DRONES AND INVASIONS OF PRIVACY: AN INTERNATIONAL COMPARISON OF LEGAL RESPONSES

DES BUTLER*†

Privacy has been recognised nationally and internationally as a major challenge posed by the growing proliferation of drones, otherwise known as 'remotely piloted aircraft', 'small unmanned aircraft' or 'unmanned aircraft systems', with surveillance capability. Currently in Australia an uneven landscape of common law causes of action, surveillance statutes and data protection laws provide fragmented protection of privacy. This article compares that legal response with those of the United Kingdom and the United States. It identifies commonalities and differences between those approaches that may be instructive as Australia determines the appropriate response to the potential of invasion of privacy posed by this form of transformative technology.

I INTRODUCTION

One evening in April 2017, a 27-year-old woman in Darwin returned home from the gym, took off her clothes and went skinny-dipping in what she thought to be the seclusion of her backyard pool. However, she soon became aware that she was not alone and was shocked to see a small drone hovering 10–15 metres above her head.[1] One month later, a similar surprise awaited a Sydney woman who stepped out of the shower of her fifth floor apartment and saw a drone looking back at her through a window.[2] Drones are now also being employed to spy on prominent individuals for commercial purposes. For example, there have also been

* Professor of Law, Faculty of Law, Queensland University of Technology. I am indebted to my QUT colleague Professor Belinda Bennett for her insight, comments and suggestions on an earlier draft. I am also grateful for the research assistance of Elizabeth Dallaston and Clinton Wang.

† This article is published in respectful memory of Professor Des Butler. The *Journal* thanks Professor Butler's father, Allan Butler, with whose help and encouragement the article was prepared for publication.

1 Alana Mitchelson, '"Peeping Tom Drones" Prompt Calls for a Close Look at Privacy Law', *The New Daily* (online, 27 April 2017) <https://thenewdaily.com.au/life/tech/2017/04/27/drones-privacy-law/>.

2 Robbie Patterson, 'Sydney Couple Catch Drone Spying on Them from Fifth Floor Balcony', *Daily Telegraph* (online, 31 May 2017) <http://www.dailytelegraph.com.au/newslocal/manly-daily/sydney-couple-catch-drone-spying-on-them-from-fifth-floor-balcony/news-story/5f67377e6bb14f0d4e566340ae462ba7>.

reports of drones being operated by paparazzi to spy on public figures.[3] These reports highlight the potential for drones to be used in ways that may infringe on the privacy rights of others.

In addition, drones are increasingly being employed for other diverse purposes, such as surveying, inspection of pipelines and other infrastructure, filmmaking, monitoring of crops and vegetation, real estate listings, emergency services and surf rescue.[4] Drones may play an increasingly important role in journalism, since they offer a more cost effective alternative to helicopters and may be valuable tools for newsgathering in the public interest in circumstances where other means are not available.[5] However even such activities may inadvertently impinge upon an individual's privacy, as occurred when a Victorian woman who was sunbathing topless in her backyard was accidentally photographed by a drone that had been commissioned by a real estate firm to advertise a neighbour's property.[6] In addition to high definition cameras, drones may now be equipped with a variety of technology including facial recognition software,[7] thermal scanners and licence plate readers.[8]

The recreational use of drones has grown exponentially, promoted through their sale in electrical goods shops and department stores, where a remotely piloted aerial vehicle with a high-quality video camera with streaming capability may be purchased for as little as $100. With such technology capable of being used 'out of the box' without specialist knowledge or training, there is an evident risk to not

3 'Armytage Slams Kyle and Jackie O over "Highly Illegal" Drone Pest', *news.com.au* (online, 13 February 2017) <http://www.news.com.au/entertainment/tv/morning-shows/sam-armytage-calls-police-after-spotting-drone-hovering-above-her-sydney-home/news-story/34e69d93dc7154a2900dc4275f31973c> (television personality Samantha Armytage); Louise Yaxley, 'Barnaby Joyce Says Partner Vikki Campion Sold Their Interview after Privacy Invasions', *ABC News* (online, 30 May 2018) <http://www.abc.net.au/news/2018-05-29/australians-disgusted-barnaby-joyce-sold-his-story/9810418> (politician Barnaby Joyce).

4 Des Butler, 'The Dawn of the Age of the Drones: An Australian Privacy Law Perspective' (2014) 37(2) *University of New South Wales Law Journal* 434, 436–7 ('The Dawn of the Age of the Drones'); John Villasenor, 'Observations from Above: Unmanned Aircraft Systems and Privacy' (2013) 36(2) *Harvard Journal of Law and Public Policy* 457, 459. Drones may also be used to deliver, for example, defibrillators in a medical emergency: Andreas Claesson et al, 'Time to Delivery of an Automated External Defibrillator Using a Drone for Simulated Out-of-Hospital Cardiac Arrests vs Emergency Medical Services' (2017) 317(22) *JAMA: Journal of the American Medical Association* 2332.

5 Jason Koebler, 'The Government Is Using a No Fly Zone to Suppress Journalism at Standing Rock', *Vice* (online, 1 December 2016) <https://motherboard.vice.com/en_us/article/yp3kak/the-government-is-using-a-no-fly-zone-to-suppress-journalism-at-standing-rock> (drones being used by journalists to document alleged human rights abuses during protests against the building of an oil pipeline in North Dakota).

6 Rita Panahi, 'Mt Martha Woman Snapped Sunbaking in G-String by Real Estate Drone', *Herald Sun* (online, 17 November 2014) <http://www.heraldsun.com.au/news/victoria/mt-martha-woman-snapped-sunbaking-in-gstring-by-real-estate-drone/news-story/c3eaaeb6318d7f01dcb4394da968340a>.

7 Andrew Conte, 'Drones with Facial Recognition Technology Will End Anonymity, Everywhere', *Business Insider* (online, 27 May 2013) <http://www.businessinsider.com/facial-recognition-technology-and-drones-2013-5>.

8 Taly Matiteyahu, 'Drone Regulations and Fourth Amendment Rights: The Interaction of State Drone Statutes and the Reasonable Expectation of Privacy' (2015) 48(2) *Columbia Journal of Law and Social Problems* 265, 266–7.

only the safety of the person and/or property but also the privacy of other individuals.[9]

The Australian experience of invasions of privacy by drones is not unique – it is a growing phenomenon around the world.[10] Indeed, when addressing the inaugural World of Drones Congress in Brisbane in 2017, American futurist Thomas Frey predicted that by 2030 there could be as many as 1 billion drones in the world,[11] each with the capacity of intentionally or unintentionally capturing images of individuals. The legal responses to potential invasions of privacy associated with the use of drones may include dedicated common law causes of action for invasion of privacy, more general common law causes of action that may extend to protect privacy, dedicated statutory causes of action for breach of privacy, privacy legislation that may extend to drones and legislation that specifically applies to invasions of privacy by drones. Such responses of other countries may therefore be instructive when considering the current and possible future responses of the law to this form of invasion of privacy in this country.

Following this introduction, this article examines the regulatory and privacy laws that are relevant to invasions of privacy by drones in each of Australia, the United Kingdom and the United States. While regulation and privacy protection may be thought of as distinct issues, they are nonetheless intertwined: for example, limitations placed on where and how drones may be used may affect the opportunities to use a drone to invade another's privacy. The article then identifies commonalities and differences that may be instructive as Australia determines the appropriate response to the potential of invasion of privacy posed by this new form of technology.[12]

---

9 Rebecca Johnston, 'Got a Drone for Christmas? Know the Rules before Taking to the Skies', *The Conversation* (online, 26 December 2016) <https://theconversation.com/got-a-drone-for-christmas-know-the-rules-before-taking-to-the-skies-70341>.

10 In the United Kingdom, see, eg, Richard Madeley, 'Richard Madeley: "The Day I Took on the Drone Invading My Personal Space"', *The Telegraph* (online, 13 April 2016) <https://www.telegraph.co.uk/men/thinking-man/richard-madeley-the-day-i-took-on-the-drone-invading-my-personal/>. In the United States, see, eg, Douglas Ernst, 'Ky Man Arrested after Shooting Down $1,800 Drone Hovering over Sunbathing Daughter', *The Washington Times* (online, 30 July 2015) <https://www.washingtontimes.com/news/2015/jul/30/william-merideth-arrested-after-shooting-down-1800/>; James Queally, 'Seattle Woman Says Drone Seemed to Be Spying on Her', *Los Angeles Times* (online, 24 June 2014) <http://www.latimes.com/nation/nationnow/la-na-nn-seattle-peeping-tom-20140624-story.html>.

11 Meghna Bali, '1 Billion Drones in the World by 2030, US Futurist Thomas Frey Says', *ABC News* (online, 31 August 2017) <http://www.abc.net.au/news/2017-08-31/world-of-drones-congress-brisbane-futurist-thomas-frey/8859008>.

12 These devices are variously described in legislation as, for example, remotely piloted aircraft, unmanned aircraft and unmanned aerial systems. However, apart from when discussing provisions in specific statutes, the colloquial description 'drone' is used in this article.

II AUSTRALIA

The regulation and privacy implications of the operation of drones in Australia were the subject of analysis five years ago.[13] It is timely to revisit that analysis and examine developments since that time.

A Regulation of Drones

Australia was the first country to enact regulations governing the use of drones. In 2002 the *Civil Aviation Safety Regulations 1998* (Cth) ('*CASR*') were amended by the insertion of a new part 101 that contained regulations that were primarily concerned with the safe operation of drones, which are described as Remotely Piloted Aircraft ('RPA'). These contained a general prohibition against operation of an RPA in a way that created a hazard to another aircraft or personal property, which was supported by more specific provisions concerning the operation of RPAs.[14] These regulations were subsequently amended in 2016 to clarify requirements and limitations governing safe operation of RPAs. This new scheme categorises RPA by size and weight:

- Micro RPA – gross weight of 100 g or less
- Very small RPA – gross weight of more than 100 g but less than 2 kg
- Small RPA – gross weight of at least 2 kg but less than 25 kg
- Medium RPA – gross weight of at least 25 kg but not more than 150 kg
- Large RPA – gross weight of more than 150 kg.[15]

As a guide, some toy drones would qualify as 'micro RPAs' while 'large RPAs' include drones similar in size to the Predator drones operated by the United States military. By contrast, the DJI Phantom 4 drone, a top selling camera-mounted RPA popular among recreational users, weighs about 1.4 kg and therefore qualifies as a 'very small RPA'.

At the time of writing, the regulations provide for an 'excluded RPA category', which are judged to 'pose lower risk, having regard to their size and weight, the kind of operations in which they are engaged and the location of those operations'.[16] Pursuant to regulation 101.237, an excluded RPA can operate without certain licences and permissions, such as the requirement to have a remote pilot licence to operate an RPA.[17] The following are deemed excluded RPA by regulation 101.237:

- A micro RPA;[18]

13 See Butler, 'The Dawn of the Age of the Drones' (n 4).
14 Ibid 437–9.
15 *Civil Aviation Safety Regulations 1998* (Cth) reg 1.004 Dictionary (definitions of 'micro RPA', 'very small RPA', 'small RPA', 'medium RPA', 'large RPA').
16 Civil Aviation Safety Authority, 'Review of RPAS Operations' (Discussion Paper No DP 1708OS, August 2017) 8.
17 *Civil Aviation Safety Regulations 1998* (Cth) reg 101.252.
18 Ibid sub-reg (2).

- A very small RPA 'if it is being operated (a) for the purpose of sport or recreation, or (b) in standard RPA operating conditions';[19]
- A small RPA

  if it is being operated:

  (a) by or on behalf of the owner of the RPA; and
  (b) over land owned or occupied by the owner of the RPA; and
  (c) in standard RPA operating conditions; and
  (d) for the purposes of one or more of the following:
    (i) Aerial spotting;
    (ii) Aerial photography;
    (iii) Agricultural operations;
    (iv) Aerial communications retransmission;
    (v) The carriage of cargo;
    (vi) Any other activity that is similar to [such activities]; and

  for which no remuneration is received by the operator or the owner of the RPA, the owner or occupier of the land or any person on whose behalf the activity is being conducted;[20]
- A medium RPA in similar circumstances as a small RPA, with the additional requirement that it be operated 'by a person who holds a remote pilot licence';[21]
- A small or medium RPA 'if it is being operated for the purpose of sport or recreation', or 'if it is being operated in standard RPA operating conditions by (a) a person for the sole purpose of meeting the experience requirement … for a grant of a remote pilot licence or (b) the holder of a remote pilot licence for the sole purpose of getting practical experience and gaining competency in the operation of an RPA'.[22]

The concept of 'standard RPA operating conditions' which is common to most of these definitions is itself defined in regulation 101.238 in the following terms:

(a) The RPA is operated within the visual line of sight of the person operating [it]; and
(b) The RPA is operated at or below 400 ft [above ground level] by day; and
(c) The RPA is not operated within 30 m of a person who is not directly associated with the operation of the RPA; and
(d) The RPA is not operated:
  (i) in a prohibited area; or
  (ii) in a restricted area that is classified as RA3; or
  (iii) in a restricted area that is classified as RA2 or RA1 otherwise than in accordance with regulation 101.065 [which provides for permission from, and conditions imposed by, the authority controlling the area]; or
  (iv) over a populous area; or

19 Ibid sub-reg (3). 'Standard RPA operating conditions' are considered below.
20 Ibid sub-reg (4).
21 Ibid sub-reg (7).
22 Ibid sub-regs (5)–(6).

