 'drones') and autonomous vehicles (or 'driverless cars') – are selected to examine the extent to which existing privacy and data protection laws, and their application, can be considered adequate to address privacy and data protection risks that these technologies bring. These case studies evidence existing deficiencies with privacy protection in Australia and the inadequacy of recent reform processes, demonstrating that Australian data privacy laws are not well placed to protect individuals' rights vis-a-vis automated technologies.

Keywords: Australia; facial recognition; drones; driverless cars; data protection; privacy

1. Introduction

Automated technologies are increasingly being applied in daily life in developed countries. The term 'automation' when combined with technology can encompass a wide variety of devices and services, which are also cross-fertilised by other technological developments such as in algorithms, materials, and the Internet of Things.

Automation may bring various benefits for certain individuals and society at large. Automation may produce profit and efficiency, and facilitate the operation of highly complex systems.[1] However, dangers or disadvantages of automation have also been identified including the automation of jobs, dangers to individuals' health and wellbeing (including death) and even the possible eventual

[1] Peter Hancock, 'Automation: How Much is Too Much?' (2014) 57 (3) *Ergonomics* 449.

redundancy of humans.[2] These concerns are all, at heart, related to the ability for decisions to be made, and actions taken, by automated technologies directly or by humans on the basis of automated processes without further deliberation.[3] Among these concerns is the negative effect automation may have on individual data privacy and data protection, given many automated technologies rely on data, which they may also create about human beings, or which data which is created by humans and used by these technologies.[4]

The adequacy of existing laws to address automated technologies have been called into question in various jurisdictions. Autonomous vehicles alone are currently generating a large amount of scholarship about whether a variety of laws, from traffic regulations to the laws of war to tort liability are appropriate for the characteristics and affordances of this new technology.[5] Among the relevant areas of law is also privacy: Current privacy and data protection measures when faced with automation have been called into question in a number of jurisdictions. In the US, where the Fourth Amendment provides some privacy protection against government interferences, automated systems so far have been implicitly treated by courts as equivalent to human beings for the purposes of the Third Party Doctrine whereby Fourth Amendment protection does not apply to information an individual voluntary discloses to a third party.[6] In the EU, robots may challenge the categories of data controller and data processor on which data protection law is based and render concepts such as privacy-by-design uncertain in their application.[7]

Indeed, the challenges for privacy from automation may be so profound that it has been argued in the context of autonomous vehicles that ‘a default lack of privacy for personal travel may become the

[2] Devdatt Dubashi and Shalom Lappin, ‘AI Dangers: Imagined and Real’ (2017) 60(2) *Communications of the ACM* 43; Robert Sparrow, ‘Killer Robots’ (2007) 24(1) *Journal of Applied Philosophy* 62; Stephen Mason, ‘The presumption that computers are ‘reliable’ ‘ in Stephen Mason and Daniel Seng (eds), Electronic Evidence (4th ed, Institute for Advanced Legal Studies, 2017), at p. 124.

[3] Although in the European Union, Article 15 of the Data Protection Directive provides, subject to some exceptions, that a person should not be subject to a decision which produces legal effects concerning them or significantly affects them based solely on automated data processing intended to evaluate certain personal characteristics, such as that individual’s performance at work, creditworthiness, reliability, conduct, etc. An updated version of this provision can be found in Article 22 of the General Data Protection Regulation.

[4] Ryan Calo, ‘Robots and Privacy’, in Patrick Lin, George Bekey and Keith Abney (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press 2011); Ian Kerr and Marcus Bornfreund, ‘Buddy Bots: How Turing's Fast Friends are Under-Mining Consumer Privacy’ (2005) 14(6) *Presence: Teleoperators and Virtual Environments* 647.

[5] See e.g. Bryant W Smith, ‘Automated Vehicles Are Probably Legal in the United States’ (2014) 1 *Texas A&M Law Review* 411; Maurice Schellekens, ‘Self-driving cars and the chilling effect of liability law’ (2015) 31(4) *Computer Law and Security Review*; Gary Marchant, Braden Allenby, Ronald Arkin, Edward Barrett, Jason Borenstein, Lyn Gaudet, Orde Kittrie, Patrick Lin, George Lucas, Richard O'Meara, and Jared Silberman, ‘International Governance of Autonomous Military Robots’ (2010) 12 *Columbia Science and Technology Law Review* 272*;* Kyle Graham, ‘Of Frightened Horses and Autonomous Vehicles: Tort Law and its Assimilation of Innovations’ (2012) 52 *Santa Clara Law Review* 101.

[6] Matthew Tokson, ‘Automation and the Fourth Amendment’ (2011) 96 *Iowa Law Review* 581.

[7] Ugo Pagallo, ‘The Impact of Domestic Robots on Privacy and Data Protection, and the Troubles with Legal Regulation by Design’ in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016).

norm'.[8] Yet automation sounding the death knell for personal privacy may be a flawed technologically deterministic approach. A straightforward solution to the privacy risks – or at least a means of limiting them – in the context of robots and automation may be 'air gaps' i.e. a general policy of disconnecting robots and autonomous machines from the Internet and the cloud as a form of 'privacy before design'.[9]

In an attempt to begin to address some of the legal issues surrounding robots, the European Parliament has been pro-active with a Resolution from February 2017 on Civil Law Rules on Robotics.[10] Among the topics covered in this Resolution is privacy and data protection. The European Parliament has requested clarification as regards the rules and criteria for using cameras and sensors in robots within the GDPR's implementation framework, and has also requested that the European Commission ensures data protection principles, control mechanisms for data subjects and appropriate remedies are followed as regards robots; and that the European Commission ensure appropriate recommendations and standards are fostered and integrated into policy.

This European Parliament Resolution is the most prominent attempt by a legislature or government to engage with the privacy and data protection implications of automation and robotics globally, which perhaps is not surprising given EU data protection and privacy laws are the most advanced internationally and represent a high level of protection. Yet automation and robotics are not bound by jurisdiction, and so how other countries' legislatures and governments encounter these technologies is also of great importance for the relationship between privacy and automation. To that end, this article examines the Australian experience with automation and privacy, to provide an insight into how this particular jurisdiction is encountering the topic. Australia represents an important point of international comparison, particularly for EU privacy and data protection laws. Australian data privacy laws are based on a similar model to the EU's Data Protection Directive, but the legal system diverges sharply from its European counterparts with the absence of constitutional or enforceable fundamental rights to privacy (or data protection).

