The Use of Drones in Australia

AN AGENDA FOR REFORM

The Use of Drones in Australia: An Agenda for Reform
May 2015

A proposal prepared jointly by Reece Clothier and Peggy MacTavish of the Australian Association for Unmanned Systems and Matthew Albert, Michael Griffith and Marius Smith of Liberty Victoria. The authors thank the King & Wood Mallesons Human Rights Law Group for its assistance in preparing this proposal. Any errors or omissions are the authors' alone.

Overview

Australian privacy law regulating the use of drones and surveillance is not fit for purpose. Rapid technology change is putting many harmful kinds of surveillance beyond the law's reach. At the same time, valuable new uses of surveillance technology are being held back because the law lacks certainty.

In response to public concerns about the proliferation of new surveillance technologies, the Australian Association for Unmanned Systems and Liberty Victoria have joined to call for Australian surveillance law to be modernised and harmonised. We do so as trusted representatives of the unmanned systems and human rights communities respectively.

This proposal recommends reforming surveillance law to balance two key objectives: the need to protect Australians against harmful surveillance activity, and the need to provide certainty about lawful use of surveillance technology – in particular, valuable social and economic uses. In our view, this balance is best struck through incremental reform to existing state and territory surveillance devices legislation.

Our proposal calls for surveillance law to be harmonised and placed on a technology neutral footing. Individuals should have the right to seek redress for harmful surveillance. Penalties should be revised to reflect the increased scope of harm surveillance can cause. Lawful uses should be protected through clear, consistent exemptions. And existing state and territory regulators should be empowered to enforce the law and facilitate fast, low-cost dispute resolution.

This package of reform would put Australian surveillance law a step ahead of the technology horizon. It would encourage the development of Australia's unmanned systems industry and ensure that valuable commercial and social use of unmanned systems can be undertaken without fear of breaking the law. It would also give Australians confidence that those using surveillance for harmful ends will face appropriate consequences.

On behalf of all Australians concerned about the changing frontier of surveillance, the Australian Association for Unmanned Systems and Liberty Victoria urge Federal, state and territory governments to put surveillance law reform on the agenda.

Associate Professor KC Wong
President, Australian Association for Unmanned Systems

Jane Dixon SC
President, Liberty Victoria

Contents

This proposal is in five parts:

- **Part 1** summarises challenges for the regulation of drones arising from the current legislative landscape and our recommendations to government.
- **Part 2** describes unmanned systems and identifies some of the positive and negative implications of new surveillance technologies.
- **Part 3** describes the laws that currently regulate drones in Australia and identifies gaps where these laws fail to protect against serious privacy breaches and other kinds of drone misuse.
- **Parts 4 and 5** set out reforms to protect the privacy and safety of citizens against drone misuse, while ensuring valuable social and economic uses of such technology are not unduly restricted.

Note on terminology

In this proposal, we use the term "**unmanned systems**" to denote technology that is elsewhere described as drones, robot or remote controlled planes, pilot-less aircraft and remotely piloted vehicles or aircraft.

Beyond airborne craft, "**unmanned systems**" extends to unmanned ground and maritime systems, and to any system architecture used to control or view the output of the unmanned device (for example, surveillance video output).

> UNMANNED SYSTEMS TECHNOLOGY IS A POSITIVE TECHNOLOGICAL ADVANCEMENT BUT LIKE OTHER ADVANCEMENTS MUST BE GOVERNED RESPONSIBLY, INCLUDING PRIVACY
>
> Peggy MacTavish, AAUS

01 Executive summary Page six

02 Unmanned systems and other new surveillance technologies Page eight

03 Gaps in the regulation of unmanned systems Page eleven

04 Protecting privacy and safety without restricting beneficial and legitimate use of unmanned systems Page thirteen

05 Extending the functions of privacy regulators Page nineteen

06 Appendix: current regulation of unmanned systems Page twenty four

This package of reform would put Australian surveillance law a step ahead of the technology horizon

1. Executive summary

1.1 The need for harmonised surveillance laws

Unmanned systems, or drones, are well known for their military applications but over the past decade have also become increasingly prominent in civilian, commercial and social spheres. These technologies are playing an increasingly beneficial role across numerous domestic applications: from aerial photography and surveying crops and livestock, to monitoring natural disasters and law enforcement.[1] Falling cost, widening availability and expanding functionality is accelerating the trend.

Unmanned systems are a prominent example of a broader development: the emergence of new surveillance technologies and new uses of such technology. This development is challenging the boundaries and efficacy of existing legal frameworks and raising a range of social and ethical concerns.[2] Chief among these are the implications of broad-ranging, invasive and covert surveillance. Current debates about the use of such surveillance by government are set to widen as access to the technical means of such surveillance widens. Privacy is one of the greatest concerns, with questions arising as to how the civilian transition of these technologies will affect privacy laws and rights.[3]

The regulatory landscape in Australia is piecemeal and ill-equipped to deal with emerging surveillance technologies.[4] Federal privacy legislation generally only covers Federal agencies and large private sector organisations, and surveillance devices laws vary across the states and territories. Common law torts, such as trespass, provide limited redress.

This proposal is the result of collaboration between the Australian Association for Unmanned Systems and Liberty Victoria. We join the growing call for reform to fix the regulatory gaps through which new surveillance technology is falling. We have collaborated on this proposal out of common interest in ensuring that such reform provides both adequate protections against unreasonable and harmful invasions of privacy, and certainty to the unmanned systems industry about lawful uses of surveillance technologies.

We offer nine recommendations for reform in this proposal, some involving draft legislative provisions. These recommendations are not exhaustive of the legislative reform required, but rather set out the core substantive issues that we see as necessary in achieving meaningful progress towards harmonisation, clarity and effective regulation of unmanned systems and other new surveillance technology.

Essentially, we propose the extension, consolidation and harmonisation of Australia's existing state and territory based surveillance devices laws. We propose two general prohibitions that regulate:

- the installation or use of surveillance devices; and
- the communication or publication of private records obtained through the prohibited installation or use of surveillance devices.

These prohibitions should be subject to broad exceptions to protect legitimate and beneficial surveillance purposes. They should be technology-neutral to capture current and future

---

1 Brendan Gogarty and Meredith Hagger, 'The Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air' (2011) 19(1) *Journal of Law, Information and Science* 73.

2 Ibid 73.

3 Ibid 125.

4 House of Representatives Standing Committee on Social Policy and Legal Affairs, Parliament of Australia, *Eyes in the Sky: Inquiry into Drones and the Regulation of Air Safety and Privacy* (2014).

technologies. We also propose two further prohibitions that address intimidation, harassment, hindrance or harm caused to a person under surveillance.

Existing privacy or personal information regulators should play an important role in handling and conciliating complaints, and we believe that it is more appropriate to extend the functions of these bodies to administer a harmonised regime than to create a new regulator. We propose that substantive complaints be referred to the relevant state or territory administrative tribunal.

As the Federal, state and territory governments grapple with reform, we wish, in particular, to emphasise the need to act quickly and consistently, the need to appropriately balance the beneficial uses of surveillance technologies against community expectations of privacy, and the need to formulate an informed and workable system of harmonised rules that draws on community concern, industry knowledge and established policy best practice.

1.2 Summary of recommendations in this proposal

1. The Federal, state and territory governments should develop and adopt an intergovernmental agreement in relation to the regulation of surveillance devices. This agreement should establish a cooperative scheme requiring the parties to enact surveillance devices legislation that incorporates a uniform set of provisions.

2. The scope of 'surveillance devices' regulated by the uniform provisions should apply broadly to current and future technologies, covering any device capable of being used to monitor, observe, overhear, listen to or record an activity, or to determine or monitor the geographical location of a person or an object.

