THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

House of Representatives Standing Committee on Social Policy and Legal Affairs

Eyes in the sky

Inquiry into drones and the regulation of air safety and privacy

July 2014 | Canberra



The Parliament of the Commonwealth of Australia

Eyes in the sky

Inquiry into drones and the regulation of air safety and privacy

House of Representatives
Standing Committee on Social Policy and Legal Affairs

July 2014
Canberra

ISBN 978-1-74366-178-9 (Printed version)

ISBN 978-1-74366-179-6 (HTML version)

Contents

APPENDICES

LIST OF TEXT BOXES

Foreword

Australia's Remotely Piloted Aircraft or 'drone' industry is growing rapidly. Increasing numbers of consumers are buying and using drones, and they already play a role in a range of Australian industries, from journalism, cinematography, policing and emergency services, to agriculture, mining and scientific research. They come in a huge range of shapes and sizes, from large fixed-wing craft that look and behave much like aeroplanes right down to tiny multi-rotor helicopters weighing less than a kilogram. Drones are able to do jobs that were previously impossible, and they can reduce the cost – and the risk – of many 'dull, dirty or dangerous' jobs.

However, like any new technology, drones can be misused. They can pose a safety risk to other aircraft or to people and property on the ground, and the cameras and sensors they carry can be used to invade Australians' privacy. The challenge we face is to realise the potential of this innovative technology while protecting against its risks.

This report has surveyed the emerging issues around drone use and the adequacy of the existing regulatory framework. At a series of hearings and roundtables, the Committee heard from air safety regulators about the importance of allowing drone technology to mature so that the risk to people and property is minimised. The Committee also heard from privacy experts about the complexities and gaps in Australia's privacy laws which make it difficult to protect against privacy-invasive drone use.

Issues arising from the expanding use of drones will require sustained attention in years to come. It is the Committee's intention that the recommendations in this report serve as a starting point to adjust current privacy and air safety regimes in response to drone use. Further, the recommendations are intended to bring a more coordinated and harmonised regulatory approach to protecting Australians from malicious drone use while still permitting this dynamic new industry to grow.

I thank the Committee members for the diligence given to these serious issues and the industry groups, agencies and members of the public who assisted the Committee in this inquiry.

Mr George Christensen MP
Chair

Membership of the Committee

Chair	Mr George Christensen MP	
Deputy Chair	Ms Sharon Claydon MP	
Members	Ms Terri Butler MP (from 18/03/14)	Hon Mr Mark Dreyfus QC MP
	Hon Ms Jenny Macklin MP (to 18/03/14)	Mrs Louise Markus MP
	Mr Tony Pasin MP	Mr Graham Perrett MP
	Hon Mr Christian Porter MP	Hon Dr Sharman Stone MP
	Mr Michael Sukkar MP	

Committee Secretariat

Secretary	Dr Anna Dacre
Research Officer	Mr Peter Pullen
Administrative Officer	Ms Jessica Hargreaves

Terms of reference

On 12 December 2013, the House of Representatives Standing Committee on Social Policy and Legal Affairs resolved in accordance with Standing Order 215 (c) to conduct the following inquiry:

Inquiry into a matter arising from the 2012-13 Annual Report of the Office of the Australian Information Commissioner, namely the regulation of Unmanned Aerial Vehicles.

List of abbreviations

AAUS	Australian Association of Unmanned Systems
ACUO	Australian Certified UAV Operators' Association
AFP	Australian Federal Police
AGD	Attorney-General's Department
ALRC	Australian Law Reform Commission
ARCAA	Australian Research Centre on Aerospace Automation
CASA	Civil Aviation Safety Authority
CASR	Civil Aviation Safety Regulations
CSIRO	Commonwealth Scientific and Industrial Research Organisation
ICAO	International Civil Aviation Organisation
NFRM	Notice of Final Rule Making
NPRM	Notice of Proposed Rule Making
OAIC	Office of the Australian Information Commissioner
QFES	Queensland Fire and Emergency Services
QPS	Queensland Police Service
RPA	Remotely piloted aircraft
RPAS	Remotely piloted aircraft systems

UAS	Unmanned aircraft system
UAV	Unmanned aerial vehicle

List of recommendations

3 Safety in the air

Recommendation 1

The Committee recommends that the Australian Government, through the Civil Aviation Safety Authority, broaden future consultation processes it undertakes in relation to remotely piloted aircraft regulations so as to include industry and recreational users from a non-aviation background.

Future consultation processes should identify and seek comment from peak bodies in industries where remotely piloted aircraft use is likely to expand such as real estate, photography, media, and agriculture, amongst others.

4 Drones and privacy

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.

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.

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.

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.

1

Introduction

1.1 Australia's drone industry is booming. The number of certified commercial operators has risen dramatically in recent years, and the increasing capability and usability of drone technology has seen a huge rise in the number of businesses and consumers purchasing and using drones.

1.2 Drones, or remotely piloted aircraft (RPAs), have numerous civil and commercial applications. They offer economic benefits and significant safety improvements to a diverse range of organisations through novel or more cost-effective capabilities. As such, drone technology has the potential to offer substantial social and economic benefits to Australian society. However, their increasing use has led to a number of incidents that draw attention to the air safety and privacy implications of RPA technology. As RPAs become more popular, they are increasingly being used in unsafe ways. In addition, the increasing sensitivity of the cameras and instruments they can carry has raised concerns about privacy intrusions.

1.3 The foreword to the 2012-13 annual report of the Office of the Australian Information Commissioner stated that:

> We now expect that we will regularly see new ways in which personal information can be collected and used. Two pieces of technology that have caught the community's attention during the year because of their potential for doing just this were aerial drones, with the capacity to film while being controlled, and

> Google Glass, a wearable device that allows the user to collect, access and transmit information.[1]

1.4 This reference prompted the Committee to initiate an inquiry under Standing Order 215 (c) into RPAs and their implications for air safety and privacy. Under this Standing Order, a Committee can conduct any inquiry it wishes into the annual report of a Government department that stands referred to the Committee under the Speaker's Schedule of Annual Reports.[2]

1.5 The Committee did not initiate this examination of RPAs with the intention of conducting a comprehensive inquiry. The Committee observed that the commercial opportunities, safety risks, and privacy concerns raised by RPAs were emerging issues, and the purpose of the inquiry was to determine the adequacy of regulatory arrangements to respond to these technological developments. The Committee's inquiry focused on civil, commercial and recreational RPA applications, and consequently this report will not consider military RPAs or their uses.

Conduct of the inquiry

1.6 For this inquiry, the Committee did not seek submissions, but determined that a more effective approach was to conduct a series of roundtables with invited participants. The inquiry commenced with a roundtable discussion held in Canberra on 28 February 2014, followed by a public hearing in Canberra on 20 March and a second roundtable in Brisbane on 21 March, with a final public hearing in Canberra on 29 May 2014.

1.7 The Canberra roundtable consisted of three sessions that focused on air safety, RPA applications and privacy, and featured a range of industry stakeholders. The roundtable heard from air safety authorities like the Civil Aviation Safety Authority (CASA) and Airservices Australia, a number of industry groups, and privacy experts including the Privacy Commissioner.

1.8 The Committee's second roundtable was held in Brisbane on 21 March. The first of its two sessions focused on Queensland police and emergency services' experience using RPAs, and the privacy implications of that use.

---

1 Office of the Australian Information Commissioner, *Annual Report 2012-13,* p. xv.

2 A link to the Speaker's Schedule of Annual Reports can be found on the Parliament website at http://www.aph.gov.au/Parliamentary_Business/Committees/House.

The second session focused on the agricultural and commercial applications of RPAs in Queensland.

1.9 The Committee also held two short public hearings, in Canberra on 20 March at which the Attorney General's Department gave evidence, and on 29 May at which CASA appeared. A list of the public hearings and roundtables held by the Committee is included at Appendix A.