(v) within 3 nautical miles of the movement area of a controlled aerodrome; and

(e) the RPA is not over an area where a fire, police or other public safety or emergency operation is being conducted without the approval of the person in charge of the operation; and

(f) the person operating the RPA operates only *that* RPA.[23]

These standard RPA operating conditions reflect most of the requirements of RPA operation under the previous regime, with the addition of the reference to emergency operations.[24] Perhaps the most contentious aspect of the amended regulations, however, was the list of RPAs excluded from the licensing and permissions requirements.

At the time of writing, under Australian law neither RPAs nor RPA owners or operators were required to be registered. However, a report by the Senate Rural and Regional Affairs and Transport References Committee recommended, inter alia, the introduction of a registration requirement and a basic competence test for operators of RPAs weighing more than 250 g.[25] The Committee also recommended the development of a tiered education program concerning aviation safety rules depending on whether the drone is to be used for recreation or commercial purposes.[26] The government in response agreed with the recommendation concerning registration and competency, but only noted the recommendation concerning an education program, on the ground that the Civil Aviation Safety Authority ('CASA') was already developing an education package for not only safe use but also threats to national security.[27]

---

23 Ibid reg 101.238 (emphasis added). Certain areas of airspace may be designated as restricted, for example, because they are a police exclusion zone or are being used by the military using live weapons. There are three possible classifications: 'RA1' refers to a restricted area that may be flown through with clearance from air traffic control; 'RA2' refers to an area where clearance should not be expected, but which nonetheless may be offered to a pilot by air traffic control on a tactical basis due to exigent circumstances; and 'RA3' denotes a restricted area which may not be entered and for which clearances will not be given by air traffic control. Restricted areas may be permanent or temporary and are notified by Air Services Australia, the government organisation that manages Australia's airspace. See, eg, Air Services Australia, *Safety Net: Safe Operations Around Controlled and Restricted Airspace* (Corporate Communication No 15-094MAY) <http://www.airservicesaustralia.com/wp-content/uploads/safe_operations_fact_sheet.pdf>.

24 Cf Butler, 'The Dawn of the Age of the Drones' (n 4) 437–9.

25 Senate Rural and Regional Affairs and Transport References Committee, Parliament of Australia, *Current and Future Regulatory Requirements That Impact on the Safe Commercial and Recreational Use of Remotely Piloted Aircraft Systems (RPAS), Unmanned Aerial Systems (UAs) and Associated Systems* (Report, July 2018) 105 [8.20] ('*Safe Commercial and Recreational Use Report*'). The Civil Aviation Safety Authority ('CASA') proposes to introduce a system of registration of RPAs and RPA operator accreditation requirements from 1 July 2019: CASA, *Proposed New Remotely Piloted Aircraft (RPA) Registration and RPA Operator Accreditation Scheme* (Policy Proposal No PP 1816US, January 2019) <https://consultation.casa.gov.au/regulatory-program/pp1816us/supporting_documents/Policy%20Proposal%20%20PP%201816US.PDF>.

26 *Safe Commercial and Recreational Use Report* (n 25) 106 [8.26].

27 Australian Government, *Australian Government Response to the Senate Standing Committee on Rural and Regional Affairs and Transport Report: Regulatory Requirements That Impact on the Safe Use of Remotely Piloted Aircraft Systems, Unmanned Aerial Systems and Associated Systems* (November 2018) 4–5 ('*Response to Safe Commercial and Recreational Use Report*').

These recommendations and responses aside, the regulations in force at the time of writing do not specifically address concerns in relation to the potential for drone-mounted cameras to be used to invade another person's privacy.[28] But they may nonetheless have relevance to that question.

B Protection of Privacy

Privacy in Australia is protected by an uneven landscape of common law and legislation at both Commonwealth and State/Territory levels.[29] Protection of privacy may be provided by a combination of common law causes of action, surveillance statutes and data protection statutes.

1 Common Law

Invasion of privacy in the form of an intrusion on an individual's seclusion may base a claim for trespass to land or private nuisance.[30] However, both causes of action have limitations which make them an imperfect response to such an intrusion. Thus, for example, a trespass is not committed if the drone is flown above the operator's own land or above public land and is used to observe an individual and their activities on adjacent land.[31] Indeed, both causes of action are limited to the height of an 'ordinary user'.[32] This is a concept that has received limited judicial consideration and may be incapable of precise definition. It has been held in an English case that a trespass was committed where an untethered crane jib oversailed the plaintiff's property at a height 50 feet above the ground,[33] which was followed in a Queensland case with similar facts in which the jib was 62 feet above the ground.[34] The question is not whether the intrusion interferes with the plaintiff's actual use of the land at the time but rather whether it is of a nature and at a height that could interfere with any ordinary uses the plaintiff may wish to undertake.[35]

Naturally each case depends upon its circumstances rather than arbitrary heights above ground level. But drones may have operating heights well above 64 feet, as recognised by the 'standard RPA operating conditions' enacted by the *CASR* which contemplate drones being operated at a height of up to 400 feet above ground level. It is conceivable, therefore, for a drone to be flown over a neighbour's property at a height above that considered to be the height of an

28 In its information on 'Flying Drones or Model Aircraft Recreationally' the CASA website simply states: 'Please respect personal privacy. Don't record or photograph people without their consent – this may breach state laws': 'Flying Drones or Model Aircraft Recreationally', *Civil Aviation Safety Authority* (Web Page, 25 June 2019) <https://www.casa.gov.au/modelaircraft>.

29 See generally Butler, 'The Dawn of the Age of the Drones' (n 4).

30 See *Bernstein of Leigh (Baron) v Skyviews & General Ltd* [1978] QB 479. A new tort providing protection against unreasonable intrusion on seclusion was recognised by a Queensland District Court judge in *Grosse v Purvis* [2003] Aust Torts Reports ¶81-706 but has yet to be approved by an appellate court.

31 *Bernstein of Leigh (Baron) v Skyviews & General Ltd* [1978] QB 479, 488 (Griffiths J).

32 Ibid 486.

33 See *Woollerton & Wilson Ltd v Richard Costain Ltd* [1970] 1 All ER 483.

34 *Graham v KD Morris & Sons Pty Ltd* [1974] Qd R 1.

35 *LJP Investments Pty Ltd v Howard Chia Investments Pty Ltd* (1989) 24 NSWLR 490, 495 (Hodgson J).

ordinary user and therefore not commit either a trespass or private nuisance. Further, both causes of action are restricted with regard to those who have the necessary title to sue: only those with a right to possession may sue for trespass[36] while only those with possession or an immediate right to possession may sue for private nuisance.[37] Neither would be available to a person without a possessory interest in the property, such as a visitor. And neither would be available to invasions upon the seclusion of persons who were on public property, such as a secluded beach or bushland.

The common law concerning trespass to land and private nuisance is supplemented by legislation in a number of states which specifically provides that no action lies for trespass or nuisance with respect to an aircraft flying over a property at a reasonable height and in compliance with air navigation regulations.[38] No definition of 'aircraft' is included in most of this legislation,[39] but the Macquarie Dictionary definition of 'any machine supported for flight in the air … by dynamic action of air on its surfaces (such as aeroplanes, helicopters, gliders[)]' may include drones.[40] However, where an aircraft is operated at an unreasonable height, or not in accordance with air navigation rules, or where the intrusion is not related simply to the flyover, such as a claim related to noise, the statutory immunity may not apply.[41]

Invasions in the form of a disclosure of private information may be a consequence of an intrusion upon seclusion, for example where images of an individual captured by a drone are disseminated on the internet. In Australia the only cause of action that would be available in such a case is the action for breach of confidence,[42] which requires three elements, as explained by Megarry J in *Coco v AN Clark (Engineers) Ltd*:

> First, the information … must 'have the necessary quality of confidence about it'. Secondly, that information must have been imparted in circumstances importing an

36 See *Newington v Windeyer* (1985) 3 NSWLR 555.

37 See *Malone v Laskey* [1907] 2 KB 141.

38 See *Civil Liability Act 2002* (NSW) s 72; *Civil Liability Act 1936* (SA) s 62; *Damage by Aircraft Act 1963* (Tas) s 3; *Wrongs Act 1958* (Vic) s 30; *Damage by Aircraft Act 1964* (WA) s 4. See Pam Stewart, 'Drone Danger: Remedies for Damage by Civilian Remotely Piloted Aircraft to Persons or Property on the Ground in Australia' (2016) 23(3) *Torts Law Journal* 290, 314.

39 However, in South Australia the *Civil Liability Act 1936* (SA) s 61(2) adopts the definition in the *Damage by Aircraft Act 1999* (Cth) s 4, which in turn adopts the definition of 'aircraft' in the *Civil Aviation Act 1988* (Cth) s 3 ('any machine or craft that can derive support in the atmosphere from the reactions of the air, other than the reactions of the air against the earth's surface') but excludes model aircraft.

40 *Macquarie Dictionary* (online at 28 June 2019) 'aircraft'.

41 See also Stewart (n 38) 315. By contrast in, for example, New Zealand, the *Civil Aviation Rules* (NZ) contain specific provisions for drones, by requiring the operator of a drone to avoid flying over a property without the consent of the owner or occupier of the property and to avoid operating a drone in airspace above a person who has not given consent for the drone to be operating in that airspace: *Civil Aviation Rules* (NZ) r 101.207(a)(1). For further discussion of New Zealand law, including civil aviation and privacy laws, see Andrew V Shelley, 'Proposals to Address Privacy Violations and Surveillance by Unmanned Aerial Systems' (2016) 24 *Waikato Law Review* 142.

42 A new tort providing protection against disclosure where there was a reasonable expectation of privacy was recognised in *Doe v Australian Broadcasting Corporation* [2007] VCC 281 but has yet to be approved by an appellate court.

> obligation of confidence. Thirdly, there must be an [actual or threatened] unauthorised use of that information.[43]

Information with the necessary quality of confidence has been held to include personal secrets[44] and private activities.[45] However, the scope of what constitutes a 'personal secret' or 'private activity' has yet to be authoritatively settled. Chief Justice Gleeson ventured a test of what he called 'private matters', as follows:

> [K]inds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved … [the disclosure of which] would be highly offensive to a reasonable person of ordinary sensibilities.[46]

Accordingly, if this were accepted as a functional test, it may include intimate activities such as skinny-dipping, engaging in sexual activities, topless sunbathing or even surreptitious urinating in bushland.[47] Further, an obligation of confidence may arise where a recipient of that information ought to have realised on reasonable grounds that that information was obtained in confidence.[48] This would include where, for example, images were recorded using a telephoto lens or by other surreptitious means.[49] However, the cause of action for breach of confidence as a means of addressing breaches of privacy in the form of disclosure of private information is not available once the information enters the public domain,[50] whereas the affront to dignity caused by an invasion of privacy continues, and indeed may be exacerbated, the wider the dissemination. Further, currently in Australia the preponderance of authority holds that the only relevant defence to a breach of confidence is disclosure of an iniquity,[51] which has been interpreted to mean a 'crime, civil wrong or serious misdeed of public importance'.[52] This may provide a defence for the operator of a drone monitoring crops or bushland which inadvertently films, for example, illegal drug cultivation and who shares that information with law enforcement authorities. However, it would not provide a defence in a case involving information the disclosure of which may be in the public interest.[53]

---

43 *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41, 47 (Megarry J).

44 See, eg, *Argyll v Argyll* [1967] Ch 302.

45 See, eg, *Stephens v Avery* [1988] 1 Ch 449; *A v B plc* [2003] QB 195.

46 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 226 [42]. This view did not, however, attract the support of the other members of the court.

47 Butler, 'The Dawn of the Age of the Drones' (n 4) 451.

48 *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41, 48 (Megarry J); *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* (1948) 65 RPC 203, 215–6 (Lord Greene MR).

49 *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804, 807 (Laws J), approved by Gleeson CJ in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 224 [34]–[35].

50 See *A-G (UK) v Guardian Newspapers Ltd [No 2]* [1990] 1 AC 109.

51 See *Corrs Pavey Whiting & Byrne v Collector of Customs (Vic)* (1987) 14 FCR 434; *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services & Health* (1990) 22 FCR 73. These cases have rejected a wider defence for disclosure in the public interest, which has attracted limited support in Australia: see, eg, *A-G (UK) v Heinemann Publishers Australia Pty Ltd* (1987) 10 NSWLR 86, 169 (Kirby P).

