4

Drones and privacy

4.1 Remotely piloted aircraft (RPAs) have the potential to pose a serious threat to Australians' privacy. They can intrude on a person's or a business's private activities either intentionally, as in the case of deliberate surveillance, or inadvertently in the course of other activities like aerial photography, traffic monitoring or search and rescue. As RPAs become cheaper and more capable, and as the instruments they carry become more sensitive, they will provide governments, companies and individuals with the cost-effective capability to observe and collect information on Australians, potentially without their knowledge or consent.

4.2 This chapter will examine Australia's existing regulatory environment in relation to RPAs and privacy and examine issues to be taken into consideration to ensure that Australian privacy laws adequately address the risks posed by RPAs.

A 'fractured landscape' – RPAs and privacy laws

4.3 Australia's privacy regime is complex. There is a range of Commonwealth, State and Territory statutes and common law principles. However, the laws are complex, at times outdated by emerging technology, and significant variations exist between jurisdictions. The Committee has heard Australia's privacy regime variously described as a 'fractured

landscape', or a 'patchwork of laws'.[1] The following section provides a brief overview of the legal principles relevant to RPAs and privacy.

4.4 Just as it is critical to ensure that RPA use does not compromise public safety, so RPA use should not compromise the privacy of individuals or businesses. The capacity of RPAs to enter private property, to travel unnoticed, and to record images and sounds which can be streamed live create significant opportunities for privacy breaches.

4.5 Research by the Australian Privacy Commissioner shows that Australians' concern for their privacy has remained high in an environment where there are a growing number of ways in which it can be breached. Mr Timothy Pilgrim, the Privacy Commissioner, told the Committee that:

> our community research, that we undertake every three to four years, consistently shows that the community remains concerned about what is happening with their personal information. The community is concerned to make sure that there are protections in place for that personal information. So rather than seeing it becoming an issue that is dying, as some commentators have said in the past, it is actually a constant within the community.[2]

4.6 Like any new technology, RPAs have both positive and negative applications. In considering how to address the potential privacy issues RPA use might raise, Mr Pilgrim said:

> With such a new technology, the question comes down to how its use is going to be regulated. What are the ways in which it can be regulated so that we can still achieve the benefits that the technology can bring, at the same time as making sure that people have a right of recourse or a remedy if they believe their privacy has been invaded by misuse of those technologies?[3]

4.7 The Commonwealth *Privacy Act 1988* (the Privacy Act) provides a number of privacy protections to the Australian public. It is intended to ensure Australians are provided with information on, and some degree of choice about, the collection and use of their personal information by governments and large businesses.

4.8 The Privacy Act sets out thirteen privacy principles which govern how organisations should collect information, how they should manage it, and the circumstances under which it can be disclosed. Ms Angeline Falk of

1 Committee Hansard, 21 March 2014, p. 4; Committee Hansard, 28 February 2014, p. 37.

2 Committee Hansard, 28 February 2014, p. 34.

3 Committee Hansard, 28 February 2014, p. 34.

the Office of the Australian Information Commissioner described the Act as 'a set of principles that focuses on transparency in the way in which personal information is collected'.[4]

4.9 The Privacy Commissioner, Mr Pilgrim, told the Committee that:

> The federal Privacy Act applies to most Australian government agencies at the federal level and many private sector organisations. It does set an overarching set of principles that those entities must comply with in how they collect, use, disclose, provide access to and secure personal information as part of their roles.[5]

4.10 However, the Privacy Act does not provide Australians with comprehensive privacy protections. As Mr Andrew Walter from the Attorney-General's Department (AGD) noted '[t]he Privacy Act does not apply to the collection and use of personal information by private citizens and does not provide overarching privacy protection for the individual'.[6]

4.11 The Act contains exemptions for a number of groups. As such, the Privacy Commissioner noted that small businesses (with an annual turnover of less than $3 million), political organisations, media organisations, and individual citizens acting in the course of their personal, family or household affairs are not subject to the privacy principles.[7]

4.12 In addition to the limitations to the Privacy Act created by its exemptions, the Act is not intended to protect against intrusions into Australians' private seclusion. Dr Roger Clark from the Australian Privacy Foundation said:

> we identify privacy of personal behaviour … as the interest that people have in not being intruded upon by undue observation or interference with their activities, whether or not data is collected—after which it would then move into another space.
>
> When we look at the Privacy Act … it is all but irrelevant to behavioural privacy protection. It was designed that way; it was designed to deal with data protection only.[8]

4.13 Therefore the Privacy Act offers substantial privacy protections in certain circumstances, but there are a number of situations in which it may not protect Australians against the invasive use of RPAs.