1.10 Transcripts of these roundtables and hearings are available on the Committee website, along with a number of additional documents tendered to the Committee in the course of its inquiry, such as responses to questions on notice. A list of the documents received by the Committee is included at Appendix B.

1.11 The Committee also had the opportunity to view a variety of RPAs and discuss their capability through an RPA demonstration given to the Committee by Parrot Pty Ltd and a site inspection at Insitu Pacific's facility in Brisbane.

Structure of the report

1.12 The Committee's report consists of four chapters. This chapter sets out the context and conduct of the inquiry. Chapter 2 describes the types of RPAs and highlights the impressive range of civil and commercial applications of RPA technology, in contexts such as law enforcement, emergency services, biosecurity, agriculture and scientific research.

1.13 Chapter 3 discusses the air safety issues raised by RPA use, including concerns regarding the build quality and reliability of RPAs, and the safety risk posed by large numbers of untrained RPA operators who may not know of or understand the relevant aviation safety regulations.

1.14 Chapter 4 focuses on the privacy issues that widespread RPA use raises. It briefly examines the complex web of Federal, State and Territory laws and common law principles that are relevant to privacy, and draws attention to some of the weaknesses that emerging technologies such as RPAs may expose in the existing regulatory system.

Terminology

1.15 The names used to refer to drones are almost as varied as the forms the technology itself can take. Participants in the inquiry have used a range of terms to refer to drones, including 'unmanned aerial vehicles' (UAVs), 'unmanned aerial systems' (UAS), and 'remotely piloted aircraft systems' (RPAS).

1.16 Industry groups expressed a desire to avoid the term 'drone', as a result of perceived negative connotations arising from an association with the United States military's program of 'targeted assassinations'. This report will refer to all aircraft of this type as 'remotely piloted aircraft' (RPA or RPAs).

2

Our Drone Future

2.1 Remotely piloted aircraft (RPAs) are being seen more often in Australian skies and, as they become cheaper and more capable, larger numbers of Australians are likely to utilise them. This chapter will briefly consider the rise in RPA use, and some of the applications and opportunities of RPA technology.

2.2 The term 'RPA' can apply to a huge range of vehicles, from small multi-rotor devices weighing less than a kilogram right through to fixed-wing craft weighing hundreds of kilograms. Smaller, consumer-level RPAs might have a maximum altitude of no more than 30 metres with a battery life of less than an hour, while the largest commercial RPAs currently operating in Australia are capable of staying airborne for more than 24 hours and can operate at altitudes of more than 5 000 metres (nearly 20 000 feet).

2.3 RPAs can carry a wide range of payloads. Consumer RPAs are often sold with a fixed, front-facing high definition video camera which can record or stream video to mobile devices or social media. Larger RPAs can be fitted with gimbals which may carry professional camera equipment, or may carry a range of sensors which can be used to make recordings or conduct measurements or surveys of one kind or another.

2.4 RPA sales and imports are unregulated, so it is difficult to estimate the number of RPAs that are currently being used in Australia. As at June 2014, the Civil Aviation Safety Authority (CASA) indicated that it had certified nearly 110 commercial RPA operators, with 40 more applications in process.[1] Australian RPA manufacturer MultiWiiCopter indicated that its local client base included more than 5 000 people; consumer RPA

1 Committee Hansard, 29 May 2014, p. 9.

vendor Parrot told the Committee that it has sold 500 000 RPAs globally, and characterised Australia as a 'strong' RPA market.[2]

2.5 It is clear that decreases in costs alongside improvements in capability have made RPAs affordable to a wider range of industry and recreational users. CASA is responsible for issuing certifications to commercial RPA operators. CASA's Terry Farquharson told the Committee that, as they become cheaper, RPA use is rapidly increasing:

> The industry is booming … It is the explosion of small technology – microtechnology – that has allowed small devices to proliferate… you can go down to your local store and for something in the order of $650 buy a quad machine, and if you want to go into your iPad store you can buy something for a bit less.[3]

2.6 As RPAs become cheaper, they are also quickly becoming more capable. Dr Luis Mejias Alvares from the Australian Research Centre for Aerospace Automation (ARCAA) said:

> we may have a new unmanned aircraft every six to 12 months— smarter, perhaps smaller and with longer lasting batteries and with different levels of autonomy, ranging from small toys to more advanced and more intelligent aircraft.[4]

Current and future drone applications

2.7 A range of government, commercial and industry groups participated in the Committee's roundtable discussions. The following section outlines the current and potential uses for RPA technology and the benefits they may bring to Australia.

Law enforcement and emergency services

2.8 A number of law enforcement and emergency services authorities have used, or have plans to use, RPAs. The Committee heard from the Australian Federal Police (AFP) and the Queensland Police Service (QPS)

2 Committee Hansard, 21 March 2014, p. 17; Committee Hansard, 28 February 2014, p. 20.

3 Committee Hansard, 28 February 2014, p. 1.

4 Committee Hansard, 28 February 2014, pp. 32.

that police use of RPAs remains limited. At present, the AFP only uses RPAs to assist in the forensic examination of crime scenes:

> One could perhaps visualise the AFP's use of the UAV as no more and no less than how one would use a static cherry picker, which is what we previously have used. For expediency, cost effectiveness and mobility the process we now undertake is with the UAV.[5]

2.9 In relation to future RPA use, the AFP advised the Committee that it is 'exploring the benefits and opportunities for search and rescue and for missing persons', but that it has 'no plans, research or current activity' in relation to RPA surveillance.[6]

2.10 QPS currently has two RPAs in service, which are used to 'enhance [its] special emergency response team capabilities' at 'high-risk and significant operations'. QPS deployed RPAs operationally for the first time at a siege in Brisbane on 26 December 2013.[7]

2.11 While its current use of RPAs is limited, QPS is considering expanding its use of RPAs to enhance its capability in crime scene or road traffic crash investigations, disaster responses, and search and rescue operations.[8] However, in relation to RPA surveillance, QPS told the Committee that it is not currently pursuing use of this capability. Inspector Brad Wright said:

> QPS is acutely aware of community concerns about the pervasiveness of drones. We have always gone into this project understanding that. Our use is limited to really overt activities … It is noisy, it flies at low altitude, and it is very obvious to everyone involved that we are using that technology. There has been no effort or intention from us to do anything that is not overt.[9]

2.12 Mr Richard Alder from the Australasian Fire and Emergency Service Authorities Council told the Committee that, although RPAs are not yet widely used, fire and emergency services are interested in their potential applications:

---

5 Committee Hansard, 28 February 2014, p. 26.
6 Committee Hansard, 28 February 2014, p. 27.
7 Committee Hansard, 21 March 2014, p. 1.
8 Committee Hansard, 21 March 2014, p. 1.
9 Committee Hansard, 21 March 2014, p. 2.

> Possibilities range from the small UAV that might be operated locally—a classic application is the sort of binocular-type application where a local firefighter or incident commander just needs to see over the trees and can put up something locally to get a better view of what they are tackling—right through to the strategic surveillance opportunities.[10]

2.13 The Queensland Fire and Emergency Service (QFES) likewise emphasised the benefits RPAs could provide in a rural fire context. QFES noted that RPAs could enhance its capability in an urban environment by permitting it to search or assess dangerous or unstable premises (where there is, for example, a risk of building collapse or hazardous fumes) which would otherwise be inaccessible.[11] In this context, RPA use could enhance emergency response by providing key information on unsafe areas and this could be achieved without endangering emergency services personnel.