52 *Australian Football League v The Age Co Ltd* (2006) 15 VR 419, 436 [69] (Kellam J).

53 Although a defence might be available in such a case if the freedom of communication concerning government or political matters applied: see *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520. See also Butler, 'The Dawn of the Age of the Drones' (n 4) 453.

2 *Surveillance Laws*

At the time of writing, five of Australia's eight states and territories had enacted legislation that prohibit the use of optical surveillance devices to observe or record private activities.[54] However, these statutes are not uniform in their terms, and the variations may have practical significance when considered in a context like invasions of privacy by a camera mounted on a drone. There are also anti-voyeurism and anti-stalking laws that may apply in some circumstances.

(a) Surveillance Devices Laws

The New South Wales *Surveillance Devices Act 2007* section 8 prohibits the knowing installation, use or maintenance of an optical surveillance device 'on or within premises or a vehicle or on any other object, to record visually or observe the carrying on of an activity',[55] which involves 'entry onto or into the premises or vehicle without the express or implied consent of the owner or occupier',[56] or 'interference with the vehicle or other object without the … consent of the person having lawful possession or lawful control of the vehicle or object'.[57] The New South Wales surveillance laws may therefore be regarded as property-based. They may readily apply where, for example, a person enters premises or a vehicle without consent and there secretes a device in order to surreptitiously record activities occurring on the premises or in the vehicle. As will be shortly seen, their application in the context of drones may be more problematic.

The statutes in the Northern Territory, Victoria and Western Australia, by contrast, simply prohibit the knowing installation, use or maintenance of an optical device to record visually or observe a 'private activity'.[58] The statutes differ, however, in their definition of 'private activity'. The Northern Territory and Western Australian statutes simply define 'private activity' as

> 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,

54 *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act 2007* (NT); *Surveillance Devices Act 2016* (SA); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA). Cf the legislation in ACT, Queensland and Tasmania, which only applies to listening devices that are used to listen to or record private conversations, and which therefore do not prohibit invasions of privacy by drone-mounted cameras: *Listening Devices Act 1992* (ACT); *Invasion of Privacy Act 1971* (Qld); *Listening Devices Act 1991* (Tas). At the time of writing, the Queensland Law Reform Commission was conducting a review of surveillance laws and privacy in that jurisdiction, and had formed the preliminary view that Queensland should enact legislation capable of applying to existing and emerging surveillance technologies which achieves 'reasonable consistency' with the surveillance devices statutes in other Australian jurisdictions: see Queensland Law Reform Commission, *Review of Queensland's Laws Relating to Civil Surveillance and Protection of Privacy in the Context of Current and Emerging Technologies* (Consultation Paper WP No 77, December 2018) [3.12].

55 *Surveillance Devices Act 2007* (NSW) s 8(1).

56 Ibid s 8(1)(a).

57 Ibid s 8(1)(b).

58 *Surveillance Devices Act 2007* (NT) s 12(1); *Surveillance Devices Act 1999* (Vic) s 7(1); *Surveillance Devices Act 1998* (WA) s 6(1). The Victorian and Northern Territory prohibitions also require that the use of the device to record or observe the private activity must be without the consent of the parties to the activity.

> 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.[59]

While the Victorian definition also refers to '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', it excludes 'an activity carried on outside a building',[60] meaning that the filming of nude sunbathing would not come within the definition.

South Australia is the latest to replace its *Listening Devices Act 1972* (SA) with surveillance devices laws. It has taken a hybrid approach that combines the activity-based approach of Victoria, Western Australia and the Northern Territory with the property-based approach of New South Wales. It prohibits a person from the knowing installation, use or maintenance of an optical device 'on or in premises, a vehicle or any other thing … to record visually or observe the carrying on of a private activity'.[61] The statute makes clear that a private activity may be either an activity carried on by only one person or by more than one person – in the case of the former, 'in circumstances that may reasonably be taken to indicate that that person does not desire it to be observed by any other person' and in the latter 'in circumstances that may reasonably be taken to indicate that at least 1 party to the activity desires it to be observed only by other parties to the activity'.[62] In both cases, however, the statute excludes any activity carried on in a public place, in premises or a vehicle if the activity can be readily observed from a public place, or which is carried on 'in circumstances in which the person [or a party to the activity] ought reasonably to expect that it may be observed by some other person'.[63] The South Australian statute also prohibits knowingly installing, using or maintaining an optical device 'on or in premises, a vehicle or any other thing to record visually or observe the carrying on of a private activity without the express or implied consent of each party to the activity' where it involves entry onto or into, or interference with, premises or a vehicle owned by another without the consent of the owner or occupier of those premises or vehicle,[64] although it may be that most, if not all, cases caught by these property-based prohibitions may also be caught by the wider activity-based prohibition.

The application of these laws in the context of drones leads to anomalous results. A drone that films a person walking around naked or engaging in sexual activity in their high-rise apartment may breach the New South Wales and South Australian property-based prohibitions if the statutes were read as prohibiting the use of an optical device (namely a camera on the drone) on or within premises (namely the air space above the yard of the apartment building) to record or observe an activity where that use involves entry onto or into the premises without

---

59 *Surveillance Devices Act 2007* (NT) s 4 (definition of 'private activity'); *Surveillance Devices Act 1998* (WA) s 3 (definition of 'private activity').

60 *Surveillance Devices Act 1999* (Vic) s 3 (definition of 'private activity').

61 *Surveillance Devices Act 2016* (SA) s 5(1). In the context of drones at least, the addition of the words 'on or in premises, a vehicle or any other thing' is of little consequence since a camera mounted on a drone constitutes installation or use of an optical device on a vehicle or other thing.

62 Ibid s 3 (definition of 'private activity').

63 Ibid.

64 Ibid ss 5(2)–(3).

the express or implied consent of the owner or occupier of the apartment building. However, such an interpretation might suggest that had the drone instead being operated by the owner or occupier, or by another individual with the permission of the owner or occupier of the apartment building, it could have been used to record or observe the naked person or sexual activity without breaking the law. However, if the same facts arose in Victoria, Western Australia or the Northern Territory then the relevant law would have been broken because the optical device on the drone would have been used to record or observe a 'private activity' carried on inside a building. It may also breach the activity-based prohibition in the South Australian statute.

By contrast, a drone that films someone skinny-dipping or sunbathing in their backyard may contravene the activity-based prohibitions in Western Australia, Northern Territory and South Australia and perhaps the property-based prohibitions in New South Wales and South Australia (in the limited circumstances discussed above) but not the activity-based prohibition in Victoria, since it would be a private activity which occurred outside of a building. If a drone-mounted camera filmed a couple discreetly engaging in sexual activity in public bushland in circumstances in which they expected not to be observed, then again a different result would be reached depending on where the incident occurred. The activity-based prohibitions may be contravened if the activity occurred in Western Australia and the Northern Territory, but not the property-based prohibition in New South Wales (because it would not involve the drone entering privately owned premises), the activity-based prohibition in Victoria (because it would have occurred outside a building) or either the South Australian activity-based prohibition (because it would have occurred in a public place) or property-based prohibition (because again it would not involve the drone entering private premises). Naturally if any of these incidents occurred in Queensland, Tasmania or the Australian Capital Territory they would not breach the surveillance laws in those jurisdictions, which are currently limited to audio recordings.[65]

(b) Anti-voyeurism Laws

Several jurisdictions have enacted laws against voyeurism, but again they vary in breadth. New South Wales prohibits filming a person 'engaged in a private act',[66] which is defined as being when that person is 'in a state of undress, using the toilet, showering or bathing, engaged in a sexual act of a kind not ordinarily done in public, or engaged in any other like activity'.[67] However, the prohibition is limited to filming 'for the purpose of … sexual arousal or sexual gratification',[68] which may be difficult to show in the circumstances and suggests an intentionality that would not capture the inadvertent filming of sexual activity.

65 *Listening Devices Act 1992* (ACT); *Invasion of Privacy Act 1971* (Qld); *Listening Devices Act 1991* (Tas).
66 *Crimes Act 1900* (NSW) s 91K.
67 Ibid s 91I(2)(a).
68 Ibid s 91K.

No such limitation applies to the anti-voyeurism laws in South Australia and Queensland. In South Australia the legislation prohibits 'indecent filming',[69] which is defined as filming another person in a state of undress or engaged in a 'private act' in 'circumstances in which a reasonable person would expect to be afforded privacy', or 'another person's private region in circumstances in which a reasonable person would not expect that the person's private region might be filmed'.[70] For these purposes 'private act' is defined as '(a) a sexual act of a kind not ordinarily done in public; or (ab) an act carried out in a sexual manner or context; or (b) using a toilet' while 'private region' means 'a person's genital or anal region, or in the case of a female, the breast, when covered by underwear or bare'.[71] The Queensland act uses even broader terms, prohibiting a person from observing or visually recording another person 'in circumstances where a reasonable adult would expect to be afforded privacy (a) without the other person's consent; and (b) when the other person (i) is in a private place; or (ii) is engaging in a private act and the observation or visual recording is made for the purpose of observing or visually recording a private act'.[72] While examples are provided of 'circumstances where a reasonable adult would expect to be afforded privacy', in the form of persons in a change room or using the toilet, the prohibition would not be limited to such cases.[73] Further, intention is not stated to be an element of the offence.[74]

Accordingly, some cases which fall outside the more general surveillance laws in Queensland (which only apply to audio recordings) or South Australia (due to its exclusion of activities occurring in public places from its definition of private activity) may nonetheless fall within the ambit of the anti-voyeurism laws in those states. Even the anti-voyeurism laws in New South Wales may prohibit cases falling outside the terms of its general surveillance laws, which require entry onto premises without consent, such as a drone filming a neighbour skinny-dipping or engaging in sexual activity whilst flying without crossing the boundary, provided the operator was doing so for the purposes of sexual gratification.

(c) Anti-stalking Laws

In some circumstances a drone operated to surveil an individual may contravene anti-stalking legislation.[75] Each statute contains inclusive lists of the types of conduct that is prohibited. Whilst there are differences in these lists, most

69 *Summary Offences Act 1953* (SA) s 26D.
70 Ibid s 26A (definition of 'indecent filming').
71 Ibid s 26A (definitions of 'private act' and 'private region').
72 *Criminal Code Act 1899* (Qld) sch 1 s 227A(1) ('*Criminal Code 1899* (Qld)').
73 Butler, 'The Dawn of the Age of the Drones' (n 4) 466.
74 *Criminal Code 1899* (Qld) s 23(2).
75 See *Crimes Act 1900* (ACT) s 35; *Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13; *Criminal Code Act 1983* (NT) sch 1 s 189 ('*Criminal Code* (NT)'); *Criminal Code 1899* (Qld) s 359E; *Criminal Law Consolidation Act 1935* (SA) s 19AA; *Criminal Code 1924* (Tas) s 192; *Crimes Act 1958* (Vic) s 21A; *Criminal Code 1913* (WA) s 338E.

include keeping a person 'under surveillance or watching a person,[76] and some include '[engaging] in conduct amounting to intimidation, harassment or molestation'.[77] There are other variations in these laws. For example, several jurisdictions require 'a course of conduct'[78] or for the conduct to be 'repeated',[79] or to occur 'on at least two occasions'[80] while in some it is also sufficient if the conduct occurs on one occasion provided it is 'protracted' or 'sustained'.[81] Most statutes would also require the drone operator to act with the intention of intimidating, 'causing physical or mental harm to, or of arousing an apprehension or fear in' the person being stalked.

Like the surveillance devices and anti-voyeurism laws, the anti-stalking laws only constitute criminal offences and make no provision for the victims of the prohibited conduct to obtain civil remedies against the perpetrators.[82]

3 Data Protection Laws

Images of a person constitute 'personal information' for the purposes of Commonwealth and state data protection legislation since they are information about an identified individual whose identity 'is apparent or can reasonably be ascertained'.[83] Accordingly, drones operated by a Commonwealth agency or a private organisation with an annual turnover of over $3 million will be subject to the Australian Privacy Principles ('APPs'), while drones operated by a State (with the exception of Western Australia) or Northern Territory agency will be subject

76 *Crimes Act 1900* (ACT) s 35(2)(c); *Criminal Code* (NT) s 189(1)(f); *Criminal Code 1899* (Qld) s 359B(c)(i); *Criminal Law Consolidation Act 1935* (SA) s 19AA(1)(a)(v); *Criminal Code 1924* (Tas) s 192(1)(b); *Crimes Act 1958* (Vic) s 21A(2)(f).

77 *Crimes Act 1900* (ACT) s 35(2)(j). See also *Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 7(1)(a); *Criminal Code 1899* (Qld) s 359B(c)(iv).