4 Committee Hansard, 28 February 2014, p. 35.
5 Committee Hansard, 28 February 2014, p. 34.
6 Committee Hansard, 20 March 2014, p. 1.
7 Committee Hansard, 28 February 2014, p. 34.
8 Committee Hansard, 28 February 2014, p. 39

4.14 Mr Pilgrim noted that many States and Territories have privacy laws of their own, but that most of these are limited in much the same way as the Federal Act:

> there are a series of privacy laws within a number of the states and territories. These generally apply to the activities of state and territory government agencies as well, and tend to be limited to those entities.[9]

4.15 There are a range of additional laws that may protect against invasive or inappropriate use of RPAs. For example, each State and Territory has legislation that may make it illegal in certain circumstances to use a surveillance device to record or monitor private activities or conversations via listening devices, cameras, data surveillance devices or tracking devices.[10]

4.16 The Commonwealth *Surveillance Devices Act 2004* regulates the lawful use of surveillance devices by Federal law enforcement agencies but, according to Ms Catherine Smith from AGD, 'does not contain prohibitions on the use of surveillance devices'.[11] Those prohibitions are found in the relevant State and Territory statutes, which, according to AGD, are inconsistent:

> These prohibitions on surveillance devices are found in the laws of the states and territories. We understand that the states and territories approach their surveillance devices prohibition laws differently. Also, the committee has heard that not all states have prohibited the use of all kinds of surveillance devices.[12]

4.17 The Committee has heard that, in addition to varying between jurisdictions, in some cases these laws are outdated. According to Professor Des Butler:

> There are four of our jurisdictions that have surveillance devices laws. Four of our jurisdictions have listening devices statutes that are simply not appropriate for the 21st century, and they really do

9 Committee Hansard, 28 February 2014, p. 35.

10 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Discussion paper*, March 2014, p. 41. The Acts are: *Listening Devices Act 1992* (ACT); *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act* (NT); *Invasion of Privacy Act 1971* (Qld); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA).

11 Committee Hansard, 20 March 2014, p. 2.

12 Committee Hansard, 20 March 2014, p. 2.

> need to have a look at what they are doing. Even within the surveillance devices statutes they are inconsistent.[13]

4.18 AGD informed the Committee that the use of RPAs as surveillance devices is already regulated, since they fall within the definition of 'optical surveillance device' or 'listening device' in the Commonwealth Surveillance Devices Act.[14] However, Ms Catherine Smith from AGD noted that the Surveillance Devices Act was written to cover the use of surveillance devices physically attached to property, and did not envisage the use of mobile surveillance systems like RPAs. Ms Smith said that 'it would be of benefit' to review this legislation 'in the future as technology develops'.[15]

4.19 In addition to surveillance laws, some States and Territories have laws which make photography for indecent purposes a criminal offence, or which prohibit observing or filming a person in a private place or when that person is engaging in a private act. These laws, though they were introduced with the intention of protecting against child abuse or voyeurism, may nonetheless provide limited privacy protection against invasive RPA use.[16]

4.20 There are also a range of State and Territory stalking and harassment statutes that may be used to protect against privacy breaches caused by RPA users, though again these are not consistent across jurisdictions.

4.21 Finally, there are a number of common law torts which may also be relevant to RPA use. For example the torts of trespass, nuisance or breach of confidence may be available to people whose privacy has been invaded by RPAs, depending on the circumstances.

4.22 However, given that these principles emerged well before the development of RPA technology and in response to substantially different circumstances, they do not provide reliable protection against inappropriate RPA use.[17]

---

13 Committee Hansard, 21 March 2014, p. 4.

14 Committee Hansard, 20 March 2014, p. 2.

15 Committee Hansard, 20 March 2014, pp. 3-4.

16 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Discussion paper*, March 2014, pp. 41-42.