3. The uniform provisions should contain a general prohibition, with civil penalties, on surveillance of private activity using a surveillance device without consent that involves:
   - a mental requirement of intent or recklessness;
   - an understanding that each person holds a reasonable expectation of privacy with respect to certain activities and locations but not others; and
   - appropriate exceptions drawn from current surveillance devices laws to protect beneficial surveillance.

4. The general prohibition should protect 'private activity', which should include any activity where it would be reasonable that those engaged in the activity expected to be observed or overhead only by themselves, but not include activity where a person ought reasonably to have expected to be observed or overheard.

5. The uniform provisions should also contain a prohibition, with civil penalties, on the communication or publication of private records.

6. The term 'private record' should encompass any information obtained through the prohibited installation or use of a surveillance device.

7. The uniform provisions should contain two further prohibitions, with civil and criminal penalties, for intimidation, harassment, hindrance or harm caused to a person by the installation or use of a surveillance device.

8. A person subject to prohibited conduct under the uniform provisions should have the right to make a complaint to the relevant state or territory privacy regulator, who may reject, investigate or conciliate the complaint. On request of a complainant, complaints that cannot be conciliated should be determined by the relevant Tribunal.

9. Where a complaint is proven, the Tribunal should have jurisdiction to make orders including an order restraining the conduct, that the respondent redress the loss, damage or humiliation suffered, that the respondent pay compensation, or that no further action be taken.

2 Unmanned systems and other new surveillance technologies

Unmanned systems were originally developed for military use in the first half of the 20th century. Military operators, who are generally at the forefront of technological developments in the area, are still the main users of unmanned systems however the debate about military uses of unmanned systems is not the focus of this proposal, which is limited to domestic uses of unmanned systems technology within Australia.

Unmanned systems have become increasingly prominent in the civilian sphere as the technology has rapidly matured and prices fallen. In this context, unmanned systems are principally used for cinematography or aerial photography, civil services (eg fire fighting) and recreation.

The current technological frontier for unmanned systems reveals increasingly sophisticated, long-range data recording equipment. These devices can operate in the air, at land or at sea, and for periods far longer and in conditions far beyond the capability of traditional surveillance devices. The technology supporting airborne equipment is also rapidly evolving: researchers at the United States Naval Research Laboratory have managed to fly an 'Ion Tiger' unmanned system non-stop for over 48 hours.[5]

2.1 Unmanned systems currently in use for surveillance purposes

Unmanned systems range significantly in size: from insect-like technology to systems the size of commercial aircraft. They also range in sophistication: from 'consumer-class' technology, with basic functionality, to multi-million dollar systems with advanced sensing payloads.

Commercial bodies, not-for-profits and law enforcement agencies are increasingly employing unmanned systems for information gathering purposes. Civilian uses tend to be less sophisticated than military uses, with greater reliance on lighter, smaller and cheaper devices. Uses of unmanned systems have, however, expanded exponentially in line with rapid technological growth and falling cost. Current civilian uses of unmanned systems include:

- deployment by fire and emergency services (for example, the Melbourne Metropolitan Fire Brigade) for situational awareness at large fires;
- deployment by law enforcement agencies (for example, to identify drug crops, monitor traffic and crowds, disarm explosive devices and to monitor high risk situations[6]);
- deployment by emergency authorities (for example, to spot and monitor natural disasters where it is too risky to send a person);
- deployment by surf lifesaving clubs and coast guards (for example, to assist in identifying aquatic dangers and locating missing individuals or boats);
- capturing unique camera angles (for example, at sporting events); capturing events at sea (for example, to monitor populations and species of marine life);
- real estate and conveyancing (for example, to capture a multi-angle view of a property); and
- agricultural use to survey crops and livestock, allowing for rapid and often automated responses to variations in weather or operating conditions.

2.2 The future use of unmanned systems: the unchartered frontier

It is only in recent years that unmanned systems have started to fall within the reach of individual consumers from a financial, logistical and technological perspective. Just years ago, a small

[5] United States Naval Research Laboratory, 'NRL Shatters Endurance Record for Small Electric UAV' (9 May 2013), available at <http://www.nrl.navy.mil/media/news-releases/2013/nrl-shatters-endurance-record-for-small-electric-uav>.

[6] For example, in December 2013, Queensland police used a UAV to monitor a siege situation for the first time: <http://www.brisbanetimes.com.au/queensland/police-eye-in-the-sky-offers-remote-possibilities-20131228-300nt.html>

unmanned system would have cost thousands of dollars; today, for less than $250 Australian consumers can purchase an unmanned system featuring a high-definition camera, microphone and ultrasound altimeter, that can be remotely controlled via a mobile phone or tablet. As the technology continues to mature and prices continue to decrease, these systems are likely to proliferate.

While it is impossible to predict exactly how unmanned systems may be used in the coming years, anticipated uses are plentiful. Unmanned systems could be employed:

- by property owners and private security companies to autonomously survey their property;
- by private investigators for surveillance;
- by animal rights and environmental activists to investigate and substantiate issues of concern to them;
- for search and rescue;
- to assess dangerous or unstable premises;
- to detect and monitor invasive species;
- to improve media coverage in war and disaster zones without endangering journalists;
- for the autonomous transportation of air-freight, legitimate or otherwise;7 and
- for the delivery of emergency supplies.

2.3 Surveillance technologies

Unmanned systems are an example of many new and emerging technologies capable of recording personal information. Examples of such technologies include:

- increasingly high definition and concealable audio-visual recording devices such as those in modern mobile phones, tablets and other portable electronic devices;
- increasingly accurate location and tracking devices utilising global positioning system (GPS) and radio frequency identification (RFID) technology;
- automatic number plate recognition technology;
- body imaging devices and scanners;
- facial recognition and lip reading technology;
- 'stingray' devices, which act as a fake telecommunications network to capture mobile phone voice and data communications from targeted users;
- satellite imagery services such as Google Earth, a free online database of satellite images which provides a bird's eye view of a location, searchable by landmark or address;
- street mapping technologies such as Google Streetview, which provides a curb-side view of streets and other locations captured by vehicles with rooftop-mounted cameras; and
- Google Glass, a pair of technologically advanced glasses with an inbuilt computer overlay which can record audio-visual information as experienced by the user.

With increasingly smaller, faster, more accurate, longer lasting and cheaper data recording capabilities, devices capable of recording all forms of information are now readily available. In addition, these devices are increasingly combined with an outgoing data connection, meaning that recorded data can be easily (even automatically) transmitted to a remote user, or shared with others via the Internet, at little cost. The modern mobile phone is the most obvious manifestation of this, and now combines telephone services with GPS tracking software, digital visual and audio recording capabilities and Internet connectivity.

[7] Alison Caldwell, 'Drone allegedly used in attempt to smuggle drugs into Melbourne prison' *ABC News*, 10 March 2014 <http://www.abc.net.au/news/2014-03-10/police-have-charged-a-man-after-a-drone-was-found-over-a-melbou/5309798>.

2.4 The problem stated

In the past, traditional surveillance devices were largely limited by the high cost of the technology and by physical capabilities, namely the requirements of:

- physical proximity (for example, requiring the user to press a button to activate a device, such as a point-and-click camera); and
  physical access, usually in order to install a surveillance device (for example, a microphone or camera) which cannot easily be done on private property.

As the technological frontier expands, surveillance devices have started to move beyond these physical limits. Many devices now operate on a semi-autonomous basis (for example, starting to record information when a stimulus such as light or sound is detected). Other devices can be remote-controlled by the user, who can choose to activate recording capabilities by observing what the mobile surveillance device can 'see' or 'hear'. In these cases, no physical proximity is required to create a recording.