This paper takes three emerging 'automated technologies' as case studies in which to understand better the extent to which existing laws – in this case, in the Australian jurisdiction – are fit for purpose. The case studies comprise: automated facial recognition technology (AFRT); unmanned aerial vehicles (drones); and driverless cars. These three applications of automated technologies have been selected since they are examples of automation which are currently being rolled out among the general population in Australia, as opposed to remaining under experimental use in research conditions. They are also all technologies which pose problems and risks for the privacy and data protection of individuals, and so represent lenses through which the adequacy of existing laws – and proposals for their reform – can be tested.

[8] Daniel Fagnant and Kara Kockelman, 'Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations' (2015) 77 *Transportation Research Part A: Policy and Practice* 167.

[9] Bibi van den Berg, 'Mind the Air Gap: Preventing Privacy Issues in Robotics' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016).

[10] European Parliament, *Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)) <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0051&language=EN&ring=A8-2017-0005>

This article will proceed by providing some context on the Australian legal system's approach to privacy and data protection laws, before exploring how the system has encountered the three aforementioned automated technologies. The article's main findings are that privacy concerns have been acknowledged in the deployment of all three technologies, which include the resurfacing of pre-existing deficiencies in the Australian legal framework to protect privacy, but that no further legal or regulatory action to remedy these deficiencies has as yet taken place, leading to a situation where privacy rights are not sufficiently protected in Australia, and certainly receive a lower level of protection vis-à-vis these automated technologies than is the case in the EU.

2. Australian privacy and data protection laws

This section examines the status of privacy and data protection in existing Australian laws in order to understand the legal and regulatory backdrop against which the developments in automated technologies are taking place.

2.1 A human or constitutional right to privacy?

Australia is a signatory to various international human rights treaties, including the International Covenant on Civil and Political Rights (ICCPR), whose Article 17 protects the right to privacy.[11] Yet despite Australia's ratification of this treaty, there is no legislation implementing the rights in domestic law, with the exception of laws against sexual, racial, disability and age discrimination.[12]

Indeed, at the domestic level, Australia is exceptional among Western liberal democracies by lacking a comprehensive Bill of Rights in the Constitution or enacted via legislation. The Australian Constitution does include express protection for a few specific rights such as the right to vote and freedom of religion, but a right to free speech had to be 'implied' into the Constitution by judges during the 1990s,[13] and this implied right is very limited in its application i.e. to political communication. There is also no constitutional right, either express or implied, to privacy in Australia, in sharp contrast to similar jurisdictions such as the UK.

At the state and territory level in Australia, the Australian Capital Territory (ACT) and the State of Victoria both have human rights legislation which introduces individual rights including free expression

[11] Ronald McCallum 'The United Nations Human Rights Treaties: What Will Be Their Future Role In Protecting Our Human Rights?' (2015) Sydney Law School Research Paper No. 15/90.

[12] Jane Stratton 'Domestic operation of human rights law in Australia' (2013) 85 *Hot Topics: Legal Issues in Plain Language* 16.

[13] Starting in *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106 and *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1.

and privacy.[14] However these rights are only enforceable vis-à-vis public bodies in the ACT and Victoria respectively, and so are very limited in their application. The judiciary is also not empowered to strike down laws which are incompatible with the human rights enumerated. At the time of writing, there is a public discussion underway in Queensland as to whether a similar bill of rights, including a right to privacy, should be introduced there.

2.2 Common law

Australia is a common law jurisdiction. Various areas of law have evolved to protect aspects of an individual's space and reputation, including copyright, defamation, trespass, nuisance and confidentiality.

There is speculation as to whether a right to privacy or a tort of invasion of privacy exists in Australian common law. The leading case on this point in Australia is *Lenah Game Meats*, which left open the possibility of the judiciary introducing a tort of invasion of privacy given the right circumstances, but did not do so based on the facts at hand on which it was found that there had been no invasion of privacy.[15] In the wake of the *Lenah Game Meats* decisio*n*, there have been some cases in lower courts on this issue, but none so far has reached the Australian High Court, and it seems that the prospects are better for a statutory tort being introduced in Australian law than the recognition of a common law tort.

In this absence of an appropriate case reaching the High Court, there have been discussions in Australia about introducing a tort of serious invasions of privacy by statute. The federal Australian Law Reform Commission[16] and the New South Wales Legislative Council Standing Committee on Law and Justice[17] have recommended the introduction of such a statutory tort in their respective jurisdictions. However, the current federal government and the New South Wales state governments do not at this time support the introduction of such a tort,[18] so it is unlikely to appear on the law books in either jurisdiction any time soon.

2.3 Data privacy legislation

[14] Respectively: *Human Rights Act (ACT)* 2005; *Charter of Human Rights and Responsibilities Act (Vic)* 2006.

[15] *ABC v Lenah Game Meats Pty Ltd* (2001) 185 ALR 1.

[16] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (3 September 2014) ALRC Report 123.

[17] New South Wales Legislative Council Standing Committee on Law and Justice, *Remedies for the serious invasion of privacy in New South Wales* (3 March 2016) Report.

[18] See: Australian Government Attorney-General's Department Law, Crime and Community Safety Council, *October 2016 Communique*, 21 October 2016; New South Wales Government response to the Legislative Council Standing Committee on Law and Justice's report into *Remedies for the serious invasion of privacy in New South Wales*, 5 September 2016.

While Australia has some legislative protection of privacy, it is very much a patchwork of different statutes protecting different aspects of privacy rather than an overarching enforceable principle. It could be argued further that the practical prospects of Australia moving to protect privacy rights have been greatly diminished with the introduction of mandatory data retention laws in early 2015 (despite similar laws being ruled invalid in the EU in 2014),[19] and revelations about the dearth of privacy impact assessments conducted before national security legislation is passed in Australia.[20]

Nonetheless, the main piece of privacy legislation protecting data is the federal *Privacy Act 1988 (Cth)*. This legislation regulates the handling of personal information about individuals (natural persons) which includes the collection, use, storage and disclosure of this information, as well as access to and correction of the information. There are also laws in most Australian states and territories which regulate the state-level public authorities' use of personal information.

The *Privacy Act* gave effect to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and ICCPR Article 17 in Australian law, and saw the appointment of the first Australian Privacy Commissioner.[21] It is based on a similar model to European data protection laws. A major revision of the Act occurred in 2014, via the *Privacy Amendment (Enhancing Privacy Protection) Act* 2012. This revision introduced the Australian Privacy Principles (APPs) to regulate the handling of personal information by Australian federal government agencies and some private sector actors (usually businesses with an annual turnover of more than AU$3 million). Previously, different sets of principles applied depending on whether the organisation was from the public or private sector. Essentially, entities which are bound by the APPs must adhere to the obligations contained therein.