17 Committee Hansard, 28 February 2014, p. 37; Committee Hansard, 21 March 2014, pp. 3-5, p. 12.

Possible shortcomings of the current privacy regime

4.23 The previous section briefly outlined the range and complexity of the privacy laws that may apply in relation to RPAs. The Committee heard that this complexity has a number of unfortunate effects – in particular that: it may hinder access to remedies for breaches of privacy; RPA operators may face difficulties in complying with the law; and gaps in the law may exist which could need to be addressed. The following section discusses these concerns.

Uncertainty and access to remedies

4.24 The complexity of privacy laws generates considerable uncertainty as to the law's scope and effect. Evidence suggested that Australia's current privacy laws may not be sufficient to cope with the explosion of technologies that can be used to observe, record and broadcast potentially private behaviour. The Privacy Commissioner told the Committee that:

> there are a number of laws that, in one form or another, do regulate the handling of personal information. First of all, what I do not think we do have—and I would be the first to admit this from my position—is a completely clear understanding of whether those laws as they currently exist are going to do the job, or whether, because of the patchwork nature of some of those laws, there are going to be gaps which need to be filled when we take into account how these new technologies can be used within the community.[18]

4.25 In addition, Professor McDonald from the ALRC argued that lack of uniform laws negatively affects Australians' privacy protections:

> In terms of the surveillance laws, that has been a very common response we have had from people—that uniformity across state boundaries is very highly valued. At the moment the lack of uniformity means that there is insufficient protection of people's privacy, because people do not know what is against the law and what is not.[19]

4.26 In the same vein, Professor Des Butler noted that the lack of clarity in the law makes it more difficult for people who feel their privacy has been invaded to complain:

18 Committee Hansard, 28 February 2014, p. 35.

19 Committee Hansard, 28 February 2014, p. 38.

> when you look at these various laws, it is a complex and messy thing anywhere ... That needs to be addressed and then, in addition, people need to be able to have some understandable means of complaint—easy means of complaint—when these things start to take off, so to speak.[20]

4.27 Simple and clear ways to seek redress are particularly important in relation to privacy, since the very nature of privacy breaches may make people reluctant to seek remedies. As Professor Butler noted:

> part of the problem with any sort of breach of privacy is that a person who then seeks to get some sort of reparation for breach of privacy in fact breaches their own privacy again. So people may be reluctant to complain simply because it reignites the whole deal.[21]

4.28 While these issues are not specific to RPAs, the capability and increased use of RPAs test the privacy regime by increasing the likelihood of privacy breaches.

Burden on industry

4.29 In addition to the difficulties individuals may face in seeking remedies for inappropriate RPA use, Australia's complex privacy environment may also cause problems for RPA operators. Dr Reece Clothier, speaking for the Australian Association of Unmanned Systems, argued that in addition to privacy protections being inadequate industry faces a substantial regulatory burden:

> we believe there is not much protection for the rights of the individual in terms of privacy in this country at the moment and that there is a patchwork of legislation across this country that is very difficult to navigate from the perspective of industry.[22]

4.30 Professor McDonald noted the difficulties faced in particular by media organisations:

> it is also insufficient protection for organisations like those in the media, because they find it difficult to know what they are doing, and if they operate—as all media now do—across state boundaries, they can be breaking the law in one state and cross

20 Committee Hansard, 21 March 2014, p. 8.

21 Committee Hansard, 21 March 2014, p. 8.

22 Committee Hansard, 28 February 2014, p. 41.

> over a boundary and they are not breaking the law. So that clearly makes law much more complex.[23]

4.31 Journalist Mark Corcoran likewise highlighted the difficulties faced by media organisations as a result of Australia's privacy patchwork:

> There is a whole range of different laws in different states. That is where I think some of the media lawyers get sent grey before their time, trying to figure that out on a state-by-state basis.[24]

4.32 In this environment, the Committee heard that some RPA businesses and industry groups have adopted voluntary privacy policies. Insitu Pacific, which as a Boeing subsidiary is one of Australia's largest RPA companies, has done so. Mr Damen O'Brien, Insitu's Senior Contracts Manager, said that:

> Insitu Pacific understands and gets that there is a real concern out there about privacy … we have a privacy policy. It is a set of principles which align very closely with the privacy act and which deal with what we understand privacy to be.[25]

4.33 Mr Brad Mason from the Australian Certified UAV Operators Association (ACUO) said that ACUO was in the process of developing a privacy policy. Mr Mason said that many of ACUO's members already have privacy policies in place:

> A lot of our members already adopt a privacy policy. If it is deemed that privacy may be an issue, then we will approach the people who may be affected and at least give them an opportunity to have their say, or voice their concerns or opinions before we actually put an aircraft in the air.[26]

4.34 The implementation of voluntary codes of conduct and privacy policies by commercial RPA operators is a commendable response to public concern about the potential for invasive RPA use. However, regulatory change may ultimately be necessary to address the issue of privacy-invasive technologies.

---

23 Committee Hansard, 28 February 2014, p. 38.

24 Committee Hansard, 28 February 2014, p. 31.

25 Committee Hansard 21 March 2014, pp. 19-20.

26 Committee Hansard, 28 February 2014, p. 4.

Gaps in the law

4.35 Existing laws may not be sufficient to cope with the specific privacy issues widespread RPA use might raise. For example, many State surveillance acts may not provide for inadvertent recording of private behaviour.[27] This could create uncertainty for RPA operators in a range of contexts – for example aerial photography, survey or emergency management.

4.36 In relation to this Mr Rodney Alder, representing the Australasian Fire and Emergency Service Authorities Council, said that:

> my understanding at least with some of the state legislation … [is] that the offence is actually committed at the time of the recording … One of the most probable applications for UAVs is rapid damage assessments. So immediately after a fire or some other incident, it is a niche UASs can clearly operate in. There is a potential for inadvertent privacy breaches in that situation.[28]

4.37 In addition, the Committee notes that Australia's existing surveillance laws were written before the development of current RPA technology. While in some cases they are written in technology neutral language, and therefore may still apply to the use of RPAs, widespread RPA use and their developing capabilities may nonetheless require a reassessment of current laws.

4.38 For example, while the use of listening devices is tightly regulated, according to the Commonwealth Surveillance Devices Act 2004, police may use RPAs as optical surveillance devices without a warrant so long as they do not enter onto premises without permission, or interfere with any vehicle or thing without permission.[29]

4.39 As such, it was suggested that law enforcement agencies could deploy cheap and widespread aerial surveillance capability without requiring a warrant. The Committee notes that both the AFP and the Queensland Police have indicated that at present they have no plans to use RPAs for surveillance purposes.[30] While these responses are reassuring, the regulatory gap remains a concern. This is an issue where technology appears to have surpassed situations envisaged when the relevant regulations were drafted, and confirms the need for regulatory review.

---

27 Committee Hansard, 28 February 2014, p. 5.

28 Committee Hansard, 28 February 2014, p. 19.

29 Surveillance Devices Act (2004) (Cth), section 37.

30 Committee Hansard, 28 February 2014, p. 27; Committee Hansard, 21 March 2014, p. 2.

Private surveillance

4.40 While many of the issues raised by roundtable participants highlight problems that may arise in the future, the Committee notes that RPA use by animal rights groups has already brought the complexities of RPA use and privacy into focus. At its first roundtable, the Committee heard debate about the extent to which Australia's privacy laws should protect farmers from unauthorised use of RPAs to monitor farming facilities.

4.41 The Committee is aware of media reports that animal protection groups have used RPAs to monitor agricultural facilities without their owners' consent, with the intention of exposing animal cruelty or evidence of inaccurate claims about farms' free-range status.[31]

4.42 Some farming groups do not consider the use of RPAs by activist groups to be appropriate. Ms Deborah Kerr of Australian Pork Limited said that:

> our view would be that it is not the role of activist organisations to actually undertake those activities. We would prefer to see the appropriate regulators who are accorded the relevant authority to investigate those matters actually able to undertake those activities. We certainly would not be supporting activists to be undertaking drone activities above our producers' properties.[32]

4.43 Ms Kerr noted that that many farmers consider their production facilities to be private spaces:

> In fact, many of them would feel similar to what homeowners feel if they had been burgled: they would feel that they had been traumatised and that they had been invaded; they would feel dirty and that their staff had been put at risk. So dealing with the issue of privacy is a high priority.[33]