There is nothing inherently negative about the evolution of these technologies. Indeed, there are vast productive and positive uses of these technologies in criminal investigations, asset protection, public safety and operational business needs. However, the sheer scale on which mobile surveillance devices — including unmanned systems — currently or will soon exist, dramatically increases the scope for these technologies to be used in ways inconsistent with community expectations and understandings of privacy.

3 Gaps in the regulation of unmanned systems

The expansion of surveillance technologies has created gaps where Australia's civil and criminal laws do not address new forms of unwanted conduct. As the Australian Privacy Commissioner, Timothy Pilgrim, noted in his call for a review of regulation in response to drone technologies:

> Where an agency or private sector organization covered by the *Privacy Act* intends to use drone technology, it must do so in accordance with the *Privacy Act*. This would include giving notice to affected individuals about the collection of their personal information, only using and disclosing the personal information as permitted by the *Privacy Act*, and keeping it secure. The *Privacy Act* does not however cover the actions of individuals in their private capacity, including any use of drones by individuals.[8]

Nor does the *Privacy Act 1988* (Cth) cover the actions of most private sector organisations with an annual turnover of less than $3 million.

3.1 Gaps in privacy and surveillance laws

The use of unmanned systems serves to expose a number of gaps in Australia's privacy and surveillance regulatory framework.

The Civil Aviation Safety Authority ("**CASA**") established the first operational regulation for unmanned aircraft in the world. These regulate where and how unmanned aircraft, including unmanned aerial vehicles ("**UAVs**"), may be used, and focus primarily on ensuring safety. CASA has announced plans to update these regulations and apply different limitations to separate weight classes of UAVs. CASA's Director has stated that privacy issues arising from the use of UAVs are matters for the Australian Privacy Commissioner.

The *Privacy Act 1988* (Cth) regulates the way personal information is collected and handled by Federal and ACT agencies, Federal government contracted service providers and private sector organisations. Individuals and most small business operators with an annual turnover of less than $3 million who collect personal information are not subject to this law. The Australian Capital Territory, Northern Territory, New South Wales, Queensland, Tasmania and Victoria have enacted similar legislation in relation to their own agencies. Due to the drafting of such existing legislation, most uses of unmanned systems are unlikely to result in the collection of personal information that is regulated.

Individuals and companies may sue other parties using unmanned systems for trespass to property or negligence. However, there is no established right to sue for an invasion of privacy, such as observing another person's private activities.

Criminal law has established some limitations on the acceptable use of unmanned systems, but these vary across the states and territories. Offences that may apply to a person using an unmanned system include criminal negligence causing injury to a person or property, observing a person's sexual acts or genital regions, stalking by means of surveillance, and assault. However, these offences are limited to a small range of particularly offensive conduct.

The regulation of surveillance technologies, including unmanned systems, is most obviously contemplated in Australia's surveillance devices legislation. However, the laws in each state and territory differ regarding the types of technology covered (several are limited to regulating listening devices only), the persons regulated (some relate only to use by law enforcement agencies), the types of activities that cannot be recorded, and the penalties. As the Australian Privacy

[8] Timothy Pilgrim (Australian Privacy Commissioner), 'Correspondence: Attorney-General: Regulation of drone technology September 2012' (September 2012) available at < http://www.oaic.gov.au/news-and-events/statements/privacy-statements/regulation-of-drone-technology/correspondence-attorney-general-regulation-of-drone-technology-september-2012>.

Commissioner has noted: 'individuals who may be subject to surveillance via drone technology may not currently be able to seek appropriate or consistent redress across the Commonwealth'.[9]

The picture that emerges is a piecemeal and fragmented regulatory landscape which fails to adequately address the privacy implications raised by the technology discussed in Part 2.[10] Indeed, the following arguably inappropriate uses of new surveillance technologies are currently permitted by law:

- A person could film a neighbour in New South Wales or Victoria over the back fence engaging in a private activity.
- A peeping tom can take photos looking down the tops of those coming up a shopping centre escalator on their mobile phone in Victoria.[11]
- A person could hide a mobile phone in the boot of their ex-partner's car to track their location in Victoria (but not if that person drove to NSW).
- A rival company's unmanned system could record a business plan on a whiteboard at another company's board strategic planning retreat in NSW.
- A real estate business preparing an aerial sales video could accidentally film a person skinny-dipping in his or her own swimming pool and post it on Youtube.

The Parliamentary Roundtable on Drones and Privacy, which tabled its report in July 2014, found that the piecemeal nature of existing privacy regulation results in inadequate protection of privacy rights and creates confusion and uncertainty as to the law's scope and effect. This in turn hinders access to remedies for breaches of privacy and makes it more difficult for UAV operators to comply with the law.[12]

4 Protecting privacy and safety without restricting beneficial and legitimate use of unmanned systems

Australian privacy and surveillance laws are, evidently, not comprehensive enough to ensure that unmanned systems and other new surveillance technologies will be used responsibly and consistently. These smaller, cheaper and portable devices allow for pervasive surveillance in a way not contemplated by previous legislation, and in a way that may lessen the privacy that Australians have traditionally enjoyed in their activities and movements.

Australia needs a new system of rules to ensure that we can enjoy the benefits of these technologies without unduly impacting on privacy.

As the Federal, state and territory governments grapple with reform, it is important to recognise the wide range of competing objectives and risks, including:

- the need to act quickly and consistently;
- the risk of diminished public confidence in the ability of legislators to protect the right to privacy and regulate new technologies;
- the risk, in the absence of legislative intervention, of the normalisation of previously unacceptable levels of surveillance;

[9] Ibid.

[10] Further details of Australia's current regulatory framework regarding unmanned systems are set out in Part 6 below.

[11] In some jurisdictions this activity could already fall within the definition of the criminal offence of stalking.

[12] House of Representatives Standing Committee on Social Policy and Legal Affairs, Parliament of Australia, *Eyes in the Sky: Inquiry into Drones and the Regulation of Air Safety and Privacy* (2014).

- the need to appropriately balance the beneficial uses of surveillance technology against the right to privacy;
- the need to formulate an informed and workable system of rules that draws on industry knowledge and policy proficiency; and
- the need to ensure that undue financial or regulatory burden is not placed on individuals or businesses.

We call for practical, clear and easily accessible laws detailing where, when and how unmanned systems and other surveillance technologies can be used.

Considering the gaps in the existing legislative provisions identified above, it is apparent that an entirely new legal framework is unnecessary. The reforms that we propose simply extend and consolidate Australia's existing surveillance devices laws incrementally to capture current and developing technologies and to ensure that any misuse of these technologies is subject to appropriate consequences and penalties. We believe that these reforms will:

- increase community confidence by giving individuals an avenue for meaningful redress when faced with the misuse of surveillance technologies; and
- provide certainty to the emerging unmanned systems industry by providing clear and consistent standards for lawful use across Australia.

4.1 Advancing national consistency

We propose a consolidation and simplification of the current legal framework through the introduction of a nationally consistent surveillance devices regime. This will ensure that private activities are sufficiently protected and respected in this age of rapidly developing technology. Ensuring national consistency will also assist:

- individuals subject to surveillance in determining what their rights are and how to enforce them;
- individuals, businesses and other bodies in understanding and efficiently complying with their obligations with respect to the installation or use of surveillance devices, particularly where such use extends across jurisdictional boundaries; and
- regulators in managing reviews and providing remedies.