While Waters has welcomed a consolidated set of principles, he has also criticised the fact that in terms of substantive privacy protection, 'none of the thirteen APPs is… an overall improvement on the previous principles' and in fact '[e]ight of the thirteen APPs are actually worse for privacy protection', particularly the use and disclosure principles, cross-border data transfer and anonymity principles.[22] However, Waters does also acknowledge the increase in the Privacy Commissioner's enforcement powers compared to the situation prior to the reform.[23]

2.4 Relationship with European data protection law

[19] Graham Greenleaf, 'Going Against the Flow: Australia Enacts a Data Retention Law' (2015) 134 *Privacy Laws & Business International Report* 26.

[20] Roger Clarke, 'Privacy impact assessments as a control mechanism for Australian counter-terrorism initiatives' (2016) 32 (3) *Computer Law & Security Review* 403.

[21] Australian Government Office of the Australian Information Commissioner, *History of the Privacy Act* <https://www.oaic.gov.au/about-us/who-we-are/history-of-the-privacy-act>

[22] See: Nigel Waters, 'Responding to new challenges to privacy through law reform: a privacy advocate's perspective' in Normann Witzleb, David Lindsay, Moira Paterson and Sharon Rodrick, *Emerging Challenges in Privacy Law: Comparative* Perspectives (Cambridge University Press 2014), at p. 52.

[23] Ibid at p. 54.

As mentioned above, the Australian *Privacy Act* and data privacy protections are generally based on a similar model to the origins of EU law on the topic. There is also great interest in Australia around developments in EU data protection law, such as the recognition of a Right to be Forgotten,[24] and the introduction of the General Data Protection Regulation.[25] However, there are also some important divergences between the two systems.

Firstly, Australia is not currently recognised by the European Commission as a third country which provides an adequate level of protection for the personal data of EU citizens in its own legal system. One exception is for airline Passenger Name Record (PNR) data, whose processing and transfer is facilitated by a specific bilateral agreement between the EU and Australia.

Certainly, the fact that the APPs do not apply to businesses with a turnover of less than AU$3million per year entails that many actors which handle personal data are not bound by this regime. Yet if these same small and medium businesses were based in the European Union, they would likely fall within the remit of European data protection law. This has previously been noted as a concern by the Article 29 Working Party that must be addressed if Australian data privacy laws are to be considered 'adequate' by EU standards.[26]

Furthermore, the lack of a constitutional or otherwise enforceable right to privacy is another point of sharp divergence between Australia and the European Union. Currently, in order to enforce their privacy rights, individuals must first make complaints to the organisation allegedly in breach of the APPs, and if the organisation does not address the complaint satisfactorily, the individual can then escalate the complaint to the Office of the Australian Information Commissioner (OAIC). The OAIC can then investigate the complaint and is also empowered to instigate own-initiative investigations without there being a complaint. However, over the last few years there have been serious concerns about the OAIC receiving insufficient funding and resourcing from the government to carry out its function effectively.[27] Since individuals cannot bring a case to the courts themselves, they must rely on an organisation which may be unable, due to resource constraints, to pursue their complaint. This has also resulted in the situation of very little case-law occurring in Australia on data privacy matters.

This situation is compounded by the participation of Australia's intelligence agencies along with those of the UK, US, Canada and New Zealand in the shadowy Five Eyes data gathering, sharing and

[24] Jarrod Bayliss-McCulloch, 'Does Australia Need a "Right to be Forgotten"?' (2014) 33(1) *Communications Law Bulletin.*

[25] Lora Shaw, 'The impact of the European General Data Protection Regulation in Australia' *Keypoint Law* (22 December 2015) <http://www.keypointlaw.com.au/keynotes/impact-new-european-general-data-protection-regulation-australia>

[26] See: Article 29 Data Protection Working Party, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 FINAL.

[27] See: Allie Coyne, 'Starved of funding, resources, OAIC is left to shrivel' *IT News* (17 July 2015) <http://www.itnews.com.au/blogentry/starved-of-funding-resources-oaic-is-left-to-shrivel-405273>

surveillance partnership exposed by Edward Snowden in 2013.[28] In Australia, ironically, rather than rolling back on this kind of activity, these revelations actually prompted the legislating of various data gathering activities in the form of the aforementioned mandatory data retention legislation. In light of the CJEU decision in *Schrems* invaliding the EU-US Safe Harbor post-Snowden revelations given the inadequacy of US data protection practices,[29] it seems likely that Australia's participation in the Five Eyes partnership and omission to take proactive measures to protection privacy afterwards, would further render Australian data privacy laws 'inadequate' in the EU's eyes.

3. Automated technologies in Australia

Despite these inadequacies of data privacy laws, Australia has been keen to embrace new automated technologies and can be viewed as an early adopter of many of them. In recent times, this has been supplemented by government policies around innovation such as the National Innovation and Science Agenda[30] and state-level initiatives such as Advance Queensland.[31] There is also a significant amount of academic and industry research being conducted in Australia on robotics, including applications in the agricultural and mining and resources sectors, two of the country's most economically important industries.[32]

This section examines three robotics/automation developments which are being applied in Australia and which also raise privacy and data protection concerns. The regulatory response from the Australian authorities is assessed to discern the extent to which the system is adequately addressing these concerns.

3.1 Facial recognition

Automated facial recognition technology (AFRT) involves the automated extraction, digitisation and comparison of the arrangement of facial features, using an algorithm to compare a particular template derived from the previously-captured image or images of a face to templates of facial images stored in

[28] Indeed, the Australian intelligence agencies have enjoyed a close relationship with their American counterparts. See: Nick Bisley, ' 'An ally for all the years to come': why Australia is not a conflicted US ally' (2013) 67 (4) *Australian Journal of International Affairs* 403.

[29] Case C-362/14 *Schrems v. Data Protection Commissioner* (6 October 2015).