78 *Crimes Act 1958* (Vic) s 21A(2).

79 *Criminal Code* (NT) s 189(1).

80 *Crimes Act 1900* (ACT) s 35(2); *Criminal Law Consolidation Act 1935* (SA) s 19AA(1)(a).

81 *Criminal Code 1899* (Qld) s 359B(b) (one occasion if protracted or on more than one occasion); *Criminal Code 1924* (Tas) s 192(2) (sustained conduct or conduct that occurs on more than one occasion).

82 In *Grosse v Purvis* [2003] Aust Torts Reports ¶81-706, 64184 [420] Skoien SDCJ noted that 'in perhaps all of the offences contained in the Code in which an individual person would be named in the indictment as the complainant (or victim) an actionable tort is encompassed so that the victim would have the right to sue in the civil court for damages'. The absence of a tort counterpart to stalking formed part of the basis for his Honour recognising a new tort for invasion of privacy in the form of unreasonable intrusion on an individual's seclusion: at 64187 [445]. His Honour thought that such an action would make unnecessary a tort of harassment, which was described by Gummow and Hayne JJ in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 255 [123] as a possible developing tort: see *Grosse v Purvis* [2003] Aust Torts Reports ¶81-706, 64,187–8 [448]–[451]. As already noted above in n 30, the judgment in *Grosse v Purvis* is yet to be approved by an appellate court.

83 *Privacy and Personal Information Protection Act 1998* (NSW) s 4 (definition of 'personal information'). See also *Privacy Act 1988* (Cth) s 6 (definition of 'personal information'); *Information Act 2002* (NT) s 4A; *Information Privacy Act 2009* (Qld) s 12; *Personal Information Protection Act 2004* (Tas) s 3 (definition of 'personal information'); *Privacy and Data Protection Act 2014* (Vic) s 3 (definition of 'personal information'). See, eg, *SW v Forest NSW* [2006] NSWADT 74, [31] (Member Handley); *Ng v Department of Education* [2005] VCAT 1054, [39] (Macnamara DP). Whilst South Australia does not have a legislated protection regime, it has a data protection regime by administrative order: Department of Premier and Cabinet (SA), *Cabinet Administrative Instruction 1/89*, 6 February 2017 ('*Cabinet Administrative Instruction 1/89* (SA)'). Western Australia has no data protection regime.

to the Information Privacy Principles ('IPPs'). The APPs and IPPs contain similar, but not identical provisions concerning matters such as the collection, use and disclosure of personal information. Even the IPPs are not expressed in the same terms in the State and Northern Territory instruments. For example, there are differences in providing that information must not be collected by 'unlawful'[84] or 'unlawful or unfair means';[85] or be collected 'only by lawful and fair means and not in an unreasonably intrusive way',[86] be collected 'only by lawful and fair means'[87] or be collected 'by lawful means'.[88] When determining whether the collection of images by a drone was by 'lawful' or 'unlawful' means, reference might be had to whether the drone was being flown in accordance with part 101 of the *CASR*.[89]

The data protection regimes are therefore limited in their application. They will not, for example, apply to recreational operators of drones, or organisations with an annual turnover of $3 million or less. In addition, media organisations are exempt under the *Privacy Act 1988* (Cth) from the provisions of the APPs.[90]

III UNITED KINGDOM

A Regulation of Drones

In the United Kingdom the operation of drones, like other aircraft, is governed by the *Air Navigation Order 2016* (UK) SI 2016/765 ('*ANO*'). The *ANO* was amended in 2018 with changes introduced that concern the operation of small unmanned aircraft ('SUA').

Article 94(3) provides that the remote pilot[91] of a 'small unmanned aircraft', which is defined as 'any unmanned aircraft … having a mass of not more than 20 kg',[92] must 'maintain direct, unaided visual contact with the aircraft sufficient to monitor its flight path' for the purpose of avoiding collisions with 'other aircraft,

84 *Privacy and Personal Information Protection Act 1998* (NSW) s 8(2).

85 *Information Privacy Act 2009* (Qld) sch 3 cl 1(2); *Cabinet Administrative Instruction 1/89* (SA) (n 83) [4(1)].

86 *Information Act 2002* (NT) sch 2 cl 1.2; *Privacy and Data Protection Act 2014* (Vic) sch 1 cl 1.2.

87 *Privacy Act 1988* (Cth) sch 1 cl 3.5.

88 *Personal Information Protection Act 2004* (Tas) sch 1 cl 1(2).

89 See the discussion in Butler, 'The Dawn of the Age of the Drones' (n 4) 463.

90 *Privacy Act 1988* (Cth) s 7B(4).

91 The 2018 amendments replaced the concept of a 'person in charge' of a SUA with a 'remote pilot' and a 'SUA operator'. *Air Navigation Order 2016* (UK) SI 2016/765 art 94G ('*ANO*') defines 'remote pilot' as an individual who operates the flight controls of a SUA by manual use of remote controls or who is able to intervene by operating the flight controls when the SUA is flying automatically, while a 'SUA operator' is a person who has the management of the SUA. Thus, for example, when a child has the controls of the SUA [they] would be the remote pilot while [their] parent who might be supervising the flight would be the SUA operator. In many cases, however, the remote pilot and SUA operator will be the same person: Civil Aviation Authority, *Air Navigation Order 2018 and 2019 Amendments – Guidance for Small Unmanned Aircraft Users* (CAA Publication No CAP 1763, February 2019) 9. The separate terms have been introduced to recognise different levels of responsibility and to accommodate different registration and competency requirements to be introduced in November 2019: ibid.

92 *ANO* sch 1 art 1 (definition of 'small unmanned aircraft').

persons, vehicles, vessels and structures'. Further, any small unmanned aircraft must not fly at a height of more than 400 feet above the surface[93] or in restricted airspace, within one kilometre of airport boundaries.[94] This one kilometre exclusion zone is to be expanded to five kilometres from the ends and sides of the runway,[95] a decision that shortly preceded and was vindicated by an incident in which at least one drone was spotted near Gatwick Airport shortly before Christmas in 2018 leading to days of disruption, including the cancellation of about 800 flights and affecting the travel plans of over 100,000 passengers.[96] Users who fail to observe these restrictions could be charged with recklessly or negligently acting in a manner likely to endanger an aircraft or any person in an aircraft, which could result in an unlimited fine and/or up to five years in prison.

Moreover, article 95(2) provides that a 'small unmanned surveillance aircraft' – that is a drone mounted with a camera – must not be flown:

> (a) over or within 150 metres of any congested area;
> (b) over or within 150 metres of an organised open-air assembly of more than 1,000 persons;
> (c) within 50 metres of any vessel, vehicle or structure which is not under the control of the SUA operator or the remote pilot of the aircraft; or
> (d) … within 50 metres of any person [except when taking off or landing, when it may be within 30 metres of a person].[97]

Generally speaking, the requirement in article 94 of flying with direct, visual contact would exclude a person flying a camera-mounted drone operating solely via the video streaming to a mobile phone, tablet or video goggles which might provide the operator with the equivalent of a 'pilot's eye view' (otherwise known as 'First Person View' ('FPV')). There are sound reasons for this since an operator relying on FPV may not have a sufficient appreciation of the drone's flight path and surroundings to avoid a collision. However, the Civil Aviation Authority ('CAA') has issued a General Exemption for FPV[98] where the small unmanned aircraft does not exceed 3.5 kg and the person in charge of the aircraft is accompanied by a 'competent observer' who is 'fully briefed on the planned flight and what is expected of him/her, taking into account the prevailing conditions … [stays] directly adjacent to the remote pilot and [maintains] direct unaided visual contact' with the aircraft at all times.[99]

Unmanned aircraft with a mass of more than 20 kg are subject to normal aviation regulations, although they may be exempted from some requirements by

93 Ibid art 94A(2).
94 Ibid arts 94A(4), 94B.
95 Department for Transport, *Taking Flight: The Future of Drones in the UK* (UK Government Response Paper, January 2019) 11 [2.5]. Nonetheless drone operators will be able to seek permission from air traffic controllers to fly within this exclusion zone, such as where a commercial drone operator wishes to inspect a building: at 12 [2.6].
96 See, eg, Gwyn Topham, Matthew Weaver and Haroon Siddique, 'Runway Reopens after Days of Drone Disruption at Gatwick', *The Guardian* (online, 21 December 2018) <https://www.theguardian.com/uk-news/2018/dec/20/tens-of-thousands-of-passengers-stranded-by-gatwick-airport-drones>.
97 *ANO* sch 1 art 95(2).
98 Civil Aviation Authority, *Small Unmanned Aircraft – First Person View (FPV) Flying* (ORS4 No 1294, 7 March 2019).
99 Ibid [3], [7].

the CAA. Thus, for example, the operator of such a drone must obtain a specific approval before any flight can take place.

In 2017 the UK Department of Transport released its response to a consultation on the use of drones.[100] The Report sought to strike a balance between 'enabling and supporting the UK drones application industry to grow and become world leading' and 'maintaining [the country's] world class aviation safety record and addressing security and privacy concerns'.[101] The government's response is to increase accountability of drone operators. As from 30 November 2019 all users of drones of 250 g and above will be required to register their drones and themselves.[102] The registration scheme is seen as potentially providing a platform for user education, including 'safety, security and privacy issues', as well as embedding electronic identification and tracking capability 'so that enforcement action against irresponsible drone use may be improved'.[103] In addition, mandatory competency testing will be introduced for remote pilots, whether commercial or recreational.[104] This testing, and training materials for taking the test, will include safety, security and privacy issues.[105] Users who fail to register or to take the competency tests may face fines of up to £1,000.[106]

B Protection of Privacy

Like Australia, privacy in the United Kingdom is protected by a range of common law causes of action and legislation.

1 Common Law

A right to privacy is guaranteed by article 8 of the *European Convention on Human Rights* ('*ECHR*').[107] However, in some circumstances, such as where privacy is breached by publication of private information by the media, there may be a conflict between this right and the right to free expression guaranteed by article 10. Under the *Human Rights Act 1988* (UK), English courts are obliged to ensure that the common law conforms to this Convention. Following the seminal case *Campbell v MGN Ltd*[108] these two rights are balanced by a two-stage enquiry, which may be summarised as follows:

100 Department of Transport, *Unlocking the UK's High Tech Economy: Consultation on the Safe Use of Drones in the UK* (UK Government Response Paper, July 2017) ('*Consultation on the Safe Use of Drones*').

101 Ibid 4–5.

102 See *ANO* arts 94C–94D (registration as an SUA operator).

103 *Consultation on the Safe Use of Drones* (n 100) 9.

104 See *ANO* art 94E (competency of remote pilots).

105 *Consultation on the Safe Use of Drones* (n 100) 8–9.

106 The Drone (Regulation) Bill 2017–19 is expected to have its second reading debate in the near future.

107 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953), as amended by *Protocol No 14bis to the Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 27 May 2009, CETS No 204 (entered into force 1 September 2009).

108 [2004] 2 AC 247.

(1) A determination of whether the person publishing the information knows or ought to know that there is a reasonable expectation the information in question will be kept confidential; and

(2) Once that threshold was reached, balancing, as a matter of fact and degree, the interest of the recipients in publishing the information, giving full recognition to the importance of free expression and (in a case involving the media) with a measure of latitude shown for the practical exigencies of journalism such as the fact that editorial decisions must often be made in the context of tight deadlines.[109]

The United Kingdom has a growing jurisprudence applying this two-stage test to invasions of privacy in the form of disclosure of private information,[110] or the tort of 'misuse of private information' as it is now known.[111] Thus where a person uses a drone to record footage of private activities such as topless sunbathing, skinny-dipping or sexual activity and then uploads that footage to a social media site, the case will likely be determined on the question of whether the filmed person had a reasonable expectation that the activity would be kept confidential. The mere fact that the activity takes place in view of others is not conclusive: for example children are typically afforded a high expectation of privacy.[112] Further, even cases that may be thought to involve a reasonable expectation of privacy, such as sexual activity, it is possible that there may be a countervailing right to free expression depending on the participants and the context of the relationship, such as where publication corrects a false image of a public figure.[113]

By contrast, a claim for an invasion of privacy in the form of an intrusion on seclusion was dismissed in *Kaye v Robertson*.[114] This was unchanged by the *Human Rights Act 1988* (UK): when it had the opportunity to consider the question, the House of Lords rejected the notion that as a result of article 8 of the *ECHR* and the *Human Rights Act 1988* (UK) a general tort of privacy formed part of English Law.[115] However, a form of protection against intrusion was recognised by Tugendhat J in *Goodwin v NGN Ltd*,[116] a case that initially involved a claim by the Chief Executive Officer of a global corporation seeking to restrain a newspaper from publishing details of his sexual relationship with a female employee. The businessman's claim was dismissed on the ground that publication was in the public interest, but his Honour would not allow publication of the woman's name

109 Butler, 'The Dawn of the Age of the Drones' (n 4) 449, in which the following decisions were cited regarding the first stage: *Campbell v MGN Ltd* [2004] 2 AC 457, 466 [21] (Lord Nicholls), 480 [85] (Lord Hope), 495 [134] (Baroness Hale), citing *A v B plc* [2003] QB 195, 202 [4], 207 [11] (Lord Woolf CJ). See *Venables v News Group Newspapers Ltd* [2001] Fam 430, 462 [81] (Butler-Sloss P). The following decision was cited regarding the second stage: *Campbell v MGN Ltd* [2004] 2 AC 247, 475 [62] (Lord Hoffman), 491 [120] (Lord Hope), 505 [169] (Lord Carswell).