Commercial and agricultural applications

2.14 RPAs have a wide range of commercial applications. The Australian Certified UAV Operators Association (ACUO) noted that RPA uses include:

> everything from standard real estate aerial photography and video through to mining surveys and stockpile surveys … there are agricultural applications for multispectral imagery, crop health, moisture content … pipelines, power line inspections … quite a broad range of activities.[12]

2.15 Mr Dale McDowall of Insitu Pacific, one of Australia's largest RPA companies, outlined a number of beneficial uses that RPAs can have. In addition to law enforcement and emergency management applications, RPAs may be useful in monitoring invasive species and weeds, monitoring marine life, inspecting resource industry stock and infrastructure, and in 'precision agriculture'.[13]

2.16 Mr Chris James of the Minerals Council of Australia characterised RPAs as an 'emerging technology', and said that they will be more widely used in

10 Committee Hansard, 28 February 2014, p. 16.
11 Committee Hansard, 21 March 2014, pp. 5-6.
12 Committee Hansard, 28 February 2014, p. 4.
13 Committee Hansard, 21 March 2014, p. 16.

the resources sector as they become more cost effective. Mr James said their current and future uses:

> range from stockpile surveying, environmental scanning/monitoring; fire monitoring; subsidence monitoring; pit wall mapping; infrastructure assessments; general aerial photography; blast monitoring—because the UAVs can fly through a blast cloud; and also spare parts transportation out to LNG rigs out off the North West Shelf.[14]

2.17 While expressing concern about the potential for misuse of RPA technology, AgForce Queensland noted the many beneficial uses RPAs may have for the agricultural sector, including:

> [detecting] crop stress, disease surveillance, fire monitoring and search and rescue … There is weed detection, there is land use infrastructure monitoring and property surveying and mapping. They are all great uses.[15]

2.18 Biosecurity QLD advised the Committee that RPAs may provide significantly more cost-effective means to detect invasive species and weeds, and control them with the precision application of pesticides. RPAs may also assist in certifying that Queensland is free of various pests, which is crucial for the agricultural industry's ongoing access to overseas markets.[16]

2.19 The capacity of RPAs to access remote areas and provide large scale monitoring offers opportunities across a range of commercial sectors. While some businesses in the mining, real estate and agriculture industries are already utilising RPAs, it is evident that as RPA capabilities increase, their commercial use will rapidly expand.

Media applications

2.20 Media organisations have or will soon use RPAs in a range of situations. Although widespread media use of RPAs has the potential to raise privacy issues (see chapter 4), they also have many useful applications. Journalist Mark Corcoran said that RPAs are already being used for sporting events and documentary filmmaking, and that they can be used to enhance

14 Committee Hansard, 28 February 2014, pp. 15-16.
15 Committee Hansard, 21 March 2014, p. 25.
16 Committee Hansard, 21 March 2014, p. 27.

reporters' safety in war or disaster zones. Mr Corcoran also noted that larger RPAs could give journalists novel newsgathering capabilities:

> You have a capability of ranging many hundreds of kilometres away from your point of launch. So there are stories there. Things like the clashes between whalers and environmentalists in the Southern Ocean could be independently verified. We could see what is happening with asylum seeker boats 300 kilometres over the horizon. It gives you the potential to independently verify those issues.[17]

2.21 With community appetite for instantaneous access to news stories and the expectation of visual footage, the newsgathering uses of RPAs are expanding. In addition to the capacity to access difficult locations, the use of RPAs can enhance the safety of news reporters, particularly in conflict or emergency situations.

Scientific and research uses

2.22 RPAs have a range of scientific and research uses. The Commonwealth Scientific and Industrial Research Organisation (CSIRO) has been using RPAs since 1999. Like many other organisations, CSIRO primarily uses RPAs where airborne imaging is useful; this has included crop monitoring in plant breeding experiments, beach surveys, monitoring of bushfire experiments, and simulating a flying fox to test a tracking device which would later be used to track real animals.[18]

2.23 In partnership with Murdoch University in Western Australia, Insitu Pacific has conducted trials using RPAs to monitor marine life near offshore gas and oil plants. Insitu's Mr Dale McDowall said the trials were intended:

> to try to understand how we may be able to monitor the population numbers and the species types of various marine mammals, such as whales, dolphins, dugongs and turtles, and once again over time help that operator understand the impact of their operations on the marine environment.[19]

17 Committee Hansard, 28 February 2014, p. 29.

18 Committee Hansard, 28 February 2014, p. 17.

19 Committee Hansard, 21 March 2014, pp. 16-17.

2.24 Australian scientific organisations have already found a range of uses for RPA technology. The anticipated fall in price and increase in RPA capabilities makes it likely that RPAs will be used in a range of additional scientific survey and monitoring roles.

Interest groups and recreational uses

2.25 Some lobby groups have indicated interest in the potential of RPAs to monitor or expose activities. In particular, environmental groups see value in the capability of RPAs to monitor the discharge of waste in waterways. Similarly, RPAs have been used by animal protection groups to take footage of a commercial farming operation with the intention of exposing animal cruelty. Voiceless, a non-profit think tank focused on raising awareness of animals suffering in factory farming, argued that RPAs could provide an important tool in ensuring the effective enforcement of animal cruelty regulations:

> [RPA] 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 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.[20]

2.26 Other commercial uses of RPAs are also increasing. The Committee heard from Parrot Pty Ltd, a company that designs and sells consumer-level RPAs that can be controlled by a smartphone. Parrot's RPAs come equipped with a forward-facing high definition camera, footage from which can be uploaded to social media directly from the smartphone.[21] Event photographers, real estate agents, and tourism guides are some of the industries utilising this technology.

2.27 Sporting events are being recorded by RPAs, either to track the safety of participants or to provide footage for spectators. YouTube hosts an enormous array of video taken by RPAs to promote tourist destinations, promote extreme sports or for educational or environmental purposes. Much of this footage is taken by recreational RPA users with an interest in a particular field.

---

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

21 Committee Hansard, 28 February 2014, p. 20.

2.28 The range of users and uses of RPAs is set to expand. While this provides business potential for developers, efficiencies for a number of sectors, and applications for recreational users, these opportunities must not come at the cost of privacy or safety.

2.29 Many roundtable participants expressed concern at the potential privacy and safety concerns that may arise from widespread use of RPAs by members of the public who do not have an aviation background or appropriate training. These issues will be explored more fully in chapters 3 and 4.

2.30 It is clear that RPAs have a very broad range of civil and commercial applications, in addition to their interest as a consumer product. The evidence above suggests that RPAs will be used more and more often in circumstances where they can provide new capabilities, reduce the risk associated with a given job, or do the job more cheaply. As ARCAA's Dr Mejias noted:

> The technology is here; we need to start thinking of embracing the technology and perhaps focusing on defining the guidelines for its responsible use … and regulations for the safe use of the technology.[22]

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

3

Safety in the air

3.1 The previous chapter outlined the current and future uses remotely piloted aircraft (RPAs) may have in a range of industries. However, as a result of air safety concerns it holds in relation to RPAs, the Civil Aviation Safety Authority (CASA) does not permit RPAs to use shared airspace, and substantial restrictions on commercial RPA operators remain in place.

3.2 This chapter will examine the risks to air safety raised by CASA and other roundtable participants, which arise both from the technology used to build and control RPAs, and from non-certified or unsafe RPA use. It examines the complexities of regulating RPA use due to the rapid development of technology, the enormous range in size and capability of RPAs, and the breadth of RPA users, from hobbyists to large scale commercial operators.

Safety concerns arising from RPA technology

3.3 RPAs are an emerging technology and have not yet achieved the reliability expected of mature technologies. In particular, roundtable participants drew the Committee's attention to two aspects of RPA technology which give rise to safety concerns – the quality and durability of the material from which RPAs are constructed, and the technology that controls how they behave.