[30] Australian Government, *National Innovation and Science Agenda* <http://www.innovation.gov.au/>

[31] Queensland Government, *Advance Queensland* <http://advance.qld.gov.au/>

[32] See: Kathryn Diss, 'Robotic trucks taking over Pilbara mining operations in shift to automation' *ABC News*, (26 April 2014) <http://www.abc.net.au/news/2014-04-25/computer-controlled-trucks-taking-over-in-pilbara-mining-wa/5412642>; Sarina Locke, 'Robotics to revolutionise farming and attract young people back to agriculture says Australian Centre for Field Robotics at Sydney University' *ABC Rural* (4 February 2015) <http://www.abc.net.au/news/2015-02-04/agricultural-robotics-future-jobs/6068450>

a database.[33] Recent developments internationally have seen real-time facial recognition technology being integrated with CCTV ('Smart CCTV') and deployed in public places and in 'pre-crime' scenarios.[34]

Facial recognition technology has been used by both public and private sector organisations for their own purposes. The most prominent legal assessment of facial recognition can be found in the wrangling around Facebook's use of it in the EU without explicit opt-in user consent. The Hamburg data protection authority viewed this to be incompatible with EU data protection law, and in response Facebook disabled this feature for its EU users.[35] The Article 29 Working Party has also examined facial recognition as a subset of biometric technology, and considered that users must be informed if facial recognition technology will be used and must have an option to consent to this happening; their acceptance of overall terms and conditions will not usually be sufficient to constitute consent to the use of facial recognition technology.[36]

In the Australian context, a similar issue has not been dealt with by legal and regulatory authorities. There has, however, been some theoretical discussion on the matter. For example, Bunn has considered what the Australian law position would be vis-à-vis Facebook's facial recognition feature, and this position appears to be more ambiguous than what has been arrived at in the EU, although facial recognition being applied to the photos of non-Facebook users by Facebook would probably constitute a breach of the APPs.[37] Bunn views the use of facial recognition technology on users' uploaded photos and the creation of further data from about the images ('metadata') may create compliance risks vis-à-vis the APPs regarding user consent for an organisation carrying out these activities under general terms and conditions.

Facial recognition technology is being deployed in practice in Australia by law enforcement and security agencies. The introduction of biometric drivers' licences also involved the introduction of facial recognition techniques to verify the identity of the applicants.[38] Smart CCTV is currently used in some Australian jurisdictions by law enforcement agencies.[39] Furthermore, the Australian National Open Source Intelligence Centre collects and analyses information publicly available online, which can include photos on social media sites such as Facebook.[40] Recently, the Australian Government

[33] Andy Adler and Michael E. Schuckers, 'Comparing Human and Automatic Face Recognition Performance' (2007) 37(5) *IEEE Transactions on Systems, Man, and Cybernetics* 1248.

[34] See: James Byrne and Gary Marx, 'Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact' (2011) 3 *Journal of Police Studies* 17.

[35] Information Age (2011) 'Facebook facial recognition breaks EU law – regulator' <http://www.information-age.com/technology/security/1669438/facebook-facial-recognition-breaks-eu-law---regulator>

[36] Article 29 Working Party, *Opinion 03/2012 on developments in biometric technologies* (WP193).

[37] Anna Bunn, 'Facebook and face recognition: kinda cool, kinda creepy' (2013) 25(1) *Bond Law Review* 35.

[38] See: Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40(1) *University of New South Wales Law Journal* (in press).

[39] NEC 'NEC facial recognition helps NT Police solve cold cases and increase public safety in Australia' press release (1 September 2015) <http://au.nec.com/en_AU/press/201509/nec-facial-recognition-increases-public-safety-in-australia.html>

[40] National Open Source Intelligence Centre <http://www.nosic.com.au/index.htm>.

announced additional funding for the Australian Federal Police to develop a new big data capability to gather information from social media sites to add to existing intelligence sources.[41]

Mann and Smith have noted that Australian state and territory jurisdictions have been preparing for the expansion of facial recognition use over the last few years, particularly to enable data sharing of images with federal agencies.[42] One example is New South Wales, which amended its legislation to permit photographs held by the road authority for the purpose of issuing drivers licences to be released to various law enforcement and security agencies, seemingly without the need for a judicial warrant, and also without the knowledge or consent of the individual involved.[43]

The Australian Federal Government also announced that a National Facial Biometric Matching Capability, known by its somewhat Orwellian short form 'the Capability', would be introduced by mid-2016, enabling law enforcement and security agencies to share images (such as those obtained for passport and visa-issuing purposes) for facial recognition purposes, with the possibility of integration with Smart CCTV and other municipal, state and federal surveillance systems. Yet the design of the Capability will not be a centralised hub containing facial images, as this would require federal legislation to effect. Mann and Smith consider that the Capability will include the images of all Australians holding biometric passports which comprises around 12 million people.[44] The first phase of the Face Verification Service was launched in November 2016 which provides the Department of Foreign Affairs and the Australian Federal Police with access to citizenship images held by the Department of Immigration and Border Protection, with the intention that this scheme will expand later to include other government agencies.[45]While the Capability did pass a Privacy Impact Assessment,[46] this has not allayed privacy concerns about the use of facial recognition technology by Australian law enforcement and security agencies in these ways.[47]

The APPs would be a priori applicable to the Capability, since facial images will constitute 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or … biometric templates', which constitute 'sensitive information' for the purposes of

[41] Michael Keenan, 'New 18.5 million biometrics tool to put a face to crime. Media Release for Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism' media release (9 September 2015) <https://www.ministerjustice.gov.au/Mediareleases/Pages/2015/ThirdQuarter/9-September-2015-New-$18-5-million-biometrics-tool-to-put-a-face-to-crime.aspx>.

[42] Mann and Smith, supra n38, at p. 6.

[43] See: *Road Transport Legislation Amendment (Release of Stored Photographs) Regulation 2015 (NSW)* amending cl 107 of the *Road Transport (Driver Licensing) Regulation 2008* (NSW)

[44] Mann and Smith, supra n38, at p. 8.

[45] Australian Government Attorney-General's Department, *Face Verification Service,* <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Face-verification-service.aspx>

[46] Information Integrity Solutions, *National Facial Biometric Matching Capability Privacy Impact Assessment – Interoperability Hub (*August 2015) <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Privacy-Impact-Assessment-National-Facial-Biometric-Matching-Capability.PDF>

[47] Mann and Smith, supra n38, p. 11.

the *Privacy Act*.[48] According to APP 3, sensitive information must generally only be collected if the individual consents to it, but a government agency can collect sensitive information without consent if it is an 'enforcement body' and it reasonably believes that 'the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities'. While, in general, according to APP 6 an entity should not use or disclose information which has been collected for a particular purpose (e.g. issuing a passport) for a secondary purpose (e.g. marketing) without the individual's consent, there is an exception to this if the entity 'reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body'. As Mann and Smith put it, '[t]hese exemptions are significant because agencies with an enforcement function do not need consent, a warrant, or a court order to collect and retain photographs, to process this information to create facial templates and disclose or share this information with other agencies'.[49] These carve-outs within the individual APPs to permit enforcement activity vis-à-vis personal information without individual consent are also accompanied by total exemptions from the *Privacy Act* for a number of Australian security agencies.[50] These carve-outs and exemptions have already been criticised as being too broad,[51] and as trading individual rights for community interests in security and law and order.[52]

Thus it seems that the use of AFRT for law enforcement and security purposes in Australia will generally be permitted under privacy laws and individuals may have no knowledge that their data is being captured, and used for different purposes from the original reason why it was collected. The sidestepping of Parliamentary scrutiny for implementation of the Capability is concerning from a rule of law perspective, and also avoids the possibility of privacy concerns being debated by legislators, forming another example of Ericson's 'counter-law' in Australia (where law enforcement activities are technically legal in accordance with statutory authority, but undermine the rule of law and civil liberties),[53] along with mandatory data retention and government use of computer network operations.[54] The lack of a constitutional right to privacy in Australia also ensures that these measures cannot be challenged on the basis that they are disproportionate infringements of citizens' privacy rights, in contrast to the situation, for instance, in the EU. Accordingly, Australian law here can be seen as providing very little – if not no – redress for the privacy concerns raised by this form of automation.