4.44 Voiceless, an Australian think tank which aims to raise awareness of animal cruelty, told the Committee that undercover investigations have revealed animal neglect, cruelty and illegal activity on some farms in the past. RPA surveillance could help reduce that activity:

> surveillance assists with reducing the rate of contravention of animal welfare regulations in our view, and it can be used not only by animal protection groups but also by enforcement arms like the

31 See, for example, S Murphy, "Animal Liberation activists launch spy drone to test free-range claims", *ABC News*, 30 August 2013, http://www.abc.net.au/news/2013-08-30/drone-used-to-record-intensive-farm-production/4921814, viewed 30 June 2014.

32 Committee Hansard, 28 February 2014, p. 45.

33 Committee Hansard, 28 February 2014, p. 45.

> police or the RSPCA in each state or territory, or the Animal Welfare League in New South Wales, to monitor and therefore enforce animal protection legislation.[34]

4.45 Academic Mr Geoff Holland noted that surveillance of factory farming facilities has been effective in exposing illegal activity in the past:

> A number of prosecutions of farms where there has either been mistreatment of animals or prosecutions under the Australian Consumer Law, the Trade Practices Act, has arisen because of information obtained either through static cameras that have been installed or, more recently, through the use of drones, particularly in the areas with the ACCC taking action for farmers or producers of both meat and eggs that are claiming that they were free range, or raised under certain conditions, and yet the surveillance showed that that was false.[35]

4.46 The potential of RPAs to unobtrusively gain footage of illegal activities is enormous, and their use is obviously attractive to certain lobby groups. However, as with enforcement agencies, the unfettered use of RPAs to undertake surveillance operations and monitor the activities of an individual or a company is not consistent with the intent of privacy laws.

4.47 If technology has now enabled situations not considered when aspects of privacy and surveillance laws were drafted, then there is a pressing need to review the current regime and its adequacy to respond to RPA use.

Prospects for reform

4.48 The issues outlined above illustrate that RPAs can give rise to significant privacy concerns. However, roundtable participants emphasised that RPAs are just one of many emerging technologies that have the potential to seriously affect privacy in Australia. Any reform of Australia's privacy laws, they argued, should address the issue of privacy without focusing on specific technologies.

4.49 In the first place, the use of RPAs is likely to prove extremely difficult to regulate. CASA's Mr John McCormick noted that if and when large numbers of Australians begin purchasing consumer-level RPAs, CASA is unlikely to be able to regulate their use:

---

34 Committee Hansard, 28 February 2014, p. 22.

35 Committee Hansard, 28 February 2014, p. 45.

> From CASA's point of view, if we now try to do something to say that you cannot operate a lightweight UAV unless you tell us—leaving aside the grey area of the model aircraft—when it becomes something that is commercially viable I would be in a situation of writing of regulation that I know I cannot enforce. That is bad law.[36]

4.50 Further, RPAs are one among a large number of new technologies that may impact on Australians' privacy. Journalist Mr Mark Corcoran noted that while RPAs provide 'phenomenal capability' to media organisations, other new technologies exist which might be used to invade people's privacy:

> this is absolutely a surveillance technology, but I would argue that there are an equal number of other new technologies available that are equally invasive.[37]

4.51 Similarly, Dr Reece Clothier argued that, instead of focusing on the privacy threats posed by RPA use, it is necessary to take a broader view of how privacy is affected by technological advances:

> We need to step away from this idea that it is a specific piece of technology or a specific device and say, 'Let's protect the interests of privacy' … Google Glass is a much more invasive technology that every person is going to be wearing in the next five years. So whether it is drones, Google Glass or the fact that I can collect metadata on your Facebook account and marry that up with your LinkedIn and actually track your movements, it is your personal information … it is an issue much broader than unmanned aircraft.[38]

4.52 The Australian Privacy Foundation argued that, while RPAs give rise to some unique policy and legal problems, they highlight the inadequacies of Australia's current privacy and surveillance laws:

> the biggest problem is not drones per se; drones exacerbate existing massive deficiencies in surveillance law in Australia and … we need to separate out those issues and solve the problems where the problems are.[39]

---

36 Committee Hansard, 28 February 2014, p. 5.
37 Committee Hansard, 28 February 2014, p. 30.
38 Committee Hansard, 28 February 2014, p. 42.
39 Committee Hansard, 28 February 2014, p. 40.