3.4 In relation to the quality of materials, roundtable participants noted that while commercial aircraft are built to very stringent standards that provide relative certainty about their airworthiness, the same cannot be

said for RPAs. CASA's Director of Aviation Safety, Mr John McCormick, said that:

> The difficulty with the proliferation of these UASs … is that they are not built to any standard. There is no international standard at this stage. So their ability to maintain altitude, their ability to maintain heading, their ability to suffer equipment failure and then not crash, have not been established.[1]

3.5 CASA's concerns about the general build quality of RPAs were echoed by VidiAir, an Australian RPA company that specialises in aerial surveillance solutions. VidiAir's Managing Director Mr Anthony Hoy told the Committee that:

> The primary concern for me and my colleagues has been systems reliability - which is difficult to regulate and is unregulated, as things stand - to the point where we have engaged our own microelectronics engineer because of our concerns. I think it is fair to say that the general consensus on the part of insurers and many other operators is that critical systems failure is significantly under-reported, particularly on the part of the unauthorised users.[2]

3.6 VidiAir conducted an audit on the microelectronic componentry of an RPA valued at $12 000, and said its findings were 'of some considerable concern':

> A lot of the machines fail because the standard of componentry in even the premium brands is of a hobbyist standard in a lot of cases. We found vital components missing, such as decoupling capacitors. We replaced batteries with lower internal resistance and significantly higher amperage. There was just inadequate fit-out. There were battery connector plugs that were inadequate for the power required for the unit. Each of these things is capable of causing a fly-away or a crash, as does happen and is happening, I can assure you.[3]

1 Committee Hansard, 28 February 2014, p. 2.
2 Committee Hansard, 28 February 2014, p. 8.
3 Committee Hansard, 28 February 2014, p. 8.

Text Box 3.1

Sydney, New South Wales – October 2013

On Wednesday 2 October 2013, an RPA crashed into the Sydney Harbour bridge, sparking safety concerns. The RPA, a quad-copter piloted by a recreational RPA user, collided with a bridge pylon and landed on the bridge's train line after its pilot lost control of the vehicle.

The RPA's pilot, Mr Edward Prescott, said he was testing new equipment on the RPA when he lost control of the vehicle. Mr Prescott said that he had assumed the RPA had crashed into Sydney Harbour, and it was only when he read news stories about an incident involving a 'mystery drone' that he realised it had not.

Mr Prescott said he had no intention of flying the RPA into the bridge. Video from the RPA's camera has been posted to the internet, and shows Sydney transport workers retrieving the RPA.

Mr Prescott was fined $850 as a result of the incident.

Sources C Cosier, "'I don't know whether it's a bomb or not': Train driver flummoxed after drone hits Sydney Harbour Bridge", Sydney Morning Herald, 26 November 2013; L. Silmalis, "Backyard drone operators to be handed guidelines after one crashed into the Harbour Bridge", The Daily Telegraph, 3 May 2014.

3.7 Even RPAs built to military standards – which are much higher standards than current civil and recreational RPAs are built to – may require improvements before CASA would consider integrating them into Australian airspace:

> the military is prepared to accept losses and in the operational sphere they do accept that some of these will not come back, as we have seen reported often in the newspapers. Of course, to the civilian world that is intolerable. We would like to get that risk as low as reasonably practicable.[4]

3.8 Professor Duncan Campbell, Director of the Australian Research Centre for Aerospace Automation (ARCAA), noted that confidence in the build quality of an aircraft is vital when that craft shares the skies with other vehicles:

> The fact is that the police, the Queensland fire service, farmers with precision ag[riculture] and so forth are more likely to be flying in airspace that could be shared with other airspace users, and this is where this whole notion of airworthiness comes in. So you do not want a cheap $100 machine up there that is likely to break and cause some sort of hazard for other airspace users.[5]

3.9 In addition to problems with build quality, the systems and technologies that enable unpiloted aircraft to function safely in shared airspace are yet

4 Committee Hansard, 28 February 2014, p. 8.

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

to reach full maturity. A range of technologies must be in place to ensure that remotely piloted aircraft can operate without risk to vehicles in their vicinity, and although substantial progress has been made in recent years, more work is required to reach a sufficiently safe operating environment.

3.10 The Queensland government has taken a particularly active interest in facilitating the growth of a viable RPA industry. Much of its focus has been on sponsoring research into technologies that work to make RPAs safer, with the goal of fully integrating RPAs into Australian airspace. Mr Lindsay Pears of the Queensland Department of State Development, Infrastructure and Planning (DSDIP) said the government's focus has been on:

> ensuring that the barriers to safety of UAV operations were dealt with by way of technology. That includes see-and-avoid [and] safety of flight technologies, as well as sensors for commercial applications, autonomous systems to improve navigation and the like.[6]

3.11 Mr Pears said the Queensland government had funded a number of joint projects with this goal in mind:

> Two major projects have been co-funded by the state government with Boeing, Insitu and others. One is called SmartSkies, which is now completed. The objective of that program was to deal with the see-and-avoid and air space management issues associated with safe operation of UAVs. The other, which is ongoing, is Project ResQ, which is about extension of that SmartSkies technology into commercial applications.[7]

3.12 However, Mr Pears noted that more research is required to develop the necessary technical capability:

> There is more to be done, on the research front in particular, and we will be working with ARCAA and others to do that, particularly around things like improved navigation, autopilots, onboard processing systems, control systems, secure data link, which cannot be jammed, and also image processing and enhanced extraction of information and dissemination to a wide front.[8]

---

6 Committee Hansard, 21 March 2014, p. 15.

7 Committee Hansard, 21 March 2014, p. 15.

8 Committee Hansard, 21 March 2014, p. 16.

3.13 The recent safety incident in Geraldton involving injury to a participant in a sporting event allegedly caused by a nearby RPA (see Text box 3.2) highlights the safety issues associated with RPA technology. Witnesses suggested that the RPA operator either lost control of the aircraft or suffered a component failure, which caused the craft to crash; the RPA operator suggested that someone had 'hijacked' the RPA by taking over the remote control link.

3.14 That the incident may have arisen from any or a combination of these factors highlights the serious safety issues of RPA technology, and the lack of standards in RPA design and operation. A failure of RPA technology in a larger size RPA, leading to either a 'hijacked' craft or the descent of an uncontrolled RPA poses serious safety and security concerns.

Text Box 3.2

Geraldton, Western Australia – April 2014

On 6 April 2014, a triathlete was allegedly struck by an RPA while competing in a race in Geraldton, Western Australia. The RPA was being used to take footage of the competition.

Triathlete Raija Ogden was treated for head injuries by paramedics at the scene of the race before being taken to hospital in a stable condition. The RPA operator lost control of the vehicle and it dropped 10 metres at which point, according to Mrs Ogden, it struck her in the head.

The RPA operator, Mr Warren Abrams, claimed that the vehicle crashed near Ms Ogden, startling her and causing her to fall. He said that his initial investigation indicated that control over the RPA was hijacked by someone nearby using a technique Mr Abrams referred to as 'channel hopping'.

CASA regulations specify that RPA operators must ensure that their vehicles remain more than 30m away from people not directly involved in using the craft.

CASA referred the matter to the Commonwealth Director of Public Prosecutions (DPP) in June 2014. The DPP will determine whether Mr Abrams will face prosecution.