110 See, eg, *Douglas v Hello! Ltd [No 3]* [2008] 1 AC 1; *Murray v Express Newspapers plc* [2009] Ch 481; *K v News Group Newspapers Ltd* [2011] EWCA Civ 439.

111 See, eg, *Campbell v MGN* [2004] 2 AC 457, 465 [14] (Lord Nicholls); *Vidal-Hall v Google Inc* [2016] QB 1003.

112 See, eg, *Murray v Express Newspapers plc* [2009] Ch 481; *AAA v Associated Newspapers Ltd* [2012] EWHC 2103 (QB); *Weller v Associated Newspapers Ltd* [2014] EWHC 1163 (QB).

113 See, eg, *Campbell v MGN Ltd* [2004] 2 AC 457; *Ferdinand v MGN Ltd* [2011] EWHC 2454 (QB).

114 (1991) 19 IPR 147.

115 See *Wainwright v Home Office* [2004] 2 AC 406.

116 [2011] EWHC 1437 (QB).

on the ground of the intrusion into her private life.[117] He saw article 8 as embracing two core components: unwanted access to private information, which he called 'confidentiality', and unwanted access to or intrusion into one's personal space, which he called 'intrusion'. Further, the same balancing exercise applied in both types of case: the first question was whether there was a reasonable expectation of privacy in the circumstances, and if so then it must be balanced against the freedom of expression guaranteed by article 10. However, it is not clear whether the protection against intrusion only arises where there is also publication or threatened publication.

It is yet to be seen whether such recognition of protection of privacy against intrusion may apply in other contexts, such as a drone filming a skinny-dipper or sexual activity, with or without a threatened or actual misuse of that information by wide dissemination. If not, then a person who is aggrieved in such a way would have resort only to other established causes of action such as trespass to land or private nuisance, with the same limitations as already identified.[118]

2 Protection from Harassment Act 1997 (UK)

While there are no general surveillance statutes similar to those in most Australian jurisdictions, the *Protection from Harassment Act 1997* (UK) may provide redress in some cases of intrusion that is similar to conduct prohibited by Australian anti-stalking laws.

This statute prohibits a person from pursuing 'a course of conduct' that amounts to 'harassment of another, and … which [they know] or ought to know amounts to harassment of the other'.[119] Harassment is a crime[120] but may also give rise to a civil remedy in the form of damages, which 'may be awarded for (among other things) any anxiety … and any financial loss resulting from the harassment'.[121] The statute provides that 'course of conduct' must involve conduct on at least two occasions.[122]

Accordingly, the statute would not apply to, for example, a single instance where the person uses a drone to spy on a neighbour and thereby causes the neighbour to suffer anxiety or distress, but may apply if that person repeated the behaviour. Lord Hoffmann has observed that the requirement of a course of conduct 'shows that Parliament was conscious that it might not be in the public interest to allow the law to be set in motion for one boorish incident'.[123]

3 Data Protection

In the United Kingdom the *Data Protection Act 2018* (UK) ('*DPA*') governs the processing (collecting, using, storing and disclosing) of 'personal data', that is

117 Ibid [125].

118 As in Australia, no trespass or private nuisance is committed by an aircraft flying at a reasonable height: see the *Civil Aviation Act 1982* (UK) s 76.

119 *Protection from Harassment Act 1997* (UK) s 1(1).

120 Ibid s 2.

121 Ibid s 3(2).

122 Ibid s 7(3).

123 *Wainwright v Home Office* [2004] 2 AC 406, 426 [46].

'any information relating to an identified or identifiable living individual'.[124] Like the various Australian data protection statutes, this act may therefore apply where a drone mounted with a camera captures the image of a person's face, car registration numbers or other such information from which an individual may be identified. The act expressly acknowledges[125] that processing of personal data is subject to the General Data Protection Regulation (EU) 2016/679 ('*GDPR*'),[126] which automatically became binding on Member States on 25 May 2018. The *DPA* gained the Royal Assent on 23 May 2018.

Article 5 of the *GDPR* provides, inter alia, that personal data shall be processed 'lawfully, fairly and in a transparent manner' and 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'. Further, article 13 provides that where personal data relating to a data subject is collected from the data subject, the 'controller shall, at the time when personal data is obtained, provide the data subject with … information' including the 'identity and the contact details of the controller'. *GDPR* article 4(7) defines 'controller' as the 'natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.

The *DPA* has none of the limits on application to government agencies and private organisations of a certain size found in Australian data privacy laws.[127] Accordingly, its provisions prima facie apply to controllers that are not only government agencies and private organisations of any size but also individual operators of drones, including those being used for recreational purposes. However, there is an exclusion in section 21 for 'the processing of personal data by an individual in the course of a purely personal or household activity'. Thus, for example, where a drone is used for recreational purposes by an individual to film family and friends for their own enjoyment the provisions of the *GDPR* will not apply. However, where, for example, an individual uses a drone to surreptitiously film a neighbour who is skinny-dipping or engaging in sexual activity and then uploads that footage to a social media site, they may no longer be regarded as having collected and disclosed that personal data for 'personal or household activity' and will therefore be obliged to comply with the *GDPR*, including articles 5 and 13. It is easy to conceive of a breach of the *GDPR* in such circumstances.

Further, article 85 of the *GDPR* allows Member States to enact exemptions in order to strike their own balances between 'protection of personal data pursuant to [the *GDPR* and] the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or

124 *DPA* s 3(2).

125 Ibid s 1.

126 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('*GDPR*').

127 As noted, drones operated by a Commonwealth agency or a private organisation with an annual turnover of over $3 million are subject to the APPs, while drones operated by a state (with the exception of Western Australia) or Northern Territory agency are subject to the IPPs.

literary expression'. The United Kingdom enacted paragraph 26 in part 5 of schedule 2 of the *DPA*, which provides that many of the provisions of the *GDPR*, including articles 5(a)–(e)[128] and 13, do not apply where 'the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material, and … the controller reasonably believes that the publication of the material would be in the public interest'.[129] Further, when 'determining whether it is reasonable to believe that the publication would be in the public interest, the controller must have regard to any of the [relevant] codes of practice or guidelines',[130] namely the BBC Editorial Guidelines, the Ofcom Broadcasting Code (for television broadcasters) or the Editors' Code of Practice (for newspapers and magazines). 'Journalism' for the purposes of the previous exemption in section 32 of the *Data Protection Act 1998*, which the *DPA* replaced, was held to be a broad and elastic concept which goes beyond simply the activities of media undertakings and incorporates other activities which have as their own objective the disclosure to the public of information, opinions and ideas.[131] The same interpretation is likely to be applied to the *DPA* exemption. The exemption is therefore a wide one that might extend to a drone being operated by, for example, a paparazzo.

Regulation of the media, including its handling of data, has been the subject of extensive debate in the United Kingdom, both inside and outside Parliament, in the wake of the Leveson Inquiry into the culture, practices and ethics of the British press.[132] This Inquiry found that there had been widespread abuses by journalists and others associated with News International, including the hacking of the phones of murder victims, families of fallen soldiers, and celebrities. The updating of the data protection laws ahead of the GDPR coming into effect involved addressing a number of issues.[133] This included debate about which of the two regulatory bodies – IPSO (Independent Press Standards Organisation) or IMPRESS (Independent Monitor for the Press) – would have its code included in the guidelines. Most of the major national newspapers, several of which have the same owner such as Rupert Murdoch's News UK, and many regional newspapers are members of IPSO, while the membership of IMPRESS currently is limited to small circulation newspapers. IMPRESS has been found by the independent Press Recognition Panel ('PRP') to be fully compliant with the 29 criteria for satisfactory regulation set by the Leveson Inquiry.[134] Whilst lauded by the current Conservative

128 The exemption from *GDPR* article 5 concerning processing of personal data does not include the obligation to process data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing: article 5(f).

129 *DPA* sch 2 cl 26(2).

130 Ibid sch 2 cl 26(5).

131 *NT1 v Google LLC* [2018] EWHC 799 (QB), [98] (Warby J).

132 Lord Justice Brian Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (Report, November 2012).

133 See generally Greg Callus, 'The New Regime: GDPR and Journalism', *Press Gazette* (online, 1 June 2018) <https://www.pressgazette.co.uk/the-new-regime-gdpr-and-journalism/>.

134 See Press Recognition Panel, *PRP Board Decision in Respect of the Application for Recognition from IMPRESS: The Independent Monitor of the Press CIC* (Report, 25 October 2016) <https://pressrecognitionpanel.org.uk/wp-content/uploads/2016/07/IMPRESS-decision-report-21-November-2016.pdf>.

Government and major tabloid newspapers, IPSO by contrast has been criticised by the PRP as being deficient against these criteria, particularly in relation to the most important among them.[135] Nevertheless, only IPSO's code, which is known as the Editor's Code of Practice, was included in the PDA exemption. Moreover, while section 32 required the court to consider the editor's compliance with the code when publishing, the *DPA* paragraph 26 exemption requires the controller, that is the media organisation, to have regard to the relevant code. This may have practical significance in terms of current practices in newsrooms, and whether sufficient documented evidence is made of such matters.[136]

Accordingly, depending on the circumstances, a drone operated by a media organisation may be exempt from the provisions of the *GDPR*. This would enable, for example, a drone operated by employees of a major tabloid to take photos of individuals and publish them if the paper reasonably believes it to be in the public interest, having reference to the Editor's Code of Practice. However, this may still be problematic. For example, images of a celebrity working out might on one view be regarded as merely of interest to the public, rather than in the public interest. By contrast, the editor of such tabloid publication might claim that such images promote public health by illustrating a role model engaging in such behaviour. In any event, the reference to the IPSO code is significant. IPSO has failed to conduct a single investigation in the four years of its existence, nor managed to secure a full-page apology or correction even when there has been a front-page breach of the Editor's Code.[137] It has been observed that despite the findings of the Leveson Inquiry, elements of the media are still engaging in the same type of unethical behaviour, such as the intrusions upon the families of victims of the bombings at Manchester Arena after an Ariana Grande concert.[138] Accordingly, even if a media-operated drone were to capture images in breach of the *GDPR*, there may be little hope of the breach resulting in some form of remedy.

135 See Press Recognition Panel, Submission No DPB31 to House of Commons Public Bill Committee, *Data Protection Bill* (14 March 2018) <https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/memo/dpb31.pdf>. This includes arbitration ('not currently compliant'), independence ('insufficient information'), funding ('criterion not currently met'), powers ('criterion not currently met') and sanctions ('criteria not currently met'): Brian Cathcart, 'A Dose of Reality about IPSO for Matt Hancock' *Byline* (online, 27 June 2018) <https://www.byline.com/column/68/article/2210>.

136 Callus (n 133).

137 Cathcart (n 135).

138 Steven Barnett, 'The Government Scuppers Leveson Part 2: Is Britain's Press Undermining Democracy?' *Democratic Audit UK* (Web Page, 21 May 2018) <http://www.democraticaudit.com/2018/05/21/the-government-scuppers-leveson-part-2-is-britains-press-undermining-democracy/>.