4.53 Dr Clothier also argued that any reform undertaken to address the privacy issues caused by RPAs should be carried out carefully:

> I would hate to see legislation put in place that hamstrings the many beneficial applications of this emerging aviation industry and its flow-on effects for mining, agriculture, surf-lifesaving—everything—through a piece of legislation that is chasing the 0.0003 per cent of people or organisations that will misuse it.[40]

A tort of privacy

4.54 The Committee notes that the Australian Law Reform Commission (ALRC) is conducting an inquiry into serious invasions of privacy in the digital era and has proposed that the Australian Government create a tort for serious invasion of privacy.[41] Such a tort may serve to address some of the gaps and limitations in Australia's existing privacy law.

4.55 The Commission began its inquiry in June 2013 after a referral from then Attorney-General the Hon Mark Dreyfus QC MP. The inquiry's terms of reference require the ALRC to consider the prevention of, and remedies for, serious invasions of privacy in the digital era. The ALRC's inquiry was undertaken in response to:

> the rapidly expanded technological capacity of organisations not only to collect, store and use personal information, but also to track the physical location of individuals, to keep the activities of individuals under surveillance, to collect and use information posted on social media, to intercept and interpret the details of telecommunications and emails, and to aggregate, analyse and sell data from many sources.[42]

4.56 The ALRC released an issues paper on 8 October 2013 and invited submissions from interested parties. After a first round of submissions, the Commission released a discussion paper at the end of March 2014 which contained proposed recommendations. Further submissions, to a total of more than 120, have since been received. The Commission's inquiry has been of considerable breadth and depth.

---

40 Committee Hansard, 28 February 2014, p. 43.

41 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Discussion paper*, March 2014.

42 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Discussion paper*, March 2014, p. 21.

4.57 In its discussion paper, the ALRC proposed the creation of an action in tort for serious invasion of privacy. The proposed tort would be created by a Commonwealth Act and would define two types of fault – intrusion upon a person's seclusion or private affairs, and misuse or disclosure of private information. The tort would be confined to intentional or reckless invasions of privacy, and would only apply where a person had a reasonable expectation of privacy.[43]

4.58 The ALRC further proposed that the cause of action should only be available where the invasion of privacy is determined to be serious, and that the courts should balance a person's right to privacy against competing principles – including freedom of expression (especially freedom of political communication), press freedom, open justice, public health and safety, and national security.[44]

4.59 The ALRC has also proposed that the various pieces of Australian surveillance and workplace surveillance legislation should be harmonised. These changes, if enacted, would address a number of issues with Australia's privacy regime which have been identified in the course of this inquiry.

4.60 The ALRC is required to present its report to the Attorney-General, Senator the Hon George Brandis QC, by 30 June 2014. The Attorney-General has 15 sitting days in which to table the report in Parliament. This would require the report to be released by September 2014. A timetable for a Government response to the ALRC has not been established.

Committee comment

4.61 RPA use raises serious privacy issues for Australians, and the problem will deepen as RPAs become cheaper and the cameras and sensors they carry become more sensitive. Given the ease with which RPAs can be bought locally, or imported, it will be very difficult to enforce regulatory compliance. Media reports indicate that RPAs are already being put to unsafe and potentially invasive uses.

4.62 Given the complexity of Australia's privacy regime, it is likely that the majority of RPA users are unaware of the specific circumstances in which

43 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Discussion paper*, March 2014, pp. 9-10.

44 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era: Discussion paper*, March 2014, pp. 10-11.

their RPA use may breach someone's privacy. The Committee takes the view that steps should be taken to better inform the breadth of RPA users about possible privacy breaches and the need to operate RPAs responsibly.

Recommendation 2

The Committee recommends that the Australian Government, through the Civil Aviation Safety Authority (CASA), include information on Australia's privacy laws with the safety pamphlet CASA currently distributes to vendors of remotely piloted aircraft. The pamphlet should highlight remotely piloted aircraft users' responsibility not to monitor, record or disclose individuals' private activities without their consent and provide links to further information on Australia's privacy laws.