We are mindful of the need for flexibility, particularly in defining the devices to which the legislation should apply. Effectiveness and consistency across jurisdictions can only be achieved if the legislation is flexible enough to accommodate the different interests, practices and accountability of those involved. Particular sectors, such as law enforcement and emergency response, require specific regulations and exceptions. Although we recognise the importance of such considerations, any detail in these areas goes beyond the scope of this proposal and we do no more than note the existing warrant-based regimes currently in operation.

National consistency can be achieved in a number of ways, however we suggest that the most appropriate way is through the adoption of a cooperative scheme in which each state and territory passes uniform legislation. Containing key elements such as the relevant definitions, prohibitions and exceptions, these laws would regulate surveillance devices equally across the country.

While there would be advantages in having a single, national surveillance devices law administered by a single regulator, we note concerns relating to the need for state and territory legislation to work with local conditions and existing laws. We also recognise the advantages of having existing state and territory regulators handle complaints, impart advice and undertake educational functions. Accordingly, it is our view that the Federal Parliament should exercise its legislative

power only in relation to the handling of surveillance devices by the Australian Federal Police and Federal agencies, as it does currently under the *Surveillance Devices Act 2004* (Cth).

> **Recommendation One**
> The Federal, state and territory governments should develop and adopt an intergovernmental agreement in relation to the regulation of surveillance devices. This agreement should establish a cooperative scheme requiring the parties to enact legislation that incorporates a standard set of provisions concerning surveillance devices.

4.2 Characterising surveillance devices

While surveillance has been said to be 'at least as old as recorded history',[13] technological developments and the wider availability of surveillance devices generate significant privacy risks.[14] The growth and increased sophistication of modern surveillance devices not only makes it imperative to introduce some legislative control on their installation and use,[15] but also makes it necessary to define such devices broadly so as to accommodate for current and future technologies. Any definition of the term 'surveillance device' should therefore be technology neutral, that is, the rules 'should neither require nor assume a particular technology'.[16] For example, there should be no distinction between those devices that are able, and those devices for which the primary purpose is, to monitor a private activity or the geographical location of a person or an object.[17] As discussed previously, modern devices can perform a range of roles, and we believe that it is important to prohibit invasions of privacy where any device is used inappropriately.

> **Recommendation Two**
> The term 'surveillance device' should be defined broadly to cover both current and future technologies. We propose the following:
> ***surveillance device*** *means any device capable of being used to:*
>
> *(a) monitor, observe, overhear, listen to or record an activity; or*
>
> *(b) determine or monitor the geographical location of a person or an object.*

4.3 Restricting the installation or use of surveillance devices

As we have noted, the laws regulating surveillance devices are fragmented and inconsistent across Australia, causing confusion and failing their purpose to safeguard Australians from invasions of privacy. This problem is best rectified through amending current surveillance devices laws to include a general prohibition on surveillance of private activity using a surveillance device without consent.

This general prohibition should involve *a mental requirement of intent or recklessness* to avoid capturing unintended or innocent surveillance. For example, a family member may inadvertently capture a stranger breastfeeding when taking photos of their relative and his or her newborn child

---

13 New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report No 98 (2001) [1.18].

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) [9.89].

15 Australian Law Reform Commission, *Privacy*, Report No 22 (1983) 1187.

16 Chris Reed, 'Taking Sides of Technology Neutrality' (2007) 4(3) *SCRIPTed* 263 <http://www2.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp> 266.

17 For example, section 3 of the *Surveillance Devices Act 1999* (Vic) currently defines a tracking device as 'an electronic device the primary purpose of which is to determine the geographical location of a person or object' and therefore excludes modern mobile phones.

in a maternity ward – this should not provide the stranger in question with a legal right of complaint.

Secondly, the prohibition should be restricted to instances where people have *a reasonable expectation of privacy*. In *R v Broadcasting Standards Commission*,[18] Lord Mustill attempted to delineate the essence of privacy as follows:

> To my mind the privacy of a human being denotes at the same time the personal 'space' in which the individual is free to be itself, and also the carapace, or shell, or umbrella, or whatever other metaphor is preferred, which protects that space from intrusion. An infringement of privacy is an affront to the personality, which is damaged both by the violation and by the demonstration that the personal space is not inviolate.

The prohibition should apply to these 'personal spaces' in which each person should feel free to express him or herself: in the home, while talking to close friends, while meeting another in a technically public yet secluded space. Current surveillance devices laws address this issue by defining what constitutes a 'private conversation' and a 'private activity'. We see these classifications as useful guides in determining what is and is not a reasonable expectation of privacy, but seek to integrate them into a single, broader concept of 'private activity' that encompasses all visual or verbal communications.

Thirdly, the prohibition should be subject to appropriate exceptions. Some forms of surveillance are beneficial and/or necessary and should be permitted in certain circumstances. For example, participant monitoring, whereby a person records a private activity to which they are a party, may help a person to protect their lawful interests in commercial and domestic contexts. It has been used in domestic violence and family law situations, such as when a woman records her ex-partner's communications with her as evidence of breach of an intervention order.[19] Other well-recognised exceptions include surveillance undertaken in accordance with a warrant or with the express or implied consent of one of the parties.

Recommendation Three

The uniform provisions should contain a general prohibition on the installation or use of surveillance devices. This should involve:

- a mental requirement of intent or recklessness;
- an understanding that each person holds a reasonable expectation of privacy with respect to certain activities and locations; and
- appropriate exceptions drawn from current surveillance devices laws.

We propose the following:

(1) A person must not intentionally or recklessly install or use, or cause to be installed or used, a surveillance device to:

(a) monitor, observe, overhear, listen to or record a private activity without the express or implied consent of each party to that activity; or

(b) determine the geographical location of:

(i) a person without his or her express or implied consent; or

(ii) an object without the express or implied consent of a person in lawful possession or having lawful control of that object (except for the sole purpose of retrieval of that object to its owner).

Civil penalty: _____.

[18] [2001] QB 855, 48.

[19] Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 117 [6.59].

(2) Subsection (1) does not apply to the installation or use of a surveillance device:

(a) authorised or required by law;

(b) by a person acting in their capacity as a police or public officer, provided such conduct was neither disproportionate to the activity nor committed in the course of a trespass;

(c) reasonably necessary to protect a person from significant harm; or

(d) in the public interest.

Recommendation Four

The term 'private activity' should encompass any interaction or communication between the parties. We propose the following:
***private activity** means any activity (including any communication) conducted in circumstances that may reasonably be taken to indicate that any or all of the parties to it expected it to be observed or overheard only by themselves, but does not include an activity carried on in any circumstances in which the parties to it ought reasonably to expect that it may be observed or overheard by someone else.*

4.4 Restricting the communication or publication of private records

Current surveillance devices laws contain separate prohibitions regarding the installation or use of surveillance devices and the communication or publication of private records obtained through the prohibited installation or use of surveillance devices. These should continue as two separate offences because:

- the person who communicates or publishes the private record may not necessarily be the person who originally installed or used the surveillance device, but should nonetheless be held responsible for intentionally or recklessly making the private record known to others; and
- the communication or publication of the private record is an additional breach of the right to privacy.

Surveillance devices laws in New South Wales, Victoria and Western Australia use the terms 'record' or 'report' to describe private information obtained through the prohibited installation or use of surveillance devices.[20] We believe that a considered definition of 'private record' can be used to effectively integrate these concepts.

Consistent with the general prohibition on the installation or use of surveillance devices, this prohibition should include a mental requirement of intent or recklessness and be subject to appropriate exceptions.

[20] See *Surveillance Devices Act 2007* (NSW) s 11; *Surveillance Devices Act 1999* (Vic) s 11; *Surveillance Devices Act 1998* (WA) s 9.