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

[49] Mann and Smith, supra n38, p. 13

[50] Namely: the Office of National Assessments; the Australian Security Intelligence Organisation; the Australian Secret Intelligence Service; the Australian Signals Directorate; the Defence Intelligence Organisation; and the Australian Geospatial-Intelligence Organisation.

[51] See: Roger Clarke, *The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines* (15 February 1997) <http://www.rogerclarke.com/DV/PActOECD.html >; Graham Greenleaf, '"Tabula Rasa": Ten Reasons Why Australian Privacy Law Does Not Exist' (2001) 24(1) *University of New South Wales Law Journal* 262.

[52] Simon Bronitt and James Stellios, 'Telecommunications Interception in Australia: Recent Trends and Regulatory Prospects' (2005) 29(11) *Telecommunications Policy* 875

[53] Richard Ericson, 'Security, surveillance and counter-law' (2007) 68(1) *Criminal Justice Matters* 6.

[54] Adam Molnar, Christopher Parsons & Erik Zouave, 'Computer Network Operations and 'rule-with-law' in Australia' (2017) 6(1) *Internet Policy Review*. See also: Nicolas Suzor, Kylie Pappalardo and Natalie McIntosh, 'The passage of Australia's data retention regime: national security, human rights and media scrutiny' (2017) 6(1) *Internet* Policy *Review*.

3.2 Drones

Another automated technology which is growing in application in Australia is unmanned aerial vehicles, better known as ‘drones’.[55] Cheap models are retailing for under AU$100 and so within the purchasing power of the average Australian. More sophisticated and expensive models are also available commercially, and there is, in addition, military and police use of drones for security and law enforcement purposes, from the more mundane (traffic control), to the more dramatic (use in the ‘War on Terror’).[56]

Drones as a technology do not inherently pose privacy concerns, but their roll-out has usually involved them being coupled with cameras to take photos, make recordings and feed back real-time footage, and also in some cases Internet accessibility (thus adding drones as artefacts to the growing ‘Internet of Things’).[57]

So far in Australia, drones have only been specifically governed by the *Civil Aviation Safety Regulations 1998* (Cth), which are designed to ensure the safe use of aircraft, rather than any specific privacy purpose. In 2002, these Regulations were modified to include rules specifically governing the use of drones (reportedly a world first), again laying down rules primarily concerned with the safe operation of these machines, including a rule that drones should not be operated within 30 meters of a person not involved in their operation and drones should not be operated over ‘populous’ areas.[58] In 2016, these measures were updated, and entailed that the operators of small commercial drones would be exempt from paying AUS$1400 in regulatory fees and individuals would be able to operate drones of up to 25 kg in weight on their property without the need for prior regulatory approval.[59] The updating of the rules seems to take a largely deregulatory approach, which has been criticised for possible adverse consequences for the safety of people and property,[60] and stands in sharp contrast to the approach in

[55] See: Roger Clarke, ‘Understanding the drone epidemic’ (2014) 30(3) *Computer Law and Security Review* 230.

[56] See: Australian Government Department of Defence, *2016 White Paper*, <http://www.defence.gov.au/whitepaper/Docs/2016-Defence-White-Paper.pdf>; Alex Edney-Browne, ‘Imprecise, Automated, Deadly: Why Australia Shouldn’t Buy Into The Drone War’ *New Matilda* (16 March 2016) <https://newmatilda.com/2016/03/16/imprecise-automated-deadly-why-australia-shouldnt-buy-into-the-drone-war/>; Omar Mubin, ‘Police drones: can we trust the eyes in the skies?’ *The Conversation* (29 February 2016) <https://theconversation.com/police-drones-can-we-trust-the-eyes-in-the-skies-53981>.

[57] See: Ryan Calo, ‘The Drone as Privacy Catalyst’ (2011) 64 *Stanford Law Review Online* 29; Rachel Finn and David Wright, ‘Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications’ (2012) 28(2) *Computer Law and Security Review* 184.

[58] *Civil Aviation Safety Regulations 1998* (Cth) Part 101. See also: Roger Clarke and Lyria Bennett Moses, ‘The regulation of civilian drones’ impacts on public safety’ (2014) 30(3) *Computer Law and Security Review* 263

[59] Alexandra Beech, ‘Drone laws could lead to mid-air collisions, pilots and air traffic controllers warn’ *ABC News*, 28 September 2016 <http://www.abc.net.au/news/2016-09-28/new-drone-laws-could-lead-to-mid-air-collisions-pilots-say/7884574>

[60] Chris Pash, ‘Insurers are worried about new Australian drone laws which come into force today’ *Business Insider* (29 September 2016) <https://www.businessinsider.com.au/insurers-are-worried-about-new-australian-drone-laws-which-come-into-force-today-2016-9>/

Sweden, for instance, which has recently introduced further regulatory measures relating to drones which also relate to privacy issues.[61]

The aviation regulator, the Civil Aviation Safety Authority (CASA), has acknowledged the privacy concerns that drones engender, but views privacy as an area outside of its remit, and instead has claimed that these privacy issues are within the powers of the federal Privacy Commissioner.[62] So far, the Privacy Commissioner has not issued any official Guidance as to how Australian data privacy laws might apply to drone use. This contrasts with its UK counterpart, the Information Commissioner's Office, which updated its Guidance to CCTV operators to include advice on drones, including practical steps to implementing privacy by design and providing information to passers-by about drone use in a particular area.[63]

As to how current Australian privacy laws (including data privacy laws as detailed above) apply to drones, Butler has considered this point in detail.[64] He has concluded that 'the current Australian legal landscape regarding personal privacy is an uneven patchwork' and that when 'viewed through the prism of a specific context, such as the potential for invasions of privacy by using cameras mounted on UAVs… the many nuances of these laws can be made apparent and deficiencies laid bare'.[65] Butler considers that the surveillance devices legislation in the Northern Territory and Western Australia are best designed to address privacy invasions from civilian aerial drone use, as they prohibit the use of 'surveillance devices' to record 'private activity', defined as 'activity carried on in circumstances that may reasonably be taken to indicate the parties to the activity desire it to be observed only by themselves'.[66]

One large impediment to the application of the federal *Privacy Act* and the APPs to civilian drone activity is the threshold requirement for private sector organisations to have a turnover of more than AU$3 million per year. Thus much individual and small and medium enterprise use of drones would exclude APP application. However, in certain circumstances, other laws such as anti-stalking laws and trespass to property laws may apply to civilian drone activity which infringes individual privacy.