IV UNITED STATES

A Regulation of Drones

In 2016, title 14 *Code of Federal Regulations* ('14 CFR') was amended by insertion of a new part 107[139] governing the operation of small unmanned aircraft systems ('UAS'), which are defined as unmanned aircraft weighing less than 55 pounds (25 kg) for non-recreational, commercial use. The regulations establish a number of operating rules which include:

- A restriction to visual line of sight (which is not satisfied by first person view camera on the UAS) and daylight operations;[140]
- A limit on operating height to 400 feet above ground level and ground speed of 87 knots (100 mph or 160 kph);[141]
- A prohibition against operation over any person who is not directly participating in the operation, under a covered structure or inside a covered stationary vehicle;[142] and
- A prohibition against flying near airports and in other designated airspace.[143]

A person operating a small UAS must either hold a remote pilot certificate with a small UAS rating or be under the direct supervision of a person who holds a remote pilot certificate. Obtaining a remote pilot certificate requires the applicant to be at least 16 years old, pass an aeronautical knowledge test at an FAA-approved knowledge-testing centre and be vetted by the Transportation Security Administration.[144]

For a time, part 107 did not apply to small UAS not being operated for commercial purposes. The 'Special Rule for Model Aircraft' under section 336 of the *FAA Modernization and Reform Act of 2012*, Pub L No 112-95, 126 Stat 11 provided that the FAA could not promulgate regulations regarding a model aircraft that did not exceed 55 pounds (25 kg) that was flown for hobby or recreational purposes. Nonetheless, the US Code was amended to provide that a small UAS of greater than 0.55 pounds (250 g) and less than 55 pounds (25 kg), whether operated for commercial or hobby or recreational purposes, is like any other aircraft required to be registered as a condition of its operation in US airspace.[145] While these requirements were challenged as being contrary to section 336, leading to

139 The regulations, which were promulgated by the Federal Aviation Administration (FAA) after consultations with stakeholders, were in response to the *FAA Modernization and Reform Act of 2012*, Pub L No 112-95, 126 Stat 11 (2012), which inter alia provided deadlines for the safe integration of unmanned aerial systems into the national airspace by late 2015.

140 See 14 *CFR* §§ 107.29, 107.31 (2019).

141 Ibid § 107.51 (2019).

142 Ibid § 107.39 (2019).

143 Ibid §§ 107.41, 107.43, 107.45, 107.47 (2019).

144 Ibid §§ 107.53–107.79 (2019).

145 See 49 USC §§ 44101–6, 44110–13 (2018).

them being struck down before being restored,[146] the position was ultimately clarified by the repeal of section 336 itself.[147] The purpose of registration is to identify the aircraft to its owner and to educate operators about the safe and responsible use of unmanned aircraft.[148] The FAA will also be able to enact regulations that include remote identification and tracking of all drones.[149]

B Protection of Privacy

While part 107 of 14 CPR addressed the safe integration of drones in the national airspace, the FAA explicitly stated that issues of privacy were beyond the scope of its remit, which solely concerns safety.[150] Accordingly, President Obama issued an executive memorandum directing the federal government to create standards addressing privacy issues associated with drones operated by federal government agencies.[151] While the executive memorandum left privately operated drones and those operated by state government agencies to be largely addressed by the states,[152] it also directed the National Telecommunications and Information Administration of the US Department of Commerce to create a private-sector engagement process to develop involuntary best practices for privacy and

146 *Taylor v Huerta* (DC Cir, No 15-1495, 19 May 2017). However, this decision was specifically overturned and the requirements reinstated by the *National Defense Authorization Act for Fiscal Year 2018*, Pub L No 115-91, § 1092, 131 Stat 1283.

147 *FAA Reauthorization Act of 2018*, Pub L No 115-254, § 349(2), 132 Stat 3186.

148 United States Government Accountability Office, *Small Unmanned Aircraft Systems: FAA Should Improve Its Management of Safety Risks* (Report to Congressional Committees No GAO-18-110, May 2018) 19–23.

149 In December 2018 the FAA issued a 'Request for Information' for partners in the development of an approach to sharing data that would be required to remotely identify small drones in controlled airspace, which will include data such as a unique identifier for the UAV, tracking information, and drone owner and remote pilot identification: FAA, *FAA UAS Remote Identification Request for Information (RFI)* (Special Notice Announcement No 32227, 20 December 2018). <https://faaco.faa.gov/index.cfm/announcement/view/32227>

150 See the FAA's Notice of Proposed Rule Making: *Operation and Certification of Small Unmanned Aircraft Systems* 80 Fed Reg 9544, 9552 (23 February 2015). Proceedings were commenced against the FAA by the Electronic Privacy Information Center ('EPIC') alleging that the *FAA Modernization and Reform Act of 2012*, Pub L No 112-95, 126 Stat 11 (2012) required the agency in its rulemaking to not only consider safety issues but also privacy issues raised by drones. However, the action was dismissed on the grounds that EPIC lacked standing to maintain the suit: *Electronic Privacy Information Center v Federal Aviation Administration* (DC Cir, No 16-1297, 19 June 2018).

151 The White House, Office of the Press Secretary, *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (Presidential Memorandum, 15 February 2015) <https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua>. For an example of standards developed following President Obama's Presidential Memorandum, see US Department of Homeland Security Privacy Civil Rights & Civil Liberties Unmanned Aircraft Systems Working Group, *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft Systems Programs* (18 December 2015) <https://www.dhs.gov/sites/default/files/publications/UAS%20Best%20Practices.pdf>.

152 For a discussion of common law privacy-related torts in the United States, see Rebecca L Scharf, 'Drone Invasion: Unmanned Aerial Vehicles and the Right to Privacy' (2019) 94(3) *Indiana Law Journal* (forthcoming).

commercial and private drone use. These best practices were issued in May 2016.[153]

The privacy implications of the operation of drones in the United States also cannot be divorced from the constitutional context operating in that country. In particular, the Fourth Amendment of the *United States Constitution* will be relevant to any invasion of privacy by government agencies while the First Amendment may be relevant in some cases involving non-government entities.[154]

1 Surveillance and the Fourth Amendment

The Fourth Amendment of the *United States Constitution* provides protection against 'unreasonable searches and seizures'. This was originally interpreted in terms of providing protection from law enforcement trespassing upon real property,[155] but is now seen as embodying two questions: (1) whether 'a person [has] exhibited an actual (subjective) expectation of privacy' and (2) whether 'the expectation [is] one that society is prepared to recognize as reasonable'.[156]

The United States Supreme Court has not yet considered the Fourth Amendment in the context of invasions of privacy by drones, but nonetheless in a series of cases has established jurisprudence concerning aerial surveillance which will be apropos.[157] These cases have generally involved the use of light aircraft or helicopters to observe or conduct surveillance on properties suspected of being used for nefarious or undesirable activities,[158] as well as one concerning the use of technology for surveillance,[159] and have held that relevant questions when determining whether there is a reasonable expectation of privacy for the purposes of the Fourth Amendment in the context of surveillance by a government agency from the air will include whether the observations are made from public airspace at a height the public may be expected to travel and whether the technology used is in general public use.[160] It is reasonable to expect that the extent to which the second aspect provides protection for privacy will diminish as drones become

153 National Telecommunications and Information Administration, *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability: Consensus, Stakeholder-Drafted Best Practices Created in the NTIA-Convened Multistakeholder Process* (18 May 2016). <https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf>.

154 As a matter of technicality, the Fourteenth Amendment will also be relevant in applying the Bill of Rights equally in a state rather than federal context: see, eg, *Near v Minnesota*, 283 US 697 (1931) (First Amendment); *Mapp v Ohio*, 367 US 643 (1961) (Fourth Amendment).

155 *Olmstead v United States*, 277 US 438, 464–6 (Taft CJ) (1928).

156 *Katz v United States*, 389 US 347, 361 (Harlan J) (1967).

157 See also Jessica Dwyer-Moss, 'The Sky Police: Drones and the Fourth Amendment' (2018) 81(3) *Albany Law Review* 1047.

158 See *Dow Chemical Co v United States*, 476 US 227 (1986) (Environmental Protection Agency used light aircraft to fly in navigable airspace to photograph a chemical plant); *California v Ciraolo*, 476 US 207 (1986) (law enforcement officers flew at a height of 1,000 feet in a light aircraft to observe premises suspected of being used to cultivate drugs); *Florida v Riley*, 488 US 445 (1989) (law enforcement officers flew in a helicopter at a height of 400 feet to observe premises suspected of being used to cultivate drugs).

159 *Kyllo v United States*, 533 US 27 (2001) (law enforcement used thermal imaging device to measure external temperature of wall and roof of property suspected of being used for drug cultivation).

160 See also Villasenor (n 4) 486.

more commonplace. Perhaps of greater significance will be the meaning of 'public navigable airspace' when applied in the context of drones.[161]

This will be a complex problem to resolve. Whilst FAA-regulated altitudes for operation of fixed wing aircraft[162] would suggest that drones would largely operate beneath such airspace, helicopters (with which drones are more analogous) are exempt from such regulated altitudes provided their operation 'is conducted without hazard to person or property on the surface'.[163] However, they are subject to the general requirement that they be operated at an altitude that is high enough to allow 'an emergency landing without undue hazard to persons or property on the surface'.[164] The height needed to safely land a drone in case of emergency is likely to be lower – in many cases significantly so – than a helicopter. There are two further complications. First, as already noted, in the case of a small UAS there is a prescribed *maximum* height of operation of 400 feet. Secondly, the US Supreme Court has recognised that the rights of a landowner extend to the exclusive control of the 'immediate reaches of the enveloping atmosphere'.[165] Consequently, if there is to be a 'public navigable airspace' for drones it will need to be above the height of the 'immediate reaches of the enveloping atmosphere' and below the maximum height operation for such craft.

2 Common Law

In the United States, like Australia and the United Kingdom, an aggrieved individual may seek to base a claim on trespass to land, but may also have recourse to more specific privacy torts in the form of intrusion on seclusion[166] and public disclosure of private facts,[167] which have been recognised by courts in most states. The intrusion tort has the advantage of not being dependant on property rights in the same way as the action for trespass to land whilst the disclosure tort provides a remedy for dissemination of any private information, including video and images, that may have been acquired. Other actions that may be relevant include negligent,[168] or even intentional,[169] infliction of emotional distress.

---

161 See generally ibid 489–93.

162 See 14 CFR § 91.119(b)–(c) (2019), which prescribes a minimum height of 1,000 feet over congested areas and 500 feet over non-congested areas when not taking off or landing.

163 Ibid § 91.119(d) (2019).

164 Ibid § 91.119(a) (2019).

165 *United States v Causby*, 328 US 256, 264 (Douglas J) (1946).

166 See American Law Institute, *Restatement (Second) of Torts* (1977) § 652B, which provides a remedy where 'one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person'.

167 Ibid § 652D, which provides a remedy where one person 'gives publicity to a matter concerning the private life of another [which is matter] of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public'.

168 Ibid § 313.

169 Ibid §§ 46, 312. This tort, also known as the 'tort of outrage', is now supported by an extensive body of jurisprudence in the United States, whereas the counterpart in Australia and the United Kingdom, the rule in *Wilkinson v Downton* [1897] 2 QB 57, has had limited application, perhaps due to the requirement of showing a recognisable psychiatric injury rather than mere emotional distress: see, eg, Des Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29(2) *Melbourne University Law Review* 339, 367.

In relation to the privacy torts, the primary consideration will be whether the aggrieved person had a reasonable expectation of privacy in the circumstances. As has already been argued, a person filmed by a drone engaging in intimate activities inside their house or skinny-dipping in their pool will likely have such an expectation where those activities are otherwise not readily observable. Even public figures, who are presumed to have a lesser expectation of privacy than private individuals,[170] are entitled to expect that their homes may offer a safe haven from scrutiny.

However, in some cases the First Amendment may provide important protection against common claims for invasion of privacy for drone operators including media organisations or other private entities seeking to gather information.[171] Nevertheless, it has been recognised that the First Amendment protection is not absolute. This was illustrated in a Californian case in which a television reality program centred on emergency services recorded video and audio of the victims of a car accident, both at the scene of the accident and in a rescue helicopter while they were being transported to a hospital, without the consent of the victims.[172] The victims' claims for intrusion upon seclusion and giving publicity to private facts were dismissed by the trial judge on the basis that the program producers' activities were protected under the First Amendment. This was reversed in part by both the Court of Appeal and the California Supreme Court. It was held that while the accident, rescue and airlift were newsworthy events of legitimate public concern and therefore protected by the First Amendment, the victims still had a reasonable expectation of privacy in relation to their conversations with the treating nurse and other rescue workers at the scene of the accident and in the helicopter. In other words, a distinction could be drawn between mere information about a newsworthy event that was freely available to members of the public and the more intimate information intended only to be heard by those closely involved in the incident which could not be heard by onlookers at the scene.

3 Statutory-Based Actions

A variety of drone-specific legislation has been enacted in many states in recent years. For example, in 2017 alone 18 states passed 24 pieces of legislation,[173] including a prohibition on the use of drones to disturb or harm livestock in Utah,[174] a prohibition on the use of drones near correctional facilities in North Carolina,[175] and the creation of a number of offences in Indiana such as a prohibition on the

170 See, eg, *Hustler Magazine Inc v Falvwell*, 485 US 46 (1988).

171 See *Branzburg v Hayes*, 408 US 665 (1972). In this case the court held that the protection afforded by the First Amendment was not limited to freedom of speech or of the press but extended to a range of conduct that was related to the gathering and dissemination of information.

172 *Shulman v Group W Productions Inc*, 955 P 2d 469 (Cal 1998).

173 'Current Unmanned Aircraft State Law Landscape' *National Conference of State Legislatures* (Web Page, 10 September 2018) <http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx>.