Recommendation Five

Drawing on current surveillance devices laws, the uniform provisions should include a prohibition on the communication or publication of private records. We propose the following:

(1) Subject to subsection (2), a person must not intentionally or recklessly publish or communicate to any person a private record without the consent of each party reasonably identifiable from that record.
Civil penalty: _____.
(2) Subsection (1) does not apply to publication or communication:

(a) authorised or required by law;

(b) by a person acting in their capacity as a police or public officer, provided such conduct was neither disproportionate to the matter being investigated nor committed in the course of a trespass;

(c) reasonably necessary to protect a person from significant harm;

(d) in the public interest;

(e) by a person who did not know or was not reckless as to whether the record was a private record; or

(f) of a private record that has entered the public domain.

Recommendation Six

The term 'private record' should be used to describe any information obtained through the prohibited installation or use of a surveillance device. We propose the following:

***private record** means a record of:*

(a) a private activity; and/or

(b) the geographical location of a person or an object,

that has been made as a direct or indirect result of the use of a surveillance device.

4.5 Acknowledging harm caused

The offences proposed in Recommendations 3 and 6 focus largely on the intention of the offender and apply regardless of the consequences to any 'victim' of the prohibited conduct. We recommend that there be two further prohibitions, with higher penalties, for conduct that results in particular consequences for a person, in order of increasing severity.

Recommendation Seven
We propose the following:
(1) A person must not use a surveillance device in such a way as to:

(a) intimidate, demean or harass a person of reasonable sensibilities; or

(b) prevent or hinder a person from performing an act they are lawfully entitled to do.
Civil penalty: _____.

Criminal penalty: _____.
(2) A person must not engage in conduct prohibited under [the provisions in Recommendations 3 and 6] and thereby cause psychological or physical harm to another person.

Civil penalty: _____.

Criminal penalty: _____.

5 Extending the functions of privacy regulators

In protecting privacy and safety through the establishment of a cooperative scheme on surveillance devices, it is more appropriate to extend the functions of existing privacy or personal information regulators than to create a new regulator. This approach is more cost-effective and should minimise the regulatory burden on government agencies and organisations.[21] With current regulatory and educative roles in relation to the privacy of personal information, these regulators are 'an obvious choice'.[22] The Victorian Privacy Commissioner, in a submission to the Victorian Law Reform Committee, has demonstrated support for this approach in relation to public place surveillance:

> While I have no settled view as to who should perform this independent regulatory role, a number of the proposed functions are similar to those currently bestowed on the Victorian Privacy Commission by the [Information Privacy Act 2000 (Vic)], which include some regulation of surveillance when undertaken by Victorian public sector agencies or contracted service providers. It may therefore make sense, in the absence of a new, specialist, independent regulator, for the functions to be added to these.[23]

Individuals can currently make privacy complaints to a range of different regulatory bodies under any applicable Federal, state and territory laws.[24] We note the differences in these arrangements, and call attention to the fact that we have developed the recommendations below based on the workings of the Victorian Privacy Commission and Commissioner. The functions of existing privacy or personal information regulators in each jurisdiction can and should be extended in these ways. For the purpose of this proposal, the relevant body will be collectively referred to as the 'Privacy Commission', as represented by the 'Privacy Commissioner'.

5.1 Handling complaints

The Privacy Commissioner should play an important role in handling complaints, and should therefore be the first port of call for those seeking redress. Where a person believes that surveillance devices have been used, either intentionally or recklessly, to capture private activities, they should lodge a written complaint with the Privacy Commission. Administrative costs should be mitigated through an initial complaints lodgement fee, payable to the Privacy Commission.

We recognise that, with the introduction of a nationally consistent surveillance devices regime, complaints may be made in the absence of intention or recklessness. Accordingly, we think that the uniform provisions should provide the Privacy Commissioner with the discretion to distinguish between meritorious and unmeritorious claims. A similar approach is already in place in Victoria, Queensland and the Northern Territory.

The Privacy Commissioner should not entertain complaints where:

- the complainant has not complained to the respondent, and it would be reasonable for the complainant to do so before complaining to the Privacy Commissioner;
- the complaint was made more than 30 days after the complainant became aware of the conduct; or
- the complaint is frivolous, vexatious, misconceived or lacking in substance.

---

21 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 99 [5.99].

22 Ibid [5.100].

23 Submission 29, Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 100 [5.101].

24 See, for example, *Privacy and Personal Information Protection Act 1998* (NSW) s 45 ("Privacy Commissioner"); *Privacy and Data Protection Act 2014* (Vic) s 57 ("Privacy and Data Protection Commissioner"); *Information Privacy Act 2009* (Qld) s 165 ("Information Commissioner"); *Information Act 2002* (NT) ss 103–4 ("Information Commissioner"); *Personal Information Protection Act 2004* (Tas) s 18 ("the Ombudsman").

Where a complainant is unsatisfied with the Privacy Commissioner's decision to reject their complaint, they should be able to apply to the relevant administrative tribunal ("**the Tribunal**") on a question of law. The Tribunal should have to the power to confirm or revoke the decision, remit the matter to the Privacy Commissioner or dismiss the appeal altogether.

In evaluating the merits of a claim, the Privacy Commissioner should exercise their powers to investigate the complaint by requiring that the complainant or a third party provide evidence relating to the potential breach.

5.2 Conciliating complaints

Where the Privacy Commissioner accepts a complaint, the matter should be submitted to conciliation if the Privacy Commissioner believes that it is reasonably possible for the complaint to be successfully conciliated. However, where successful conciliation is unlikely, the Privacy Commissioner should notify the complainant in writing and, at the request of the complainant, refer the matter to the Tribunal for determination.

Recommendation Eight
We propose the following:

(1) A person subject to conduct prohibited under [the provisions in Recommendations 3, 6 or 7 ("the prohibition provisions")] may make a complaint about such conduct to the Privacy Commissioner.

(2) The complaint must be in the form, and accompanied by the fee, specified in the Regulations.

(3) The Privacy Commissioner may at any time reject a complaint by notifying the complainant in writing if the Privacy Commissioner considers that:

(a) the complainant has not made the same complaint in writing to the respondent first (if the respondent is known to, or their identity can be reasonably ascertained by, the complainant) and it would be reasonable for the complainant to do so before complaining to the Privacy Commissioner;

(b) the complaint to the Privacy Commissioner was made more than 30 days after the complainant became aware of the conduct; or

(c) the complaint is frivolous, vexatious, misconceived or lacking in substance.

(4) The Privacy Commissioner may investigate and obtain evidence about a complaint or any other conduct which the Privacy Commissioner considers may constitute a breach of the prohibition provisions.

(5) If the Privacy Commissioner considers it reasonably possible that a complaint may be successfully conciliated, the Privacy Commissioner must make all reasonable endeavours to conciliate the complaint.

(6) If the Privacy Commissioner does not consider it reasonably possible that the complaint may be successfully conciliated, the Privacy Commissioner must notify the complainant and respondent in writing.

(7) If subsection (6) applies, the Privacy Commissioner must, at the request of the complainant, refer the complaint to the Tribunal for hearing.

5.3 Providing appropriate remedies

Although the Privacy Commissioner should be responsible for investigating potential breaches of the uniform provisions, we believe that the Tribunal is the most appropriate forum for the resolution of substantive disputes. Taking the Victorian Civil and Administrative Tribunal, Administrative Decisions Tribunal of New South Wales and Queensland Civil and Administrative Tribunal as examples, the Tribunal is an ideal forum because it is a low cost jurisdiction and is comprised of a broad range of decision makers who have experience in weighing competing interests and shaping the law.[25]

In line with current practice, the Tribunal should have the jurisdiction to make a number of orders after hearing the evidence of the parties, including:

- an order to restrain the respondent from repeating or continuing the practice that gave rise to the dispute (an order equivalent to a mandatory injunction);
- an order for the respondent to redress any loss or damage including injury to feelings;
- an order of compensation not exceeding $100,000 for loss or damage, injury to feelings or humiliation;
- an order that the complainant is entitled to be reimbursed for expenses reasonably incurred in connection with making the complaint and instigating the proceedings; or
- decline to take further action or dismiss the action.