[61] ABC News, 'Sweden places ban on drone filming without surveillance permit' (24 October 2016) <http://www.abc.net.au/news/2016-10-24/sweden-bans-drone-cameras/7959108>.

[62] See: Australian Government Civil Aviation Safety Authority, *Flying drones/remotely piloted aircraft in Australia* <https://www.casa.gov.au/aircraft/landing-page/flying-drones-australia>. However, as will be seen below, this is a problematic statement given the various APPs exemptions e.g. for individuals and SMEs, and the fact that the federal Privacy Commissioner only has powers vis-à-vis data privacy issues rather than the full spectrum of privacy issues e.g. around behavioural privacy problems caused by drones as identified by Clarke. See: Roger Clarke, 'The regulation of civilian drones' impacts on behavioural privacy' (2014) 30(3) *Computer Law & Security Review* 286.

[63] UK Information Commissioner's Office, *In the picture: A data protection code of practice for surveillance cameras and personal information* (2015) < https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>.

[64] Desmond Butler, 'The dawn of the age of the drones: an Australian privacy law perspective' (2014) 37(2) *UNSW Law Journal* 434.

[65] Ibid at p. 469.

[66] *Surveillance Devices Act 2007* (NT) s. 4.

Police or military drone activity in Australia is likely to either be carried out by one of the security agencies which are exempted from the *Privacy Act*'s application, or fall within 'enforcement activities' which permit the collection and use of individuals' personal data within the APPs. The federal *Surveillance Devices Act* (Cth) 2004 also permits some agencies including the Australian Federal Police to use 'optical surveillance devices' without needing to obtain a warrant, which would include drones, and this authorisation is mirrored in the state-level surveillance device laws. Indeed, Molnar and Parsons have argued that '[t]he legal permissiveness for Australian police or military to deploy UAVs creates expansive conditions for the aerial surveillance of Australian citizens'.[67]

There has been some parliamentary consideration in Australia of the use of drones. The House of Representatives Standing Committee on Social Policy and Legal Affairs issued a report in July 2014 following its inquiry into air safety and privacy aspects of drones.[68] The report included various recommendations for the Australian Government:

- introduce legislation that would protection against 'privacy-invasive technologies';
- consider giving effect to the creation of a tort of serious invasion of privacy regarding the risks posed by drones;
- harmonise Australian state and territory-level laws on surveillance devices;
- consider an assessment of the adequacy of internal practices and procedures of Australian law enforcement agencies using drones for surveillance purposes;
- initiate action to harmonise appropriate and approved drone use by law enforcement agencies at the federal and state levels in Australia; and
- coordinate with CASA and the Australian Privacy Commissioner to review the adequacy of privacy and air safety law and regulation regarding drones.

At the time of writing, the Australian Government has not put these recommendations concerning privacy into practice. The only regulatory action as regards drones in the meantime has been the CASA rule reforms, which have only involved air safety issues and have essentially been a deregulatory move. There was, however, discussion of an Australian Senate Inquiry being launched into drone issues in late 2016, although reports suggest that its focus will be on air safety and potential industrial applications of drones in agricultural, as opposed to privacy.[69] This inquiry has indeed been launched, and while its terms of reference frame the inquiry within the notion of safety, the relationship between aviation safety and privacy protection is explicitly mentioned.[70] A report is due coming out of this inquiry in late 2017.

[67] Adam Molnar and Christopher Parsons, 'Unmanned Aerial Vehicles (UAVs) and Law Enforcement in Australia and Canada: Governance Through 'Privacy' in an Era of Counter-Law?' in Randy Lippert, Kevin Walby, Ian Warren and Darren Palmer (eds), *Security, Surveillance and Law in Comparative Context* (Palgrave 2016).

[68] Parliament of Australia, *Eyes in the Skies: Inquiry into drones and the regulation of air safety and privacy* (2014) <http://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Drones/Report>.

[69] ABC News, 'Drones set to come under scrutiny in Senate inquiry' (12 October 2016) <http://www.abc.net.au/news/2016-10-12/inquiry-into-the-use-of-drones/7923834>.

[70] Parliament of Australia Senate Standing Committees on Rural and Regional Affairs and Transport, *Regulatory requirements that impact on the safe use of Remotely Piloted Aircraft Systems, Unmanned Aerial Systems and associated systems* <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Rural_and_Regional_Affairs_and_Transport/Drones>

At the same time, privacy concerns regarding drone use in Australia are becoming more prominent, with reports that drones have been hovering over female sunbathers on Australian beaches and flying over a celebrity's private property.[71] The Australian Associated for Unmanned Systems, the country's main industry group for unmanned systems, has also called for a prohibition on the use of drones to record private activity, similar to the Swedish ban.[72]

It remains to be seen whether this latest inquiry results in any regulatory action being taken which would encompass greater privacy protections vis-à-vis the use of drones. Yet the fact that the Australian Government has not acted on the 2014 recommendations detailed above does not paint an optimistic picture for any reforms to accommodate the privacy concerns implicated by drones being implemented in the near future. However, there have been some small-scale measures taken against drones at the local level, with some local governments and national prohibiting the recreational use of drones in the areas under their control.[73]

Thus, the privacy implications of drones are barely addressed by existing legislation and regulation in Australia. Again, pre-existing problems with the privacy framework are exposed, including exemptions for small businesses and individuals, and law enforcement and security activities. Again, individuals are also not empowered to enforce their privacy rights via the courts so cannot curtail excessive uses of drones which infringe their privacy by law enforcement and security agencies. This leads to the Australian privacy approach to drones being a further situation of counter-law, where legislation largely permits the use of drones and data-gathering, but where the scope of such sweeping permissions in practice is problematic from a rule of law and civil liberties perspective in not constraining executive power to engage in mass surveillance of the population.[74]

3.3 Driverless cars

A third, emerging area of autonomous, intelligent machines in Australia are autonomous vehicles, more popularly known as 'driverless cars'. Given the long distances in Australia, and the car-based nature of much transportation, driverless cars may have significant popular appeal in such a country where people spend many hours on the road. Accordingly, it has been reported that Australia is one of the world's

[71] Kieran Gair, 'Privacy concerns mount as drones take to the skies' *Sydney Morning Herald* (12 December 2015) <http://www.smh.com.au/digital-life/consumer-security/privacy-concerns-mount-as-drones-take-to-the-skies-20151208-glijvk.html>

[72] See: Andy Kollmorgen, 'Drones and Australian law' *Choice* (10 October 2016) <https://www.choice.com.au/electronics-and-technology/gadgets/tech-gadgets/articles/drones-and-privacy-rights>.