4.63 While it is difficult to prevent the misuse of new technologies, it may be possible to give people who have been the victims of that misuse easier access to justice. The current complexity of Australian privacy law is a burden to these individuals that should be addressed.

4.64 The Committee emphasises that while RPAs pose specific privacy problems, they are just one of many emerging technologies that have privacy implications. Addressing the issues RPA use raises should be part of a broader effort to update Australian privacy law to deal with the gamut of invasive technologies.

4.65 The Committee notes that the ALRC's inquiry into serious invasions of privacy in the digital era is nearing completion. The Committee notes from its discussion paper that the ALRC may recommend the creation of a tort of serious invasion of privacy, and that it may recommend the standardisation of surveillance and harassment laws across jurisdictions. There is a clear need for reforms of this type.

Recommendation 3

The Committee recommends that the Australian Government consider introducing legislation by July 2015 which provides protection against privacy-invasive technologies (including remotely piloted aircraft), with particular emphasis on protecting against intrusions on a person's seclusion or private affairs.

The Committee recommends that in considering the type and extent of protection to be afforded, the Government consider giving effect to the Australian Law Reform Commission's proposal for the creation of a tort of serious invasion of privacy, or include alternate measures to achieve similar outcomes, with respect to invasive technologies including remotely piloted aircraft.

Recommendation 4

The Committee recommends that, at the late-2014 meeting of COAG's Law, Crime and Community Safety Council, the Australian Government initiate action to simplify Australia's privacy regime by introducing harmonised Australia-wide surveillance laws that cover the use of:

- **listening devices**
- **optical surveillance devices**
- **data surveillance devices, and**
- **tracking devices**

The unified regime should contain technology neutral definitions of the kinds of surveillance devices, and should not provide fewer protections in any state or territory than presently exist.

4.66 The Committee notes that law enforcement agencies have stated that at present they have no plans to use RPAs in a surveillance capability. However it is apparent that, given the rate at which RPA technology is developing, Australia's law enforcement agencies will soon have access to cost-effective mass surveillance technology.

4.67 Moreover, evidence to this inquiry has indicated that the Commonwealth Surveillance Devices Act is no impediment to the deployment of that capability by law enforcement agencies. Australia's surveillance laws were not designed with this capability in mind and, in order to protect

Australian citizens' rights and freedoms, the Committee is of the view that the use of RPAs for surveillance should be subject to a rigorous approval process.

Recommendation 5

The Committee recommends that the Australian Government consider the measures operating to regulate the use or potential use of RPAs by Commonwealth law enforcement agencies for surveillance purposes in circumstances where that use may give rise to issues regarding a person's seclusion or private affairs. This consideration should involve both assessment of the adequacy of presently existing internal practices and procedures of relevant Commonwealth law enforcement agencies, as well as the adequacy of relevant provisions of the Surveillance Devices Act 2004 (Cth) relating but not limited to warrant provisions.

Further, the Committee recommends that the Australian Government initiate action at COAG's Law, Crime and Community Safety Council to harmonise what may be determined to be an appropriate and approved use of RPAs by law enforcement agencies across jurisdictions.

4.68 RPAs have introduced privacy and safety issues not conceived of a decade ago. The Committee is aware that the technology of RPAs a decade from now may exceed what we can currently imagine. Given the seriousness of both privacy and air safety and the expected surge in the use of low cost RPAs, the Committee considers it imperative that a forward plan is in place to monitor RPA use and regulation.

4.69 While the current work of CASA and the ALRC is appropriately addressing current issues, a more coordinated approach for the future is required. Further, given the diversity of users and rapid technological change, there must be better coordination in the review and development of privacy and air safety regulation relating to RPAs.

Recommendation 6

The Committee recommends that the Australian Government coordinate with the Civil Aviation Safety Authority and the Australian Privacy Commissioner to review the adequacy of the privacy and air safety regimes in relation to remotely piloted aircraft, highlighting any regulatory issues and future areas of action. This review should be publicly released by June 2016.

Mr George Christensen MP
Chair

8 July 2014