Practically speaking, this means that the respondent may be ordered to remove the surveillance device and compensate the complainant for emotional or mental damage caused. In addition, the Tribunal should be able to make a declaration to the effect that the individual's privacy has been breached as a result of the prohibited installation or use of a surveillance device, or the communication or publication of a private record.

The right to appeal a decision of a Tribunal should remain unchanged.[26]

[25] See Victorian Law Reform Commission, Surveillance in Public Places, Report No 18 (2010) 148 [7.122].

[26] For example, under s 148 of the *Victorian Civil and Administrative Tribunal Act 1998* (Vic), there is a right of appeal from the VCAT to the Supreme Court (or where the VCAT is constituted by a Judge, to the Court of Appeal of Victoria) within 28 days of the order of VCAT. The appeal is limited to an appeal on a question of law. Similarly, an order of the Administrative Decisions Tribunal in NSW can be appealed within 28 days after the Tribunal gives the party reasons for the appealable decision. An appeal made to the Appeal Panel is restricted to questions of law. See *Administrative Decisions Tribunal Act 1997* (NSW) ss 112, 113.

Recommendation Nine
We propose the following:
(1) After hearing the evidence and submissions that the parties to a complaint desire to adduce or make, the Tribunal may:

(a) find the complaint or any part of it proven and make one or more of the following orders:

(i) an order restraining the respondent from repeating or continuing any act or practice the subject of the complaint which the Tribunal has found proven;

(ii) an order that the respondent redress:

(A) loss or damage suffered by the complainant, including injury to the complainant's feelings; or

(B) humiliation suffered by the complainant, by reason of the interference.

(iii) an order that the complainant is entitled to a specified amount, not exceeding $100 000, by way of compensation for any loss or damage suffered by the complainant, including injury to the complainant's feelings or humiliation suffered by the complainant, by reason of the interference;
(b) find the complaint or any part of it proven but decline to take any further action; or
(c) find the complaint or any part of it is not proven and make an order that the complaint or any part of it be dismissed; or
(d) in any case, order the respondent to pay the complainant a specified amount for expenses reasonably incurred in connection with the making of the complaint and the proceedings held under this Act.

5.4 Imposing civil and criminal penalties

A civil penalty is a fine or sanction, which is founded on the notion of 'preventing or punishing public harm'.[27] Civil penalties have a lower standard of proof than their criminal counterparts, and do not involve findings of criminal responsibility.[28] Although the contravention may be similar to a criminal offence, the procedure by which the person is sanctioned is based on civil court processes.[29] Civil penalties are important to regulation, as they may be sufficiently serious to act as a punishment and as a deterrent if imposed at a high enough level.

Civil penalties are considered appropriate and effective where:

- criminal punishment is not warranted (for example, where an offence involves harm to a person or presents a serious danger to public safety, it is relatively clear that this should result in criminal punishment);
- the penalty is sufficient to justify court proceedings; or
- there is corporate wrongdoing.[30]

[27] Australian Law Reform Commission, *Federal Civil and Administrative Penalties in Australia*, Report No 95 (2003) 2.47.

[28] Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 7.

[29] Australian Law Reform Commission, *Federal Civil and Administrative Penalties in Australia*, Report No 95 (2003) 2.47.

[30] Australian Government, Attorney General's Department, *A Guide to Framing Federal Offences: Civil Penalties and Enforcement Powers* (2007) 63-4.

A criminal penalty usually serves, in a regulatory context, 'as a last-resort punishment after repeated or wilful violations'.[31] Fines and imprisonment are the main criminal penalties used in Australian legislation.[32] Current surveillance devices laws provide for criminal penalties where a person installs or uses a surveillance device, or publishes information gained by the use of a surveillance device, in prohibited ways.[33]

The following test for criminality, as developed by the Law Reform Commission of Canada, is useful in determining which prohibitions, if any, should constitute criminal conduct under the uniform provisions:

- Does the act seriously harm other people?
- Does it in some way so seriously contravene our fundamental values as to be harmful to society?
- Are we confident that the enforcement measures necessary for using criminal law against the act will not themselves seriously contravene our fundamental values?
- Given that we answer 'yes' to the above three questions, are we satisfied that criminal law can make a significant contribution to dealing with the problem?[34]

With the increased use and pervasiveness of surveillance technologies by a wider range of people, it is likely that there will be a range of breaches – some minor and others more serious or systematic. It is our view that:

- the prohibitions relating to the installation or use of surveillance devices, and the communication or publication of private records (Recommendations 3 and 6), should be subject to civil penalties; and
- the prohibitions relating to intimidation, harassment and harm (Recommendations 7 and 8) should be subject to civil and criminal penalties.

There is 'growing support for the use of civil penalties' as proportional remedies in regulatory contexts.[35] Introducing civil penalties under the uniform provisions would:

- likely reduce the cost and complexity of the regulatory process;
- invite the Privacy Commissioner to act on less serious matters; and
- provide greater flexibility to best address the circumstances of each case.

With respect to the criminal penalty provisions, if the Privacy Commissioner forms the opinion, during an investigation, that a criminal offence has been committed, they should cease the investigation and refer the matter to the relevant police force. It is not the purpose of this proposal to determine the maximum criminal penalty that should apply under the uniform provisions. We leave that task entirely to those elected to make such decisions: legislators.

---

31 Australian Law Reform Commission, *Federal Civil and Administrative Penalties in Australia*, Report No 95 (2003) 2.41.

32 Australian Law Reform Commission, *Federal Civil and Administrative Penalties in Australia*, Report No 95 (2003) 2.40.

33 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 121 [6.82].

34 Law Reform Commission of Canada, *Our Criminal Law*, 4 (1976), Information Canada, Ottawa, 33.

35 See Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) 121-2. [6.82]-[6.93].

6 APPENDIX: existing regulation of unmanned systems in Australia

The use of unmanned systems in Australia is currently subject to two separate categories of regulation – civil aviation safety laws, and privacy and surveillance laws.

6.1 Civil aviation safety regulations

Part 101 of the *Civil Aviation Safety Regulations 1998* (Cth) ("**Regulations**"), promulgated in 2002 and supplemented by Advisory Circulars 101-1(0), 101-2(0) and 103-3(0), was the first operational regulation for unmanned aircraft in the world. The Regulations regulate where and how unmanned aircraft, including unmanned aerial vehicles ("**UAVs**") (defined as "unmanned aircraft other than a balloon or a kite": reg 101.240) may be used.

The Regulations are focused primarily, if not exclusively, on ensuring safety. The main object of the *Civil Aviation Act 1988* (Cth) under which the Regulations are made "is to establish a regulatory framework for maintaining, enhancing and promoting the safety of civil aviation, with particular emphasis on preventing aviation accidents and incidents."[36]

CASA, whose function is to conduct "the safety regulation" of civil air operations,[37] must, in performing that function and exercising its powers, "regard the safety of air navigation as the most important consideration".[38]

As John McCormick, then Director of CASA, said in a speech to the Association for Unmanned Vehicle Systems Australia on 25 February 2013: "CASA is Australia's civil aviation safety regulator. We have no authority to allow economic or commercial considerations to influence safety-related decisions we are obliged to make … The right to privacy is another controversial topic one hears when discussing [remotely piloted aircraft]. Dealing with matters related to privacy is not part of CASA's role; it is a matter for the Australian Privacy Commissioner."