174 Livestock Harassment, HB 217, 2017 Gen Sess (Utah 2017), enacting Utah Code Ann §76-9-308.

175 Prohibit Drone Use Over Prison/Jail, HB 128, 2017 Gen Sess (NC 2017), amending NC Gen Stat §15A-300.3.

use of drones to stalk victims by sex offenders or to obstruct or interfere with public safety officials.[176]

A small number of jurisdictions have enacted legislation that provides civil remedies for individuals who have had their privacy invaded by drones. Thus, Oregon's statute provides that 'a person who owns or lawfully occupies real property … may bring an action against any person or public body that operates an unmanned aircraft system that is flown over the property' if (a) the operator of the drone has flown it over the property on at least one previous occasion and (b) the person notified the owner or operator that they did not want the drone flown over the property.[177] The provision is therefore significantly restricted: it would not apply, for example, to isolated cases of invasion of privacy by drones, or even repeated invasion where the owner or occupier of the land does not know the identity of the drone operator and therefore cannot provide the necessary notification that they must not fly over the property. It would also provide no remedy for visitors to the property.

Other statutes are not so limited. In Idaho the statute prohibits 'a person, entity or state agency' from using a drone to conduct surveillance of a targeted person or property, or 'to photograph or otherwise record an individual, without such individual's written consent, for the purpose of publishing or otherwise publicly disseminating such photograph'.[178] An aggrieved individual may recover the greater of $1,000 or actual and general damages plus legal costs for breach of this section.[179] This provision has been criticised by the American Civil Liberties Union ('ACLU') on the ground that it may contravene the First Amendment, since it is so broad that it could prohibit 'a news station from using a drone to gather information for their traffic report absent written consent of everyone on the road' or an aerial photographer from using a drone to take pictures of the State Capitol building in case individuals were also captured in the photograph.[180]

By contrast, Texas has enacted the *Use of Unmanned Aircraft* statute[181] to address concerns regarding the use of drones to invade privacy. Section 423.002 provides a lengthy list of circumstances in which it is lawful to use a drone to capture an 'image', which is defined as 'any capturing of sound waves, thermal, infrared, ultraviolet, visible light, or other electromagnetic waves, odor, or other conditions existing on or about real property in this state or an individual on that property'.[182] The list of eclectic uses which are deemed lawful includes capturing images by drone:

176 SB 299, 120th Gen Assemb, 1st Reg Sess (Ind 2017), amending various provisions of the Ind Code.
177 Or Rev Stat § 837.380(1) (2015).
178 Idaho Code Ann § 21-213(2) (2013).
179 Ibid § 21-213(3).
180 Allie Bohm, 'The First State Laws on Drones', *American Civil Liberties Union* (Blog Post, 15 April 2013) <https://www.aclu.org/blog/national-security/first-state-laws-drones>, cited in Matiteyahu (n 8) 283.
181 *Use of Unmanned Aircraft* Tex Code Ann 423.
182 Ibid § 423.001 (2013).

- 'for the purpose of professional or scholarly research … or for another academic purpose by a person acting on behalf of an institution of higher education';[183]
- by or for an electric or natural gas utility or a telecommunications provider 'for operations and maintenance of utility or telecommunications facilities' or by 'the owner or operator of an oil, gas, water, or other pipeline for the purpose of inspecting, maintaining, or repairing pipelines or other related facilities';[184]
- 'with the consent of the individual who owns or lawfully occupies the real property captured in the image';[185]
- 'at the scene of a spill, or a suspected spill, of hazardous materials';[186]
- by 'a Texas licensed real estate broker in connection with the marketing, sale, or financing of real property', by a 'registered professional land surveyor in connection with the practice of professional surveying' or by a licensed professional engineer in connection with the practice of engineering, provided in any of these cases that no individual is identifiable in the image;[187] and
- 'from a height no more than eight feet above ground level in a public place, if the image was captured without using any … means to amplify the image beyond normal human perception'.[188]

Like the Idaho statute, under section 423.003 it is unlawful to either capture an image using a drone if the images of an individual or privately-owned property 'with the intent to conduct surveillance on the individual or property'. Capturing an image using a drone in violation of the statute is a Class C misdemeanour punishable by a fine of up to $500 and may give rise to a civil action which may allow the aggrieved person to obtain an injunction or a civil penalty of $5000 for all images captured in a single violation.[189] Possessing such an image is also a Class C misdemeanour which may result in a fine of up to $500 whilst use or disclosure of such an image is a Class B misdemeanour which may result in up to 180 days in jail and up to a $2000 fine.[190] It is a defence to these offences if the defendant destroys the image as soon as [they have] knowledge that the image was captured in contravention of the statute and the image was not disclosed, displayed or distributed to a third party.[191] Use or disclosure may also entitle the aggrieved party to an injunction, a civil penalty of up to $10,000 and/or actual damages if the person who captured the image distributes the image with malice.[192] Texas also

183 Ibid § 423.002(a)(1) (2017).
184 Ibid §§ 423.002(a)(5)(A), (16) (2017).
185 Ibid § 423.002(a)(6) (2017).
186 Ibid § 423.002(a)(10) (2017).
187 Ibid §§ 423.002 (a)(13), (19), (20) (2017).
188 Ibid § 423.002(a)(14) (2017).
189 Ibid §§ 423.003, 423.006(a) (2013).
190 Ibid § 423.004 (2013).
191 Ibid §§ 423.003(c), 423.004(d) (2013).
192 Ibid § 423.006 (2013).

prohibits the use of unmanned aircraft over critical infrastructure facilities, which was originally defined as including facilities such as oil refineries and electricity generating stations, but extended in 2017 to also include 'a concentrated animal feeding operation'.[193] Opponents claim that, rather than protecting critical infrastructure from potential terrorist attacks, the 2017 amendment was designed to prevent animal rights groups from taking videos by drone of the abuse of animals at such facilities.[194] Like the Oregon statute, the ACLU regards the Texan statute as being contrary to the First Amendment rights of private citizens and media outlets.[195]

4 Data Protection

The United States has no single overarching data protection statute similar to those in Australia and the United Kingdom. Instead it takes a 'sectoral' approach,[196] involving a patchwork of sometimes overlapping, sometimes contradictory federal and state legislation that govern different specific areas, such as medical information,[197] financial information,[198] credit information[199] and so on, as well as self-regulation.

The Presidential Memorandum directed federal government agencies to examine their policies and to implement a range of guidelines concerning drones. For example, agencies are only to collect information 'to the extent that such collection or use is consistent with and relevant to an authorized purpose'.[200] Further, if information collected using drones contains 'personally identifiable information' (which is defined as 'information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual')[201] the information is

> not to be retained for more than 180 days unless the retention is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the [*Privacy Act of 1974*, 5 USC § 552a (2014)] or is required to be retained for a longer period by any other applicable law or regulation.[202]

193 Ibid § 423.0045(1)(A)(xiii) (2017).

194 Tiffany Dowell, 'Overview of Amendments to Use of Unmanned Aircraft Statute', *Texas Agriculture Law Blog* (Blog Post, 25 July 2017) <https://agrilife.org/texasaglaw/2017/07/25/texas-legislature-adds-protections-cafos-drone-bill/>.

195 Matiteyahu (n 8) 284.

196 Shawn Boyne, 'Data Protection in the United States: US National Report' (Research Paper No 2017-11, Robert H McKinney School of Law, Indiana University, 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089004>.

197 *Health Insurance Portability and Accountability Act of 1996*, Pub L 104-191, 110 Stat 1936 (1996) ('*HIPAA*'). See 42 USC § 1301 ff.

198 *Financial Services Modernization Act of 1999*, Pub L 106-102, 113 Stat 1338 (1999) ('*Gramm-Leach-Bliley Act*'). See 15 USC §§ 6801-27.

199 *Fair Credit Reporting Act*, 15 USC § 1681 (1970).

200 The White House, Office of the Press Secretary (n 151) § 1(a)(i).

201 Ibid § 3(e).

202 Ibid § 1(a)(ii).

V COMPLEX RESPONSES TO A COMPLEX PROBLEM

Similarities are emerging in the regulatory approaches to drones in Australia, the United Kingdom and the United States. For example, all three countries currently require drones to be operated within visual line of sight and not over human beings[203] and impose restrictions on flying near airports and other sensitive areas. Also, registration of drones exceeding 250 g has been implemented in the United States, and will shortly be introduced in the United Kingdom and Australia. The focus of regulation in all three countries is principally for the purpose of safety – even though both CASA in Australia and the FAA in the United States have acknowledged the potential for drones to be used to invade privacy – whilst only the United Kingdom presently acknowledges the opportunity provided by registration to provide a measure of protection of privacy through education.

In whatever country they are flown, drones pose the same challenges in terms of potential invasions of privacy, including intrusion upon the seclusion of individuals, enabling the disclosure of private facts obtained in the course of intrusion, issues involving surveillance and voyeurism and the collection, use and disclosure of personal data. In these respects there are differences in the responses to these challenges. These differences are the product of a number of influences, such as constitutional contexts, legislative priorities and the relative development of the common law.

Data protection laws are a point of distinction. Without the constitutional limitations of either Australia or the United States, the data protection laws in the United Kingdom apply equally to all drones whether operated by government agencies, or for commercial or recreational purposes, although there is a wide exemption for journalism. By contrast, data protection laws in Australia only apply to drones operated by Commonwealth agencies and state agencies other than in Western Australia and some commercial organisations with the requisite annual turnover, but not those operated for recreational purposes. In the absence of such laws of general application in the United States, data protection by federal agencies follows the drone-specific Presidential Memorandum signed by President Obama and any specific drone-specific legislation enacted at a state level.

The common law in the United States recognises specific causes of action that provide reparation in cases of unreasonable intrusion on seclusion and disclosure of private facts although such a claim may be trumped in some cases by the drone operator's First Amendment rights to free speech and a free press. Similarly, the common law in the United Kingdom provides protection against the misuse of private facts that may also be obtained as a result of an intrusion balanced against the right to free expression, although a civil remedy may be obtained if the

203 Although, in the United States waivers may be granted in appropriate circumstances. For example, in December 2018 the FAA granted its first three-prong waiver for 'flying Beyond Visual Line of Sight (BVLOS) for automated drone operations, over human beings, with a visual observer that is not required to keep a visual line of sight on the drone'. The operator obtained the waiver for automated drones servicing mining operations by companies such as BHP in Arizona: Jason Reagan, 'Airobotics Receives Unique FAA Waiver for Arizona Drone Flights', *Dronelife* (News Post, 15 December 2018) <https://dronelife.com/2018/12/15/airobotics-receives-unique-faa-waiver-for-arizona-drone-flights>.

circumstances fall within the ambit of section 3 of the *Protection of Harassment Act 1997* (UK). By contrast, aggrieved individuals in Australia have limited opportunities to obtain a remedy: in the absence of a dedicated tort protecting privacy, any claim would need to fall within the ambit of existing causes of action such as trespass to land, private nuisance and/or breach of confidence, each of which has its own limitations. In some cases an invasion of privacy by drone may contravene Australian surveillance laws but these are inconsistent: at the time of writing only five jurisdictions have laws that would apply to drone-mounted cameras, with Queensland likely to follow suit. The New South Wales statute is property-based, whilst those in Western Australia, Victoria and the Northern Territory are activity-based and the South Australian statute is a hybrid, containing both property-based and activity-based prohibitions, although the drone context demonstrates that privacy interests may be sufficiently protected by an activity-based prohibition, making a property-based prohibition unnecessary. Further, the activity-based statutes differ in relation to the activities they cover. Moreover, these statutes, like other legislation prohibiting voyeurism and stalking, only provide for criminal offences and make no provision for civil remedies.

The shortcomings of existing laws protecting privacy in Australia have been recognised by five separate Law Reform Commission inquiries – two by the Australian Law Reform Commission ('ALRC')[204] and one each by the New South Wales Law Reform Commission ('NSWLRC'),[205] the Victorian Law Reform Commission[206] and the South Australian Law Reform Institute[207] – all of which have recommended enactment of a statutory cause of action protecting personal privacy. Whilst there were differences in the exact formulations of such a cause of action, in essence each suggested a claim should be available where there is either an intrusion or disclosure in circumstances where there was a reasonable expectation of privacy, with the public interest as either a defence[208] or as a factor relevant to the expectation of privacy.[209] To date no government has enacted any of these recommendations. The issue has a political dimension that should be acknowledged. The Rudd-Gillard Federal Labor Government responded to the recommendations of the 2008 ALRC inquiry in two stages: the first stage included enactment of the APPs while the second stage, which was in response to the recommendation of a statutory cause of action protecting personal privacy, was to establish the second ALRC inquiry in order to specifically consider the matter. However, by the time the 2014 ALRC inquiry made its recommendations the Abbott Coalition Government had been elected. Attorney-General Senator Brandis

204 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, 12 August 2008) ('*For Your Information*'); Australian Law Reform Commission, *Serious Invasions of Privacy in a Digital Era* (Report No 123, 3 September 2014) ('*Serious Invasions of Privacy*').