Source *S Taillier, "Triathlete injured as drone filming race falls to ground", ABC News, 8 April 2014; L Thomas 'Drone operator confident of "accident" finding', The West Australian, 26 June 2014.*

CASA regulations – commercial and recreational use

3.15 The lack of a standard build quality and the technological limitations of RPAs have given rise to a number of restrictions on when and where RPAs can operate. The Commonwealth regulates air safety through the *Civil Aviation Act 1988*, made under the trade and commerce power of the Constitution. CASA is the agency responsible for regulating the use of

RPAs in Australia. Mr McCormick explained that CASA must, by law, focus primarily on aviation safety:

> There is no doubt whatsoever that if a large UAV crashes, it will not be without harm. That is one of the issues which we always have in the back of our minds … the Civil Aviation Act says at section 3A that our prime purpose is that maximum emphasis has to be on aviation safety - protecting the public.[9]

3.16 Airservices Australia, the government agency responsible for air traffic control, has a similar focus. Mr Sean Lake from Airservices Australia said:

> we are acutely aware of the rapid proliferation of UAV operations. We are working closely with CASA and our focus is very much the same as CASA—it is on safety, totally ... The question of integrating operations into controlled airspace, as opposed to the segregation which we have been doing up until now, is probably our primary focus.[10]

3.17 Professor Campbell noted that the challenge of integrating RPAs into Australian airspace could be particularly difficult. In his view, the difficulty faced by regulators, and by RPA companies was:

> how to open up the skies for applications. The challenge is, of course, that our skies are very cluttered. I think we can all relate to the US skies. Indeed, if we look at Brisbane, Sydney, Melbourne and Adelaide, that is referred to as the J curve around Australia. Our air space in that corridor is just as dense as it would be overseas.[11]

3.18 Mr McCormick expressed CASA's view that, at present, the reliability and control limitations of RPAs remain sufficiently serious that they cannot be safely integrated into shared airspace:

> Integration into controlled airspace becomes a problem both for our services and for us from the point of view of knowing just how that vehicle will react and how it will behave. So there is a risk of interference with other vehicles, interference with other aircraft, and the possibility of crashing in public areas, with the obvious response.[12]

---

9 Committee Hansard, 28 February 2014, p. 3

10 Committee Hansard, 28 February 2014, p. 7.

11 Committee Hansard, 21 March 2014, p. 10

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

3.19 RPA use is regulated under Part 101 of Australia's Civil Aviation Safety Regulations (CASR 101). CASR 101 distinguishes between commercial and recreational RPA use – at present, commercial RPA use of any kind can only be carried out with CASA certification.

3.20 Recreational use is governed by the same regulations that apply to model aircraft. While recreational RPA users do not have to seek CASA certification or training before they use their RPAs, there are a number of rules to ensure that the risk of a safety incident is minimised. These rules, referred to as the 'standard operating conditions', require that RPAs:

- may only be operated in visual line of sight (that is, the RPA can be directly seen by its pilot without the aid of binoculars or a telescope)
- may only be operated below 400 feet above ground level, in visual meteorological conditions, by day
- may not be operated over populous areas, or within 3 nautical miles (about 5km) of an aerodrome, in controlled airspace, or over prohibited areas
- may not be operated within 30 metres of a person not directly associated with the operation of the RPA (that is, a person in the operating team).[13]

3.21 At present, commercial RPA use of any kind requires CASA certification. CASA defines 'commercial use' as 'any RPA operated for a commercial reason', whether that be for hire and reward, remuneration, or any other consideration.[14] CASA's Mr Grant Mazowita said:

> If it is not recreational/sport-type activity, generally you are caught by the regulatory standards that we apply. Now, there are certain places in our regulations where we refer to research and development and scientific-type things but, by and large, the recreational operations are treated as model aircraft and the commercial operations are treated as RPAs.[15]

3.22 CASA's RPA certification process has two components – a remote piloting certificate and an operating certificate. CASA's Mr Terry Farquharson described the certification process in this way:

> There are two aspects of certification. One is the pilot, the controller, certificate. They are assessed against a knowledge

13 Committee Hansard, 29 May 2014, p. 2
14 Committee Hansard, 29 May 2014, p. 5.
15 Committee Hansard, 29 May 2014, p. 5.

> standard and a competency standard. The second part of the assessment is in relation to the operating certificate. There is an operations manual and appropriate controls put in place that the organisation has the right set of resources to do what it is intending to do. At the end of that, the person can be certified individually as a controller or an organisation receives an operating certificate.[16]

3.23 Mr Brad Mason from the Australian Certified UAV Operators Association (ACUO) said that certified RPA operators face substantial limits on their activities:

> we are quite heavily limited in what we can do and where we can go. It is not like we can just put an aircraft up in the air anywhere at any time. We have to go through very strict procedures, quite strict safety and risk management assessments, before we put an aircraft in the air.[17]

3.24 The operating certificate specifies when and where RPAs may be used, and variations to that use must be approved by the regulator. Mr Farquharson said:

> Each certificate is issued with a number of things that the operator can do, and that is all they are authorised to do. If they want to expand that or remove something then we amend the certificate through a process.[18]

Non-certified RPA use

3.25 CASA's restrictions on the commercial use of RPAs aim to maintain air safety and minimise the risk of a serious RPA crash. However, recent improvements in RPA piloting and control technologies, combined with drastic reductions in price have led to a substantial increase in the number of RPAs sold, both to consumers and potential business operators. The Committee has heard that this has led to a large increase in the number of untrained RPA operators, many of whom are either unaware of, or do not follow, CASA's regulations. This presents a substantial risk to air safety.

16 Committee Hansard, 28 February 2014, p. 9.
17 Committee Hansard, 28 February 2014, p. 4.
18 Committee Hansard, 28 February 2014, p. 6.

3.26 As stated above, currently RPAs used for recreational purposes, and within standard operating conditions, do not require a certification process. Professor Duncan Campbell from ARCAA said that it was important to distinguish between RPA users who are aware of and comply with CASA regulations and those who do not:

> I think we can identify there are two groups of people. There are the hobbyists—that is too great a generalisation, but those who enter this area and are not aware of any of the laws, whether it be privacy or air safety regulations—and there are those who come in very much from an airmanship point of view and are very aware of air safety.[19]

3.27 Similarly, Mr Quinton Marais, Director of Australian RPA manufacturer MultiWiiCopter, said:

> I think you have to split this off into consumers and professionals. The classic real estate agent looking to photograph suburbia is a consumer. He is not an aviator and does not understand aviation culture. He does not know how the aviation system or airspace works and he certainly does not understand risk.[20]

3.28 Industry groups suggested that commercial RPA use without the appropriate certification is becoming increasingly common. Mr Mason from ACUO told the Committee that:

> what we are seeing is that there is a lot of illegal and unauthorised use of UAVs. We understand that the regulator is doing its best to try and combat that but … they are so easily available and so cheap to buy these days that anybody can buy one and anyone can go out and operate one. It is really difficult to regulate, manage and catch those people.[21]

3.29 According to Mr Mason:

> A lot of those people are coming from a non-aviation background, too, so they do not have an aviation knowledge set. They are coming from a commercial business background, so they are not really aware of some of the things they are doing and some of the safety implications of what they are doing ... the greatest threat,

19 Committee Hansard, 21 March 2014, p. 10.

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

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

> from both a safety and a privacy issue, is more so from the illegal and unauthorised operators than the certified operators.[22]

3.30 Mr Marais told the Committee that feedback from MultiWiiCopter's customers indicated that some consumers who purchase RPAs do not understand how to use them safely:

> But the consumers, on the other hand, are able to purchase products which are able to fly away. They do not even understand why they fly away, so they will ring us up and say, 'It's flown away.' We will say, 'Have you reported this incident to the aviation authorities?' They do not know that they should report incidents to the aviation authorities.[23]

Text Box 3.3

Newcastle, New South Wales – March 2014.

On Saturday 22 March 2014, a rescue helicopter in Newcastle was forced to take evasive action to avoid colliding with an RPA.

At approximately 10pm, while returning to base after delivering a patient to the John Hunter Hospital, the helicopter's crew saw lights at about 1000ft (300m) above ground. The crew initially thought the lights belonged to a larger aircraft in the distance, but soon realized the object was an RPA, much closer than they had thought, and took evasive action to avoid it.