[36] *Civil Aviation Act 1988* (Cth) s 3A.

[37] *Civil Aviation Act 1988* (Cth) s 9(1).

[38] *Civil Aviation Act 1988* (Cth) s 9A(1).

6.2 Privacy legislation

The *Privacy Act 1988* (Cth) ("Privacy Act") and equivalent state and territory Acts

The Privacy Act regulates the way personal information is collected and handled by Federal/ACT agencies, Federal government contracted service providers, and private sector organisations (excluding most small business operators with an annual turnover of less than $3m). The Australian Capital Territory, Northern Territory, NSW, Queensland, Tasmania and Victoria have enacted similar legislation in relation to their own agencies: see *Information Privacy Act 2014* (ACT); *Information Act 2002* (NT); *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Personal Information and Protection Act 2004* (Tas); and *Privacy and Data Protection Act 2014* (Vic). In Western Australia, the Information Privacy Bill 2007 (WA) received its second reading in the Legislative Council on 4 December 2007 but is yet to be enacted. In South Australia, there is a Cabinet Administrative Instruction (1/89, as amended on 18 May 2009) which includes a set of information privacy principles applicable to public sector agencies.

As Australian Privacy Commissioner Timothy Pilgrim pointed out in an open letter to the Attorney-General dated September 2012 calling for a review of the current regulatory framework in response to drone technology:

> Where an agency or private sector organization covered by the Privacy Act intends to use drone technology, it must do so in accordance with the Privacy Act. This would include giving notice to affected individuals about the collection of their personal information, only using and disclosing the personal information as permitted by the Privacy Act, and keeping it secure. The Privacy Act does not however cover the actions of individuals in their private capacity, including any use of drones by individuals.

Nor does the Privacy Act cover the actions of most private sector organisations with an annual turnover of less than $3m.

A further limitation of Federal, state and territory privacy legislation is that it only regulates the collection of "personal information". At the Federal level, this is defined to mean information or an opinion about an identified individual, or an individual who is reasonably

identifiable (whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not). The term "individual" is defined to mean a "natural person". Many questionable uses of unmanned systems are unlikely to result in the collection of personal information so defined.

Surveillance legislation

The installation, use and maintenance of surveillance devices is regulated by legislation in the Federal and most States and Territories: see, eg, *Surveillance Devices Act 2004* (Cth); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 2007* (NSW); *Workplace Surveillance Act 2005* (NSW); *Listening Devices Act 1992* (ACT); *Workplace Privacy Act 2011* (ACT); *Surveillance Devices Act 1998* (WA); *Surveillance Devices Act 2007* (NT); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Police Powers (Surveillance Powers) Act 2006* (Tas); *Invasion of Privacy Act 1971* (Qld); *Crime and Misconduct Act 2001* (Qld); *Police Powers and Responsibilities Act 2000* (Qld) ch 13.

However, as the Australian Privacy Commissioner pointed out in the letter referred to above, "individuals who may be subject to surveillance via drone technology may not currently be able to seek appropriate or consistent redress across the Commonwealth."

The existing surveillance regimes across Australia each have a different scope, and regulate the use of unmanned systems to varying degrees. Six jurisdictions (the Federal, Victoria, New South Wales, South Australia, Western Australia and the Northern Territory) have enacted legislation that regulates optical surveillance devices, which are likely to be attached to unmanned systems:

(a) Federal surveillance legislation is limited exclusively to surveillance undertaken by law enforcement agencies. Note that a federal law enforcement officer acting in the course of his or her duties may, without warrant, use an optical surveillance device for any purpose that is within the functions of the AFP if the use of that device does not involve entry onto premises without permission or interference without permission with any vehicle or thing (*Surveillance Devices Act 2004* (Cth) s 37).

(b) In Victoria, section 7(1) of the *Surveillance Devices Act 1999* (Vic) provides that, subject to specified exceptions, "a person must not knowingly install, use or maintain an optical surveillance device to record visually or observe a private activity to which the person is not a party, without the express or implied consent of each party to the activity." However, the term "private activity" is defined to mean "an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include (a) an activity carried on outside a building" (section 3). There is therefore no prohibition under the Act against using an unmanned system to visually record a private activity that occurs outdoors. Note, however, that the offence of knowingly installing, using or maintaining a listening device to overhear, record, monitor or listen to a private conversation to which a person is not a party without the express or implied consent of each party to the conversation (section 6(1)) is not similarly limited – that is, it applies both indoors and outdoors.

(c) By contrast with section 7(1) of the *Surveillance Devices Act 1999* (Vic), section 8 of the *Surveillance Devices Act 2007* (NSW) prohibits the knowing installation, use, or maintenance of an optical surveillance device "on or within premises or a vehicle or on any other object ... if the installation, use or maintenance of the device involves: (a) entry onto or into the premises or vehicle without the express or implied consent of the owner or occupier of the premises or vehicle; or (b) interference with the vehicle or other object without the express or implied consent of the person having lawful possession or lawful control of the vehicle or object." This prohibition is broader than the Victorian prohibition in that it covers the recording of all activities (not just private activities), but the requirement for entry onto premises or a vehicle without consent makes it narrower: it does not, for example, prohibit the use of an unmanned system to observe private activities taking place on a neighbour's property if the unmanned system remains on its owner's possession.

(d) Section 6 of the *Surveillance Devices Act 1998* (WA) provides that, subject to specified exceptions, "a person shall not install, use, or maintain, or cause to be installed, used, or maintained, an optical surveillance device to record visually or observe a private activity to which that person is not a party, or to record visually a private activity to which that person is a party." A "privacy activity" means "any activity carried on in circumstances that may reasonably be taken to indicate that any of the parties to the activity desires it to be observed only by

themselves, but does not include an activity carried on in any circumstances in which the parties to the activity ought reasonably to expect that the activity may be observed" (section 3). Unlike the Victorian legislation, this Act would likely prohibit using an unmanned system to visually record a private activity that occurs outdoors. One of the specified exceptions is that the unintentional recording or observation of a private activity will not result in a penalty, but highly mobile unmanned systems may regularly capture private activities unintentionally. However, publishing a recording of a private activity taken by an optical surveillance device is prohibited (section 9).

(e) Section 3 of the *Listening and Surveillance Devices Act 1972* (SA) defines a "surveillance device" as a visual surveillance device or a tracking device. However, while the Act prohibits the intentional use of a listening device to record private conversations (section 4), the Act only regulates surveillance devices that are to be used subject to a warrant. The Surveillance Devices Bill 2012 (SA), which would impose greater limits on the use of optical surveillance devices, has not yet passed. The Bill is currently being considered by a Legislative Council committee.

(f) The definition of "surveillance device" in section 4 of the *Surveillance Devices Act 2007* (NT) means "a data surveillance device, listening device, optical surveillance device or tracking device", or a combination of two or more of these devices. An "optical surveillance device" is "a device capable of being used to monitor, record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome the impairment and permit the person to see only sights ordinarily visible to the human eye." A person commits an offence if, subject to specific exceptions, they install, use or maintain "an optical surveillance device to monitor, record visually or observe a private activity to which the person is not a party; and knows the device is installed, used or maintained without the express or implied consent of each party to the activity" (section 12). "Private activity" means "an activity carried on in circumstances that may reasonably be taken to indicate the parties to the activity desire it to be observed only by themselves, but does not include an activity carried on in circumstances in which the parties to the activity ought reasonably to expect the activity may be observed by someone else" (section 3). Unlike the Victorian legislation, this Act would likely prohibit using an unmanned system to visually record a private activity that occurs outdoors.