[73] Brett Williamson, 'Flyers beware: Councils clamp down on use of drones and model planes in public places' (20 March 2017) < http://www.abc.net.au/news/2017-03-20/councils-clamp-down-on-use-of-drones-in-public/8369020>

[74] Molnar and Parsons, supra n67.

first markets to develop and test this innovative technology.[75] The state of South Australia has passed laws permitting trials of driverless vehicles on public roads, and is also the location of the first test of an autonomous vehicle in the Southern Hemisphere.[76] A Tesla executive has also claimed, perhaps somewhat hyperbolically, that all cars on Australian roads will be driverless by 2030.[77]

Similarly to drones, driverless cars are not a technology which inherently raise privacy issues. Yet their implementation has so far involved the fitting of sensors to gather information about the vehicle's surrounding environment, which of course can and does include gathering information about individuals operating in that environment. Furthermore, assuming an individual is within the driverless car, tracking technology will also gather information about that individual's geographical location and where she is travelling from and to, thus generating more personal information about that individual.[78] Issues also arise when driverless vehicles are integrated into sensor-laden 'smart cities', amplifying the privacy concerns.[79] Tranter has acknowledged that these data privacy concerns about driverless cars are relevant to the Australian context as well as elsewhere.[80] Indeed, at the current time in Australia, data is increasingly being captured and collected in vehicles currently on the roads and exported to manufacturers, insurance operators, etc.[81] It is likely that this trend will intensify with the introduction of driverless cars.

As far as consideration of the regulatory risks posed by driverless cars goes, in addition to South Australia, a joint New South Wales Standing Committee on road safety released a report in September 2016 on driverless vehicles and road safety.[82] The Committee made a number of Recommendations concerning road safety and the desirability of a harmonised national approach to driverless cars. However, the Committee did acknowledge privacy and data issues arising from driverless cars and the data systems which they utilise. It considered that the APPs would likely apply to driverless cars if they are found to generate personal information and the aforementioned surveillance device laws at federal and state levels. However, questions remain as to whether certain types of data generated by driverless

[75] See: Jennifer Dudley-Nicholson, 'Australia in front sear for driverless cars, with development lab and public test drives' *News.com.au* (8 July 2016) <http://www.news.com.au/technology/australia-in-front-seat-for-driverless-cars-with-development-lab-and-public-test-drives/news-story/ffcf949cceecd65117193b182380efaa>

[76] Premier of South Australia news release, 'SA becomes first Australian jurisdiction to allow on-road driverless car trials' (31 March 2016) <http://www.premier.sa.gov.au/index.php/stephen-mullighan-news-releases/337-sa-becomes-first-australian-jurisdiction-to-allow-on-road-driverless-car-trials>

[77] See: Sophie Vorrath, 'All Cars On Australian Roads Will Be Driverless By 2030: Telstra Exec' *Renew Economy* 1 August 2016 <http://reneweconomy.com.au/all-cars-on-australian-roads-will-be-driverless-by-2030-telstra-exec-33821/>

[78] Dorothy Glancy, 'Privacy in Autonomous Vehicles' (2012) 52 *Santa Clara Law Review* 1171.

[79] See: Lilian Edwards 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Perspective' (2016) 2(1) *European Data Protection Law Review* 28; Liesbet van Zoonen 'Privacy concerns in smart cities' (2016) 33(3) *Government Information Quarterly* 472.

[80] Kieran Tranter, 'The Challenges of Autonomous Motor Vehicles for Queensland Road and Criminal Laws' (2016) 16(2) *QUT Law Review* 59.

[81] See, e.g., Choice, New Car Retailing Industry Market Study, submission tot eh Australian Competition and Consumer Commission (18 November 2016) <https://www.accc.gov.au/system/files/CHOICE.pdf>

[82] Parliament of New South Wales Joint Standing Committee on Road Safety (Staysafe), *Driverless Vehicles and Road Safety in NSW* Report 2/56 (September 2016).

cars would constitute 'personal information' for the purposes of the *Privacy Act* and APPs. The NSW Committee did acknowledge 'outstanding issues' with the existing regulatory framework for privacy in Australia, including the lack of harmonisation of some areas of law, and the *Privacy Act* exemptions for small businesses and law enforcement activities.

This was followed in late 2016 by a comprehensive report from the National Transport Commission (NTC) Australia on regulatory reforms for autonomous vehicles.[83] The report's overall recommendation is that 'the Commonwealth and state and territory governments support on-road trials, remove unnecessary legal barriers, and provide for the safe operation of automated vehicles'.[84] The NTC has identified privacy concerns as a potential barrier to the take-up of driverless cars in Australia, asserting that 'Australia should aim for a high level of privacy protection for drivers and occupants of automated vehicles'.[85] The NTC acknowledges that the *Privacy Act* and APPs must be complied with, and does not recommend any changes to be made right now to the legal framework, but does consider the scenarios in which vehicle data may be accessed, and the status of the parties including insurers, parties to civil proceedings, consumers and government agencies which may wish to access it.

In order to minimise some of the data privacy risks posed by driverless cars, the NTC considers that vehicles should, wherever possible, adopt a 'privacy by design' approach and not generate 'personal information' about individuals, and that users should have the ability to use driverless cards without having to give over their personal information wherever possible.[86] The caveat 'wherever possible' is important here, as in practice it entails that these measures do not constitute a strong prohibition on vehicle manufacturers and software providers to implement systems which actually do minimise data collection and so may render them merely rhetorical overtures to data privacy concerns in reality.

The NTC also recognises government access to vehicle data as a privacy risk, and explicitly acknowledged the *Privacy Act*'s 'low threshold' to exempt enforcement activities from the APPs.[87] For the NTC, this situation may require future privacy protections being legislated to restrict government access to data, although it still believes that current data privacy protections are adequate for now. Such future legislation could, though, address accessing data to support crash analysis, network performance monitoring and infrastructure planning.[88]

In the meantime, one of the report's Recommended Actions is for the NTC to develop options to manage government access to data produced by automated vehicles in a way that balances interests in road safety, network efficiency and the efficient enforcement of traffic laws with sufficient privacy

[83] National Transport Commission Australia, *Regulatory reforms for automated road vehicles* (Policy Paper, November 2016).