Mr Glenn Ramplin from the Rescue Helicopter service said the results of a collision with the RPA could have been very serious, as the incident occurred over a residential area: 'Even things like birds can damage an aircraft so to run into the UAV (unmanned aerial vehicle) or the RPA if you will, you know, that could have been catastrophic.'

CASA regulations forbid recreational RPA users from sending their craft higher than 400 feet or from flying RPAs over populous areas. They also forbid RPA operators from flying them within five kilometres of an aerodrome.

The operator of the RPA has not been identified.

Source ABC Radio National, 'Mid-air near miss raises concerns over regulation of drones', AM Transcript, April 4 2014.

3.31 The Queensland Police Service operates a number of RPAs in tightly regulated circumstances. Inspector Brad Wright expressed concern that untrained RPA users may not be sufficiently mindful of safety:

> I am never going to fly one of my devices over a road with moving traffic; even though it is only light, it could be terrible if it hit a car. I worry about people doing that. At the moment, we have not seen it, but, yes, I certainly have concerns, because we are, as I said,

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

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

> very careful. In the police services, we understand risk; I worry about people who do not.[24]

3.32 Members of the RPA industry are concerned that unsafe RPA use by recreational users and uncertified commercial operators could potentially harm the development of the industry. Mr Lindsay Pears from the Queensland Department of State Development, Industry and Planning told the Committee that:

> A lot of the professional operators in the industry are really concerned about that. That is primarily, as you said, from the point of view that it could totally disrupt the market at an embryonic stage of growth.[25]

3.33 Mr Quinton Marais also expressed concern about the impact of unsafe RPA use by untrained or unaware operators:

> I think consumers have the ability to damage the potential of this technology through lack of understanding and lack of training. Professionals are wanting to access it and keen to comply with every regulation that they are told.[26]

3.34 Roundtable participants made a number of suggestions as to how the risk from untrained and unauthorised RPA operators could be reduced. Professor Campbell said that safety could be improved if more RPA users were made aware of how to minimise safety risks:

> There are those who are aware of the regulations—'No, they don't apply to me' or 'I choose not to comply'—and those who simply do not know. Education was touched on just previously. I think that is one key element. I have had social conversations with hobbyists and even stores that sell these things. I ask them, 'Are you aware that there are CASA regulations?' And some of them have said, 'No, I didn't know that.' So there is an education element that goes with all of that.[27]

3.35 In the same vein, Mr Pears said that education could be useful in reducing the risk from the non-certified use of RPAs:

> It is more about education and awareness—trying to capture kids as early as you possibly can—and understanding that the technology has a wide application. This can be through social

24 Committee Hansard, 21 March 2014, p. 8.
25 Committee Hansard, 21 March 2014, p. 22.
26 Committee Hansard, 21 March 2014, p. 21.
27 Committee Hansard, 21 March 2014, p. 10.

> media and education and training through the school system. Queensland also has aviation high schools where these sorts of issues can be dealt with.
>
> So over time it is just increasing public awareness and perhaps engaging some of the vendors … to actually make sure … that when you go onto a website or go to a physical shop to buy these things there is public information available to warn you of the issues, to make you aware and to cause you to ask the questions.[28]

3.36 In the wake of a number of recent safety incidents involving RPAs, many of which were being used illegally (see the text boxes throughout this chapter), CASA has reached an agreement with RPA distributors and retailers to include a flyer with information on RPA safety regulations with RPAs at the time of purchase. The flyer outlines the basic safety procedures recreational RPA users must follow and the conditions within which they are permitted to operate. A copy of the flyer is included as Appendix C of this report. Mr Terry Farquharson said that CASA has:

> a very active program of going out to the distributors and even the manufacturers of these machines … It is actually trying to catch the problem at the lowest level possible and it guides people to their responsibilities, to the things that they should be considering.[29]

3.37 Final responsibility for the safe usage of RPAs rests with RPA operators. Mr Chris Roberts from Parrot, a company that sells RPAs to the consumer market, said that the pilot of the RPA must take responsibility for ensuring that it is used safely:

> in a consumer-user environment the user has got to be responsible for where they are using the product. That is exactly the same with a remote control helicopters or planes, which have been around for 20, 30, or 40 years. It is the same ethos: the user needs to be responsible about where they fly the product.[30]

3.38 While users are ultimately responsible for the safe operation of the craft they fly, establishing what constitutes safe parameters of operation and ensuring product safety and reliability requires a regulatory framework and a more coordinated national approach.

---

28 Committee Hansard, 21 March 2014, p. 22.

29 Committee Hansard, 29 May 2014, p. 7.

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

Review of the regulations

3.39 RPA use is regulated by part 101 of the Civil Aviation Safety Regulations (CASR 101), which came into force in 2002. In mid-2011, after a substantial increase in the number of RPA users, CASA began a review of the section. As part of that review, in May 2014 CASA published for public comment a Notice of Proposed Rule Making (NPRM). This notice contains proposed amendments to CASR 101.

3.40 The period for public comment ended on 16 June 2014, having been open for approximately one month. CASA will publish its final regulatory changes in a Notice of Final Rule Making (NFRM) after taking public comment into account. CASA hopes to publish its NFRM in the third quarter of 2014.

3.41 CASA told the Committee that it frequently provides further opportunities to provide input if requested. CASA's Mr Grant Mazowita said that:

> If we are petitioned to extend that period, I think we invariably have provided those extensions to the industry. If the industry seeks additional opportunities to discuss issues with us, we entertain those requests and almost invariably agree to them.[31]

3.42 Mr Mazowita noted that the International Civil Aviation Organisation (ICAO) is currently working on model RPA regulations, and that future CASA reviews of CASR 101 will take the ICAO's work into account:

> Much of this will be driven by the work being undertaken by the International Civil Aviation Organization. They are in the process of developing and publishing international standards and recommended practices. Typically, we try not to get too far out ahead of ICAO. We like to keep in step with what is happening internationally and with our major trading partners.[32]

3.43 However, Mr Jim Coyne from CASA noted that the ICAO regulations may not be finalised for a number of years. CASA took the view that it was necessary to amend Australia's regulations more quickly than that:

> the process for developing what we call 'standards and recommended practice' is about a five- or six-year period, and we

31 Committee Hansard, 29 May 2014, p. 3.

32 Committee Hansard, 29 May 2014, p. 4.

> feel that people cannot wait that long for the ICAO system. So we need to get guidance out there quickly.[33]

3.44 The new regulations proposed by the NPRM would not change the rules in relation to recreational RPA use, provided that the RPA is operated according to the 'standard operating conditions' outlined above. Therefore, any recreational RPA users will not require CASA training or certification. CASA's John McCormick said:

> The proposed changes do not apply to amateur or privately operated drones for recreational purposes. These are model aircraft and are not included in the NPRM change proposals.[34]

3.45 CASA said that in the future it may separate the rules relating to recreational RPA use from those governing model aircraft so that it can formulate rules that are better suited to each of those categories. Mr McCormick said:

> Part 101—which originated in balloons and model aircraft—still has some role and some weight to carry in that realm. We will eventually move the RPA into another rule set of 102, so that we clearly separate the model aircraft private activities from the RPA activities. We are not sufficiently advanced to be able to do that at this stage, so we feel an amendment to 101 is a more pressing need rather than go through the process of developing 102.[35]

3.46 Consequently the amendments proposed in the NPRM relate to commercial RPA use. Most notably, the NPRM would create a new weight class of 'small' RPAs under two kilograms which could be used commercially without CASA certification in limited circumstances. Mr McCormick said:

> A key part of this amendment acknowledges the existence of a low-risk class of RPA operations, which is determined as 'small RPA' with a gross weight of two kilograms and below while—and I will stress this—they are being operated under the standard RPA operating conditions as defined and discussed in the NPRM.
>
> For these types of RPA operations under these conditions CASA proposes that the requirement for a remote pilot certificate, or an unmanned aircraft systems operator certificate, will not apply.[36]

---

33 Committee Hansard, 29 May 2014, p. 4.
34 Committee Hansard, 29 May 2014, p. 3.
35 Committee Hansard, 29 May 2014, p. 4.
36 Committee Hansard, 29 May 2014, p. 1.