Optical surveillance devices are not regulated in three jurisdictions (Queensland, Tasmania and the ACT). Each has legislation that may relate to some uses of unmanned system:

(a) The *Invasion of Privacy Act 1971* (Qld) only prohibits the use of listening devices to record private conversations (section 43). The use of optical surveillance devices is not regulated at present.

(b) The *Listening Devices Act 1991* (Tas) only prohibits the use of listening devices to record private conversations (section 5). The Act does not regulate the use of optical surveillance devices. The use of optical surveillance devices is not regulated at present.

(c) The *Listening Devices Act 1992* (ACT) only prohibits the use of listening devices to record private conversations (section 4). The Act does not regulate the use of optical surveillance devices. Employers that use optical surveillance devices to monitor workers must comply with the *Workplace Privacy Act 2011* (Tas).

6.3 Tort law

A person whose rights are impeded by another person's use of an unmanned system may take action under the law of tort. However, there is presently no action available to prevent a person from using an unmanned system to cause nuisance or invade another person's privacy.

(a) *Trespass to property*: A person causing a projectile to pass through airspace at such a height as would interfere with the occupier's ordinary use and enjoyment of land is a trespass, although transient passage above that height may not be trespass.[39] In some jurisdictions, legislation excludes liability in trespass for the overflight of aircraft at a reasonable height.[40] For example, *Wrongs Act 1958* (Vic) s 30: "No action shall lie in respect of trespass or nuisance by reason only of the flight of an aircraft over any property at a height above the ground which having regard to the wind the weather and all the circumstances is reasonable, or the ordinary incidents of such

[39] *Davies v Bennison* (1927) 22 Tas LR 52; *Clifton v Viscount Bury* (1887) 4 TLR 8.

[40] *Civil Liability Act 2002* (NSW) s 72(1); *Civil Liability Act 1936* (SA) s 62; *Damage by Aircraft Act 1963* (Tas) s 3; *Damage by Aircraft Act 1964* (WA) s 4.

flight, so long as the provisions of the Air Navigation Regulations are duly complied with."

(b) *Negligence*: A person may be negligent when, for example, their operation of an unmanned system results in damage to property or person.

(c) *Nuisance*: The common law of nuisance does not prevent a person overlooking another's land, home or activities[41] or taking photographs.[42] Other legal protection is required to prevent a person from being observed by another person who uses an unmanned system in this way.

6.4 Criminal law

A person may commit a crime based on how they use an unmanned system. These existing offences establish some limits for the acceptable use of unmanned aircraft under current law.

(a) *Criminal negligence*: A person who operates an unmanned system and causes damage to property or other people may be criminally negligent, if they fail to exercise the standard of care expected of a reasonable person.[43] For example, in Victoria a person who negligently causes serious injury commits an offence under *Crimes Act 1958* (Vic) section 24. In jurisdictions with a Criminal Code, a person has an express duty to use reasonable care and take reasonable precautions to avoid causing danger to the safety of other people.[44]

(b) *Observation of private acts or private regions*: Under section 41B of the *Summary Offences Act 1966* (Vic), it is an offence, punishable by up to 2 years' imprisonment, for a person to intentionally visually capture another person's genital or anal region in circumstances in which it would be reasonable for that other person to expect that his or her genital or anal region could not be visually captured. There is a similar prohibition on a person engaging in "indecent filming" in section 23AA of the *Summary Offences Act 1953* (SA). "Indecent filming" means filming another person in a state of undress, engaged in a private sexual act, using the toilet, or filming their genital or anal region, in circumstances in which a reasonable person would expect to be afforded privacy. Under section 227A of the *Criminal Code 1899* (Qld), a person commits a misdemeanour if they visually record another person in a private place or engaging in a private act, or visually record their genital or anal region, in circumstances where a reasonable adult would expect to be afforded privacy. A "private act" means showering or bathing, using a toilet, another activity when the person is in a state of undress, or intimate sexual activity that is not ordinarily done in public (section 207A).

(c) *Stalking*: It is an offence, punishable by up to 10 years' imprisonment, to stalk another person: *Crimes Act 1958* (Vic) section 21A(1). Section 21A(2)(f) of the Act provides that "a person (the offender) stalks another person (the victim) if the offender engages in a course of conduct which includes any of the following: ... (k) keeping the victim or any other person under surveillance". Other jurisdictions also define stalking to include keeping another person under surveillance[45] or "watching" them.[46]

(d) *Assault* (for example, where an unmanned system itself is used to interfere with a person): Under section 31 of the *Crimes Act 1958* (Vic), assault means "the direct or indirect application of force by a person to the body of, or to the clothing or equipment worn by, another person ..." and application of force includes "application of matter in solid ... form." Other jurisdictions recognise that a person may commit the offence of assault by applying force using an object such as an unmanned system.[47]

6.5 Human rights legislation

The two jurisdictions that have passed human rights legislation, Victoria and the ACT, both establish a right to privacy that applies to the use of unmanned systems by public authorities.

In Victoria and the ACT, a person has a right not to have their privacy, family, home or correspondence

---

41 *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 495, 496 (Latham CJ), 507-8 (Dixon J), 517 (Evatt J).

42 *Bathurst City Council v Saban* (1985) 2 NSWLR 704.

43 *R v Bateman* [1925] All ER Rep 45; *Callaghan v R* (1952) 87 CLR 115. Negligence causing injury is a crime under *Crimes Act 1958* (Vic) s 24.

44 *Criminal Code 1899* (Qld) s 289; *Criminal Code 1924* (Tas) s 150; Criminal *Code 1913* (WA) s 266; *Criminal Code 1983* (NT) s 151.

45 *Criminal Law Consolidation Act 1935* (SA) s 19AA; *Criminal Code 1924* (Tas) s 192; *Criminal Code Act 1983* (NT) s 189; *Crimes Act 1900* (ACT) s 35.

46 *Crimes (Domestic and Personal Violence) Act 2007* (NSW) ss 8, 13; *Criminal Code 1899* (Qld) ss 359B, 359E; *Criminal Code 1913* (WA) ss 338D (definition of "pursue"), 338E.

47 *Criminal Code 1899* (Qld) s 245; *Criminal Code 1913* (WA) s 222; *Criminal Code 1924* (Tas) s 182; *Criminal Law Consolidation Act 1935* (SA) s 20; *Criminal Code 1983* (NT) s 187.

unlawfully or arbitrarily interfered with.[48] It is unlawful for a "public authority" to act in a way that is incompatible with a human right or, in making a decision, to fail to give proper consideration to a relevant human right.[49] These provisions provide protection against the use of unmanned systems by government, but a person cannot enforce the right to privacy against individuals or companies.

This protection against public authorities' unlawful interference with a right to privacy reflects the wording of Article 17 of the *International Covenant on Civil and Political Rights* to which Australia is a party. Similar protections exist in the United States (under the Fourth Amendment to the Constitution), the European Union (under Article 8 of the *European Convention on Human Rights*) and the United Kingdom (under section 8 of the *Human Rights Act 1998*). However, the use of unmanned systems may present new issues that arise outside the scope of these existing protections.[50]

---

48 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13(a); *Human Rights Act 2004* (ACT) s 12(a).

49 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 38(1); *Human Rights Act 2004* (ACT) s 40B(1).

50 See, for example, American Civil Liberties Union, *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft* (2011) <http://www.aclu.org/technology-and-liberty/report-protecting-privacy-aerial-surveillance-recommendations-government-use>.