205 New South Wales Law Reform Commission, *Invasion of Privacy* (Report No 120, April 2009).

206 Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report No 18, 1 June 2010).

207 South Australian Law Reform Institute, *A Statutory Tort for Invasion of Privacy* (Final Report No 4, March 2016).

208 See *For Your Information* (n 204); *Surveillance in Public Places* (n 206).

209 See *Serious Invasions of Privacy* (n 204); *Surveillance in Public Places* (n 206); *A Statutory Tort for Invasion of Privacy* (n 207).

responded to the recommendation of a statutory tort protecting against serious invasions of personal privacy by simply stating: 'The government has made it clear on numerous occasions that it does not support a tort of privacy'.[210] Indeed, there was no subsequent formal response to the recommendations.

By contrast, when tasked with considering the privacy implications of drones, the bipartisan 2014 House of Representatives Standing Committee on Social Policy and Legal Affairs chaired by George Christensen MP inter alia recommended an enactment of a statutory cause of action as envisaged by the 2014 ALRC report and that the Committee of Attorneys-General initiate action to harmonise state and territory surveillance laws.[211] However, the Turnbull Coalition Federal Government rejected the recommendation for a statutory cause of action protecting privacy on the ground that

> [i]ntroducing a new cause of action would only add to the regulatory burden on business, which is contrary to the government's commitment to reducing red tape. The common law already provides avenues for individuals to seek redress for the torts of trespass, nuisance, defamation and breach of confidence. The states and territories also have their own legislation.[212]

The Government noted the recommendation that surveillance laws be harmonised through the auspices of the Council of Australian Governments ('COAG') but stated that it was for states and territories to amend their laws as appropriate.[213] The later Senate inquiry into drones merely made reference to the 'lack of national consistency with regard to state and federal privacy and surveillance legislation, coupled with the growth of local council by-laws relating to RPAS operations' which it described as making 'compliance for RPAS operators extremely challenging'[214] and recommended that as part of a whole-of-government policy approach to RPAS 'harmonisation of state and territory privacy laws should also be considered'.[215] Again the Government noted the Committee's harmonisation recommendation that the harmonisation of state and territory privacy laws 'should also be considered', reiterated that harmonisation was a matter for state and territory governments, but indicated that the Commonwealth would engage with those governments to consider national harmonisation of privacy laws as they apply to RPAs.[216]

---

210 Chris Merritt, 'Brandis Rejects Privacy Tort Call', *The Australian* (online, 4 April 2014) <http://www.theaustralian.com.au/business/legal-affairs/brandis-rejects-privacy-tort-call/story-e6frg97x-1226873913819>.

211 House of Representatives Standing Committee on Social Policy and Legal Affairs Inquiry, Parliament of Australia, *Eyes in the Sky: Inquiry into Drones and the Regulation of Air Safety and Privacy* (Report, July 2014) 47–8 [4.65] (Recommendations 3 and 4).

212 Australian Government, *Australian Government Response to the Standing Committee on Social Policy and Legal Affairs Report – Eyes in the Sky: Inquiry into Drones and the Regulation of Air Safety and Privacy* (Report, December 2016) 8. The Government also noted that in cases where the *Privacy Act 1988* (Cth) applied, aggrieved individuals could complain to the Office of the Australian Information Commissioner: at 8.

213 Ibid 9.

214 *Safe Commercial and Recreational Use Report* (n 25) 99.

215 Ibid 109 [8.45].

216 *Response to Safe Commercial and Recreational Use Report* (n 27) 10.

In New South Wales a bipartisan parliamentary committee which considered the recommendations of the NSWLRC Inquiry cited invasions of privacy by drones as one of the reasons why that State should take a leadership role and enact a statutory cause of action, since '[w]e would be ignoring the reality of the matter if we did not accept the view that this is an area of intrusion into privacy that is likely to become more topical and more widespread in coming years'.[217]

Subsequently a private member's Bill (on behalf of the Labor Opposition) was introduced into the New South Wales Legislative Assembly,[218] but ultimately lapsed. A second private member's Bill was introduced into the New South Wales Legislative Council in April 2017,[219] but to date no further action has been taken.

As Michael Kirby has observed:

> [The response of the New South Wales government], and many before, show the power of media interests in Australia to fight off law reform in the area of privacy protection. Major media outlets in Australia are controlled by relatively few interests. They generally prefer to be left alone to act as investigator, prosecutor, jury and sentencing judge, with no right of reply or appeal. Unfortunately, the political branches of government back away from a fight with the media. The abuses of privacy, including information privacy, in Australia are many. Nevertheless, the prospects of effective statutory remedies in the foreseeable future appear to be small.[220]

He continued:

> This conclusion should be remembered the next time politicians deny the necessity of any form of charter or statute of rights in Australia as inessential in a jurisdiction where parliament 'will always respond' to specific needs. The near total failure of (all) the Australian Parliaments to respond to the demonstrated need for the protection of privacy, through appropriate and adapted legislation, is a disappointing story. It tells of the failure of law reform, the timidity of legislators, the formalism of courts and the failure of the law reform process. Something old continues to be something current in Australia. The law has failed to develop a general and enforceable civil wrong for serious and unjustifiable invasions of privacy. It has left individuals unprotected by enforceable law. To be blunt, the law reform process has repeatedly failed.[221]

It is worth noting that the 2014 ALRC report also recommended that, failing enactment of a statutory cause of action protecting personal privacy, the Commonwealth should enact surveillance devices legislation to replace existing state and territory legislation, or alternatively that the states or territories enact uniform surveillance devices laws, which include, inter alia, a defence for responsible journalism rather than a broad public interest defence.[222] The ALRC thought that such legislation should be technology neutral in its terms, thereby being able to apply to a broad range of existing and emerging technology,

217 Legislative Council Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the Serious Invasion of Privacy in New South Wales* (Report No 57, 3 March 2016) 27 [2.47].

218 Civil Remedies for Serious Invasions of Privacy Bill 2016 (NSW).

219 Civil Remedies for Serious Invasions of Privacy Bill 2017 (NSW).

220 Michael Kirby, 'Privacy Today: Something Old, Something New, Something Borrowed, Something Blue' (2017) 25(1) *Journal of Law, Information & Science* 1, 17.

221 Ibid 17–18.

222 *Serious Invasions of Privacy* (n 204) 275–85 [14.1]–[14.42] (Recommendations 14-1, 14-2), 289–93 [14.58]–[14.76] (Recommendation 14-5).

expressly referencing drones as an example.[223] Such legislation would therefore be in contrast to drone-specific privacy laws like those in Texas. The ALRC also recommended that these laws should provide for not only criminal offences but also allow courts to order remedial relief to victims of unlawful surveillance.[224]

However, it should be recognised that, in the absence of fortuitous circumstances enabling the identification of the operator of the drone, such as the victim of an invasion of privacy witnessing the drone being flown by a neighbour or some other known person, such laws may have little meaning without additional measures to enable law enforcement and/or the victim to identify the operator of the drone. It is a salient warning that in the case of the Darwin skinny-dipper, the drone may have been in breach of the current Northern Territory surveillance laws but the identity of the operator was unknown. Even if Australia implemented a system of registration like that currently employed in the United States, which requires the owner to affix the relevant registration number on the outside of the drone in order to link the drone to its owner, this may be of little use to a victim who cannot see that registration number from their vantage point on the ground far from the drone. One novel suggestion has been to enable the use of radio frequency identification as a means of allowing victims to identify drones flying within a certain range of them by means of an app on their mobile phones.[225] More promising may be measures such as the electronic identification and real time tracking of drones, similar to those to be implemented in the United States and elsewhere.[226] However, there ought to be provision for such information to be accessed not only by relevant authorities for the purposes of law enforcement, but also the party who may have a greater interest in redressing the wrong: the individual who has had their dignity or autonomy affronted by the invasion of their privacy.[227]

---

223 Ibid 283–4 [14.34].

224 Ibid 295–6 [14.85]–[14.89] (Recommendation 14-7).

225 Steve Ragatzki, 'Filling in the Gaps in FAA Drone Regulations: A Proposed Dual-Zone Model of Personal Privacy' (2017) 25(1) *Michigan State International Law Review* 193, 223–9.

226 The FAA views remote identification and real time tracking as reasonable requirements and indeed critical steps in the integration of drones since '[t]he national airspace system is no place for hide and seek': Miriam McNabb, 'InterDrone Gets Started with Dan Elwell: FAA Is "Open for Business" on Drones', *Dronelife* (News Post, 5 September 2018) <https://dronelife.com/2018/09/05/interdrone-gets-started-dan-elwell-faa-is-open-for-business-on-drones/>. Cf a similar proposal in, for example, France: see Marco Margaritoff, 'Proposed French Drone Regulation Would Require Remote Identification', *The Drive* (News Post, 12 April 2018) <http://www.thedrive.com/tech/20063/proposed-french-drone-regulation-would-require-remote-identification>.

227 Butler, 'The Dawn of the Age of the Drones' (n 4) 469. It may be that such information might be able to be obtained by an aggrieved victim through pre-trial discovery under the Rules of Court, which enable an applicant to obtain discovery of the identity of a wrongdoer from a third party so that legal action may be commenced against them: see *Court Procedures Rules 2006* (ACT) r 650; *Uniform Civil Procedure Rules 2005* (NSW) r 5.2; *Supreme Court Rules 1987* (NT) r 32.03; *Supreme Court Civil Rules 2006* (SA) r 32; *Supreme Court Rules 2000* (Tas) r 403C; *Supreme Court of Victoria (General Civil Procedure) Rules 2005* (Vic) r 32.03; *Rules of the Supreme Court 1971* (WA) ord 26A r 3. In Queensland, in the absence of specific rules in the Uniform Practice Rules allowing pre-trial discovery, it might be possible to take steps such as seeking a so-called *Norwich Pharmacal* order (see *Norwich Pharmacal Co v Customs and Exercise Commissioners* [1974] AC 133) or an order for interrogatories under the *Uniform Civil Procedure Rules 1999* (Qld) r 229 in order to obtain information that can identify the wrongdoer from someone who might know.

VI CONCLUSION

Drones are a transformative technology that offer great economic and social benefits. But for all their potential, drones also pose a unique challenge to privacy: now not even a high-rise apartment, let alone a high fence, pose insuperable barriers to prying eyes. It is a challenge that enlivens diverse forms of privacy laws: those provided by the common law and/or statutes, either specifically or incidentally, and in some cases data protection laws. However, an examination of three major common law countries in the form of Australia, the United Kingdom and the United States shows the current responses of the law to the challenge posed by drones to be significantly disparate, even if the regulatory regimes may increasingly show signs of similarity.

It has been said that drones 'could be just the visceral jolt society needs to drag privacy law into the twenty-first century'.[228] Indeed the Queensland government, as part of the *Queensland Drone Strategy* that 'builds on Queensland's existing strengths and leverages our innovation success to take advantage of new and emerging opportunities', acknowledged that '[p]rivacy has been recognised nationally and internationally as a key challenge posed by the proliferation of drones and other new and emerging technology with surveillance capability'.[229] The strategy therefore signalled that the question of whether Queensland's existing legislation adequately protects privacy in the context of modern and emerging technologies would be referred to the Queensland Law Reform Commission. Drones would therefore seem to have provided the 'jolt' for Queensland to consider replacing its antiquated *Invasion of Privacy Act 1971* (Qld) with surveillance laws more appropriate to modern society. It would be hoped that such reforms will see the enactment of technology-neutral activity-based prohibitions, free from the arbitrary limitations of the definition of 'private activity' under the Victorian and South Australian surveillance legislation, together with provisions enabling aggrieved victims to obtain civil relief in a cost-effective fashion. It would also be hoped that in the near future such laws around Australia may be harmonised: in the absence of a statutory based cause of action protecting personal privacy as recommended by the 2014 ALRC report, or those recommended by similar Commissions in New South Wales, Victoria and South Australia, it may be a second-best option to addressing the challenges posed by drones. Moreover, Australia would do well to combine registration of drones, particularly those used for recreational purposes, with education not only in relation to safety but also privacy issues, together with a means of real time tracking of drones. Alerted to the potential consequences of their actions, both criminal and civil, and realising that they may be easily identified, operators of drones may be deterred from intentionally invading the privacy of others in the first place.

228 M Ryan Calo, 'The Drone as Privacy Catalyst' (2011) 64 *Stanford Law Review Online* 29, 29.

229 Queensland Government, *Queensland Drones Strategy* (Report, June 2018) 31 <https://www.premiers.qld.gov.au/publications/categories/plans/assets/qld-drones-strategy-2018.pdf>.