3.47 CASA emphasised that all RPAs weighing more than two kilograms, and all RPAs operating outside of the standard operating conditions, will still require a remote pilot certificate and an operating certificate:

> Any suggestions that operations of this type will become unregulated is not correct. RPAs with a gross weight above two kilograms, in all operating conditions, and all RPA operating outside of the standard RPA operating conditions, will require an operation approval from CASA. The operational approval process must include a documented risk assessment and treatment plan describing how identified safety risks will be managed to an acceptable level.[37]

3.48 In addition, the NPRM contains updated guidance on what constitutes a 'populous area' for the purposes of uncertified commercial RPA use. As stated above, RPAs cannot be operated in a populous area without CASA approval. However, the NPRM notes that:

> An area within an urban environment may be deemed as 'unpopulous' for the term of an RPA operation if suitable conditions are met. For example, an oval devoid of people could be utilised to photograph real estate from across the road through the use of oblique photography; or the area around a power pole within an urban area, set up as a demarcation zone with the appropriate 'temporary workplace' conditions could be approved.[38]

3.49 This guidance clarifies CASA's view that a range of uncertified commercial RPA operations could be possible in an urban environment as long as the RPA operator adheres to the standard operating conditions.

3.50 The NPRM also proposes a number of supplementary changes to CASR 101 which would update the terminology used to describe RPAs, clarify the requirements for pilot training and certification, and streamline the process for approval.[39]

3.51 Under the proposed changes to CASR 101, commercial RPA use would remain relatively tightly regulated in situations where RPAs could pose a serious safety risk. However, CASA meets frequently with government agencies, researchers and RPA industry groups to keep informed of technological developments in the field, so that the restrictions on RPA

37 Committee Hansard, 29 May 2014, pp. 1-2.

38 CASA, *Draft Advisory Circular AC101-1 - Remotely piloted aircraft systems – general*, May 2014, p. 20.

39 Committee Hansard, 29 May 2014, p. 2.

use imposed for safety reasons may be revised when RPA technology has developed sufficiently. Mr McCormick said:

> From our point of view, we are committed to working with the commercial operators … It is the reality that these things are here; we cannot turn back the tide.[40]

3.52 ARCAA is one of Australia's leading RPA research centres. Professor Campbell told the Committee that CASA personnel receive frequent briefings on the progress of ARCAA research projects:

> we have very open and frequent discussions with them. That includes with John McCormick, the Director of Aviation Safety, and a few other senior people within CASA ...we hold regular workshops with the key CASA personnel; they literally come down to our research centre and we brief them on where we are at.[41]

3.53 Industry engagement of this sort will help CASA identify when safety has improved to the extent that fewer restrictions on RPA use are required. As Professor Campbell noted:

> The regulations are there to uphold air safety, and I think we have all identified that there is a domain here where there is a question mark over air safety with people who do not understand or who choose to not understand. Some of the work we are doing is trying to identify to the regulator: for this sort of aircraft in this sort of scenario with low risk, we can change the bounds of the regulations. So we are working closely with the regulator there.[42]

3.54 While CASA's engagement with industry helps it track developments in relation to RPA safety, its consultation process does not appear to include the broader community of RPA users. Halfway through the NPRM's consultation process, CASA reported that 14 responses had been received, all from within the aviation community.[43] The broader community of commercial RPA users, including those in industries the Committee heard from in the course of its inquiry, had not participated.

3.55 The narrow range of feedback to CASA's NPRM may be related to the limited notification processes it follows. Mr Grant Mazowita, CASA's manager of standards development and quality assurance, said:

---

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

41 Committee Hansard, 21 March 2014, p. 12.

42 Committee Hansard 21 March 2014, p. 11.

43 Committee Hansard, 29 May 2014, p. 3.

> The public is notified principally through the CASA website and the notification in *The Australian* that this NPRM has been published.[44]

3.56 Mr McCormick said that CASA had not actively sought input from the wider community of RPA users:

> apart from putting the ad in the aviation supplement in Friday's *The Australian* and posting on our website that we have this out for consultation, we do not particularly go out and target the other groups unless we have to—in other words, unless we are specifically required to do so, because we don't know where to stop or start. It is very difficult to understand who all the stakeholders are in these issues.[45]

3.57 CASA did, however, note that it is attempting to broaden its communication methods:

> We are spending a considerable amount of time … in our general communications activities on how we can reach specific stakeholder groups throughout not only the industry but the broader aviation community. We have stepped into the newer communications medium. We have our own Twitter account and we are investigating other mechanisms by which we can pull people into specific topic areas on our website.[46]

3.58 Regulating for the safe use of RPAs by recreational and commercial users poses difficult challenges. Larger commercial and civil operators appear aware of air safety and certification restrictions, and are engaging with CASA to ensure that general air safety is not compromised. However, informing the wider community of recreational and commercial RPA users about CASA regulations and involving them in its regulation development processes represents an ongoing challenge.

Committee comment

3.59 The Committee notes the ongoing safety concerns associated with RPA technologies, in particular the evidence it has received about the deficiencies that may exist in the materials and components used to build

44 Committee Hansard, 29 May 2014, p. 3.
45 Committee Hansard, 29 May 2014, pp. 3-4.
46 Committee Hansard, 29 May 2014, p. 9

RPAs. The Committee also notes that the technologies used to control RPAs in flight are still developing. The Committee therefore takes the view that the restrictions CASA currently places on commercial RPA operations over a certain size are appropriate and necessary.

3.60 The Committee also notes that RPA technology is developing rapidly. The technical problems and safety risks which prevent RPAs from fully integrating into Australian airspace may well be surmountable. Given CASA's ongoing engagement with researchers and RPA industry groups, CASA should be well-informed about developments in RPA technology and the effectiveness of current regulations to maintain appropriate safety standards in Australian skies.

3.61 However, the Committee is concerned that CASA may not be receiving input into its regulatory review processes from the diverse range of RPA users. Its consultation processes are well suited to an aviation industry composed of a small number of identifiable expert stakeholders. However, RPA regulations affect a vastly higher number of stakeholders, many of whom do not have an aviation background. Their views should be heard during the process of regulatory review, particularly as they represent the fastest growing group of RPA operators.

Recommendation 1

The Committee recommends that the Australian Government, through the Civil Aviation Safety Authority, broaden future consultation processes it undertakes in relation to remotely piloted aircraft regulations so as to include industry and recreational users from a non-aviation background.

Future consultation processes should identify and seek comment from peak bodies in industries where remotely piloted aircraft use is likely to expand such as real estate, photography, media, and agriculture, amongst others.

3.62 The Committee notes the safety risks posed by untrained RPA operators. Although RPAs are becoming more capable as time passes, even substantial improvements in RPA guidance and safety technologies will not remove the risk posed by untrained or unsafe RPA operators. It is important that every commercial and consumer RPA operator is aware of their responsibility to use RPAs safely. The Committee notes with

approval CASA's attempts to ensure that Australian RPA operators are better educated about the relevant safety regulations, such as its recent initiative to distribute pamphlets outlining safety issues and regulatory information to RPA purchasers.

3.63 The Committee notes CASA's ongoing process to amend the RPA regulations contained in CASR 101. The Committee notes the NPRM updated guidance on what may constitute a non-populous area, and considers this guidance useful and appropriate. Similarly, the Committee considers that the creation of a class of commercial RPA operations that does not require certification is appropriate, considering the low risk of these small craft when used in standard operating conditions.