[84] Ibid at p. 8.

[85] Ibid at p. 17.

[86] Ibid at p. 70.

[87] Ibid at p. 71

[88] Ibid at p. 73.

protection for the users of driverless cars, and this work is to be conducted from late 2017 until late 2018.

The fact that privacy issues are featuring in Australian considerations of driverless cars is to be welcomed, since in other jurisdictions, notably the US, the regulatory focus has been almost entirely on physical road safety issues, with the exception of California which has drafted regulations including information privacy provisions.[89] The fact too that the broad exception for government agencies' enforcement activities from the APPs has been identified as potentially problematic is also to be welcomed – and may avert the regulation of driverless cars from becoming another counter-law situation - although the NTC's view that the current privacy framework is adequate is certainly a more questionable opinion, in light of the earlier discussion in this article. However, the lack of strong data minimisation measures remains problematic from a privacy perspective. There are also outstanding issues around whether data collected by driverless cars would fall into the Privacy Act's definition of 'personal information', particularly after the uncertain consequences of the recent Australian Federal Court decision in *Privacy Commissioner v Telstra*.[90]

Since driverless cars are not yet widespread in Australian roads, the overall data privacy risks at the current time may not be high, but should these vehicles be deployed on a greater scale than is the case now, and should the legal framework not be modified from its current form, then the potential infringement of Australians' privacy may be significant.

4. Analysis

These three examples of emerging and emerged autonomous technologies and the Australian legal and policy response to them can be used to judge the extent to which privacy concerns regarding the personal information generated by and about individuals using these technologies are acknowledged and addressed.

From the case studies, certain themes can be discerned as running through this discussion.

Firstly, privacy concerns and interests are acknowledged in all three of the case studies, in the government and parliamentary reports and impact assessments, as well as the academic and general commentary. Indeed, these technologies expose certain deficiencies with existing privacy laws, which include:

- the fact that businesses with less than AU$3 million in turnover are excluded from the APPs;
- the law enforcement exemptions and carve-outs in the *Privacy Act*;

[89] Ellen Goodman, 'Self-driving cars: overlooking data privacy is a car crash waiting to happen' *The Guardian*, (9 June 2016) <https://www.theguardian.com/technology/2016/jun/08/self-driving-car-legislation-drones-data-security>

[90] Anna Johnston, 'Data, Metadata & Personal Information: A Landmark Ruling From The Federal Court' (2017) 31 *Law Society of NSW Journal* 82, 82–3.

- the lack of possibility for individuals to take privacy infringement instances to the courts themselves, or to challenge government powers which are disproportionate and/or non-necessary to law enforcement and security aims.

As can be seen in the discussion above, some of these deficiencies in the existing state of the law have been acknowledged in official documentation, such as the Parliamentary inquiry into drones, and then in the NTC's report on autonomous vehicles. Yet so far this acknowledgement has not translated into legal or regulatory action to remedy the deficiencies. For the time being, it seems that Australian privacy laws' largely permissive natures entails that they fall within Lippert and Walby's characterisation as 'less a barrier to government power, and more an instrument of its exercise', facilitating a wide scope of conduct for agencies through the APP's exceptions and carve outs.[91]

While legal and regulatory action can be time-consuming, the fact that the CASA regulations relating to drones have been recently updated suggests the problem, at least for that technology, is not the slow-moving nature of the legislative and regulatory system, but in fact a lack of political and regulatory will to effect changes that would protect individual privacy.

The fact that privacy concerns are acknowledged by the road authorities in their consideration of driverless cars is to be welcomed, given the relatively early stage of deployment. The possibility thus remains that these concerns may be taken into account in any subsequent regulatory measures. However, if the experience with drones is to be followed, then all that may happen is that these privacy concerns and risks are acknowledged, but then nothing is done to address them.

Perhaps most concerning, though, is the regulatory side-stepping that the introduction of Australia's facial recognition Capability involves given the seeming lack of federal legislation being sought to introduce it. If such large data sharing can take place among law enforcement and security agencies without the need for federal parliamentary scrutiny, more than just privacy concerns are raised.

The lack of a constitutional or enforceable fundamental right to privacy in Australia also causes a sharp divergence between the emerging Australian situation around these technologies, and what would likely be permissible in European Union and Council of Europe countries.

5. Conclusion

This article has examined three emerging technologies using some form of automation – facial recognition, drones and driverless cars – and the legal, regulatory and policy discussions surrounding their privacy implications in Australia. This article has also examined to what extent the laws governing these developments in Australia are adequate in addressing privacy concerns that these technologies

[91] Randy Lippert, and Kevin Walby, 'Governing Through Privacy: Authoritarian Liberalism, Law, and Privacy Knowledge' (2016) 12(2) *Law Culture and the Humanities* 329.

involve. The conclusion is that despite these privacy concerns being acknowledged officially, limited to negligible action has actually been taken to address them. The emergence of driverless cars may yet involve stronger measures being adopted which protect privacy and personal data, but the experience with drones does not bode well for such an outcome.

For some time Australia has needed an overhaul of its data privacy laws in order to bring them up to date with global best practice and to address privacy concerns from emerging technologies and practices. The more recent updates to the *Privacy Act* introducing the Australian Privacy Principles have not achieved this objective, and so can be viewed as a missed opportunity. Instead, the unharmonised surveillance device laws and the weak *Privacy Act* constitute a problematic patchwork of laws with, in the case of the APPs, inadequate enforcement mechanisms. This situation is compounded by a lack of a constitutional right to privacy (and a lack of many other constitutional rights). So, despite being a country eager to adopt new technologies, the corresponding legal and regulatory protection of privacy vis-à-vis these technologies is weak and outdated.

In sum, while automated technologies are increasingly available in Australia and attracting the interest of public and private bodies, and individuals, alike, the laws surrounding them are not fit for purpose when it comes to privacy and data protection. Privacy also remains an important value in Australia for the Internet of Things era.[92] Thus, if it is true that more and more machines and functions will be automated in the coming years, this area of law that requires urgent attention from legislators and policymakers in order to provide an approach which balances the benefits of innovation with citizens' civil liberties and human rights.

[i] This article forms one of the outputs of the Queensland University of Technology Institute for Future Environments Catapult Research Grant 'Regulating Autonomous Vehicles'.

[92] Megan Richardson, Rachelle Bosua, Karin Clark, Jeb Webb, Atif Ahmad and Sean Maynard, 'Towards responsive regulation of the Internet of Things: Australian perspectives' (2017) 6(1) *Internet Policy Review.*