3.64 Therefore, the Committee takes the view that CASA's proposed amendments to CASR 101 strike a suitable balance between minimising safety risks on the one hand and facilitating the development of Australia's RPA industry on the other. For operators wishing to employ any RPA outside of the standard operating conditions, for example beyond line of sight or within 30 metres of persons, an exemption may be sought from CASA. The Committee notes that an exemption may be restricted to a single flight event or may be granted to an operator for any specified type of event (such as sports matches or music concerts). Such an exemption requires CASA to be satisfied of the operator's expertise and further conditions may be placed on the type of craft, safety features and environmental conditions.

3.65 It is the Committee's view that the NPRM proposes greater flexibility while maintaining a clear safety regime. However, the Committee has a number of concerns in relation to the proposed system:

- the growth of the RPA industry has led to a steep increase in the number of RPA operators seeking certification. While permitting uncertified commercial RPA operations under 2 kilograms may reduce CASA's administrative burden temporarily, assigning sufficient resources to provide timely operator approvals and exemptions will remain an ongoing concern for CASA,
- the regulations which determine whether uncertified RPA use is permissible are complex. Many RPA operators, particularly those that do not have an aviation background, may find the regulations confusing or burdensome, or may lack the capacity to adequately assess whether a given situation permits uncertified commercial use,
- compliance with CASR 101 is entirely reliant on operator awareness of the regulations. A pamphlet outlining the standard RPA operating

conditions may be sufficient for recreational users, but commercial operators require more comprehensive information, and

- in future, the pace of technological development may render the standard operating conditions more onerous than necessary for air safety. Active and ongoing review processes will be required to ensure that the regulations remain appropriate.

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

A

Appendix A – Witnesses appearing at roundtables and public hearings

Friday, 28 February 2014 – Canberra, ACT (roundtable)

Airservices Australia

Mr Sean Lake, Acting Manager, National Operations Centre

Australian Association of Unmanned Systems

Ms Peggy MacTavish, Executive Director

Australian Certified UAV Operators Association

Mr Brad Mason, Secretary

Australian Federal Police

Commander Mark Harrison, Manager, Forensic Operations

Mr Peter Whowell, Manager, Government Relations

Australian Law Reform Commission

Professor Barbara McDonald, Commissioner

Australian Pork Limited

Ms Deborah Kerr, General Manager, Policy

Australian Privacy Foundation

Dr Roger Clarke, Chair

Australasian Fire and Emergency Service Authorities Council

Mr Richard Alder, General Manager, National Aerial Firefighting Centre

Civil Aviation Safety Authority

Mr John McCormick, Director of Aviation Safety

Mr Grant Mazowita, Manager, Standards Development and Quality Assurance

Ms Cheryl Allman, Acting Executive Manager, Airspace and Aerodrome Regulation Division

Mr Terry Farquharson, Deputy Director of Aviation Safety

Commonwealth Scientific and Industrial Research Organisation

Dr Jonathan Roberts, Research Program Leader, Autonomous Systems

Individuals

Dr Reece Clothier

Dr Luis Mejias Alvarez, Senior Lecturer, Australian Research Centre for Aerospace Automation, Queensland University of Technology

Mr Geoffrey Holland

Mr Mark Corcoran

Minerals Council of Australia

Mr Chris James, Assistant Director, Workforce Skills

Office of the Australian Information Commissioner

Mr Timothy Pilgrim, Privacy Commissioner

Ms Angelene Falk, Assistant Commissioner

Parrot ANZ

Mr Chris Roberts, Managing Director

VidiAir

Mr Anthony Hoy, Director

Voiceless

Mr Emmanuel Giuffre, Legal Counsel

Thursday, 20 March 2014 - Canberra, ACT (roundtable)

Attorney-General's Department

Mr Andrew Walter, Assistant Secretary, Commercial and Administrative Law Branch

Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch

Mr Colin Minihan, Principal Legal Officer, Private Sector Privacy Section, Commercial and Administrative Law Branch

Ms Danica Yanchenko, Senior Legal Officer, Private Sector Privacy Section, Commercial and Administrative Law Branch

Friday, 21 March 2014 – Brisbane, QLD (roundtable)

AgForce Queensland

Mrs Marie Vitelli, Policy Officer

Australian Research Centre for Aerospace Automation, Queensland University of Technology

Professor Duncan Campbell, Director

Department of Agriculture, Fisheries and Forestry

Mr Salvo Vitelli, Manager, Partnering and Engagement (Biosecurity Queensland)

Department of State Development, Infrastructure and Planning

Mr Lindsay Pears, Envoy, Defence Industries Queensland

Mr Malcolm Lane, Director, Defence Industries Queensland

Individuals

Professor Des Butler, Professor of Law

Insitu Pacific

Mr Dale McDowall, Director, Business Development

Mr Damen O'Brien, Senior Contracts Manager

MultiWiiCopter

Mr Quinton Marais, Director

Queensland Fire and Emergency Services

Assistant Commissioner John Watson, Assistant Commissioner, Brisbane Region

Queensland Police Service

Superintendent Brian Huxley, Superintendent, Operations Coordinator, Forensic Services Group, Operations Support Command

Inspector Brad Wright, Specialist Response Coordinator, Specialist Response Group, Operations Support Command

Thursday, 29 May 2014 – Canberra, ACT (public hearing)

Civil Aviation Safety Authority

Mr John McCormick, Director of Aviation Safety

Mr Peter Boyd, Executive Manager, Standards Division

Mr Jim Coyne, Manager, Future Technology and Regulatory Trends

Mr Terry Farquharson, Deputy Director of Aviation Safety

Mr Grant Mazowita, Manager, Standards Development and Quality Assurance

B

Appendix B – Additional inquiry documents

1. **Civil Aviation Safety Authority –** Response to Questions on Notice taken at 28 February roundtable

2. **Australian Pork Limited –** Response to Questions on Notice taken at 28 February roundtable

3. **Attorney-General's Department –** Response to Questions on Notice taken at 20 March public hearing

4. **Queensland Police Service –** Response to Questions on Notice taken at 21 March roundtable

5. **VidiAir Pty Ltd –** Summary of RPA safety audit

In addition, the Committee received several items of correspondence relating to the inquiry.

C

Appendix C – Civil Aviation Safety Authority drone safety pamphlet

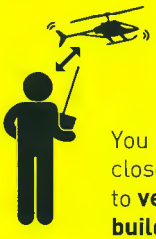
Australian Government
Civil Aviation Safety Authority

FLYING WITH CONTROL?

Get to know the rules.

IMPORTANT SAFETY INFORMATION

Congratulations on your purchase. We hope you have a lot of fun with it but there are just a few things you need to remember for everyone's safety.

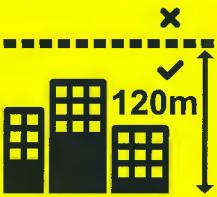


You must only operate this aircraft in your line-of-sight in daylight. **Don't let it get too far away from you.**

You must not fly closer than **30 metres** to **vehicles**, **boats**, **buildings** or **people**

You must not fly over **any populous area**, such as beaches, other people's backyards, heavily populated parks, or sports ovals where there is a game in progress

If you are in controlled airspace, which covers most Australian cities, you must **not fly higher** than 400 feet **(120 metres)**



You should not fly within **5.5 km of an airfield**.

It's illegal to fly for money or economic reward unless you have an UAV operator's certificate issued by the Civil Aviation Safety Authority (CASA).

Safe and happy flying!

Further information

Model Aeronautical Association of Australia
www.maaa.asn.au

CASA
» Model aircraft: **casa.gov.au/sportaviation**
» Remotely piloted aircraft: **casa.gov.au/rpa**
» Phone: **131 757**

1309.1818