Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

# The regulation of civilian drones' impacts on behavioural privacy

Roger Clarke [a,b,c,*]

[a] Xamax Consultancy Pty Ltd, Canberra, Australia
[b] Australian National University, Canberra, Australia
[c] University of N.S.W., Sydney, Australia

*Keywords:*
RPA
RPAS
UAV
UAVS
Visual surveillance
Behavioural privacy
Experiential privacy

ABSTRACT

Surveillance technologies have burgeoned during the last several decades. To surveillance's promises and threats, drones add a new dimension, both figuratively and literally. An assessment of the impacts of drones on behavioural privacy identifies a set of specific threats that are created or exacerbated. Natural controls, organisational and industry self-regulation, co-regulation and formal laws are reviewed, both general and specific to various forms of surveillance. Serious shortfalls in the regulatory framework are identified. Remedies are suggested, together with means whereby they may come into being.



## 1. Introduction

This is the last in a series of four papers that together identify the disbenefits and risks arising from the use of drones, and consider the extent to which they are subject to suitable controls. The first paper provided background on the nature of drones. The second reviewed existing, critical literatures, in order to ensure that the accumulated understanding of relevant technologies is brought to bear on the assessment of drone technologies as well. The third examined regulatory frameworks relating to public safety, and showed them to be far from satisfactory, particularly in regard to the smaller categories of drones.

Surveillance applications of drones include environmental monitoring, tracking of livestock and wildlife, measurement of meteorological and geophysical phenomena, and observation of large-scale human constructions such as buildings, energy infrastructure such as electricity networks and gas and water pipelines, and road-, air- and sea-traffic. This paper, however, is concerned solely with the surveillance of people, and spaces through which people pass. It excludes consideration of the use of drones in war-zones – a topic that is already copiously addressed in the literature. Its scope is limited to civilian contexts, but up to and including para-military uses by law enforcement and national security agencies, such as border protection, observation and pursuit of criminal suspects, and the observation of civil unrest. The paper's purpose is to examine the extent to which current regulatory regimes appear to exercise controls over the use of drones to conduct such surveillance.

Most privacy discussions focus on data privacy and data protection, to the virtual exclusion of other aspects of privacy. This paper, on the other hand, has as its focus not data privacy, but behavioural privacy. It commences by considering the various dimensions of privacy, with particular emphasis on the dimension that is most directly harmed by surveillance – the privacy of personal behaviour. It then reviews the current state of play in relation to the monitoring of individuals, and identifies the ways in which drones add to the already-

* Xamax Consultancy Pty Ltd, 78 Sidaway St, Chapman, ACT 2611, Australia.
E-mail address: Roger.Clarke@xamax.com.au.
http://dx.doi.org/10.1016/j.clsr.2014.03.005

intense intrusiveness of contemporary surveillance technologies. The current regulatory arrangements are then considered. The relatively 'soft' regulatory forms are shown to have little impact. Formal laws are then reviewed, commencing with potentially relevant causes of action of longstanding, and then human rights laws, aviation laws and privacy laws, culminating in laws relating to surveillance *per se*.

## 2. Privacy

The term 'privacy' is applied to a range of human interests in having private space (Warren and Brandeis, 1890; Morison, 1973; Solove, 2006). The following sections distinguish five dimensions of privacy (Clarke, 1997, 2006), narrowing the focus down to the two most directly impacted by surveillance.

### 2.1. *Dimensions of privacy*

The dimension that is most widely discussed is privacy of personal data. As data storage has become cheaper, it has become increasingly common for data-streams to be captured, and retained, and even retained indefinitely. Drones are capable of being used to capture large volumes of data. Where that data does, or may, record actions of, or involving, identifiable individuals, personal data result. Examples include drones that monitor Wifi emanations, that carry automated number-plate recognition (ANPR) capability, and that transmit real-time video of sufficient quality to enable a human operator to visually recognise an individual and associate the recording with that person. Near-future prospects include the emergence of less error-prone 'facial recognition' technologies, tracking of devices carrying RFID-chips, including motor vehicles and anklets imposed on 'open prisoners', and tracking of chips implanted in animals, including humans.

Drone activities accordingly give rise to threats to data privacy. Issues include:

- additional collection of personal data, perhaps in very large volumes
- additional storage, retention, use and disclosure of data about individuals
- use and disclosure in contexts, and for purposes, that have little or nothing to do with the original context and purpose of collection, and which accordingly invite misinterpretations
- interception of data-flows, e.g. of surveillance video transmissions (Gorman et al., 2009)
- unauthorised access to stored data
- exploitation of the data in conjunction with other data

An area of particular public concern is the generally inadequate controls over access by law enforcement agencies to increasing volumes of data. This has been accompanied by increasing attempts to collect large volumes of data, not only for retrospective investigation, and not only once the fact of a criminal act is known or reasonable grounds for suspicion exist, but also prospectively, 'just-in-case'. An example is the abuse of ANPR by various governments, to date at its most extreme in the UK, as a means of mass surveillance of road traffic (Clarke, 2009a). Another example is Internet traffic 'data retention' regimes.

Since the 1970s, data protection laws (sometimes misleadingly referred to as though they were comprehensive privacy laws) have been enacted in most countries (EPIC, 2006; Greenleaf, 2013, 2014). Moderate protections exist in Europe, and various, generally weak protections exist in other countries. The inadequacies of data protection laws have been highlighted by the exploitation of personal data by social media service-providers, and by spy agencies. The emergence of drone-based surveillance adds to an already-burning fire. The impact of drones on data privacy was the focus of a previous article in Computer Law & Security Review (Finn and Wright, 2012).

A close cousin to data privacy is privacy of personal communications, which relates to ephemeral transmissions rather than data that is of necessity stored. In most countries, this is also subject to at least some degree of legal protection.

A third dimension, privacy of the physical person, is concerned with the integrity of the individual's body. Drones may impinge on this interest to the extent that they are used to collect data such as facial images, other physical measures of the individual – commonly referred to as biometrics – and emanations from implants. Where such data is adequate to distinguish the particular physical person from all other human beings, the term 'entifier' is usefully applied to it (Clarke, 2009b). However, it is two further dimensions of privacy that are the primary concerns in this paper, because they encompass the interests that are most directly impinged upon by drone-based surveillance.

### 2.2. *Behavioural privacy*

The privacy of personal behaviour is concerned with freedom of the individual to behave as they wish, without undue observation and interference from others. The term 'behaviour' in this context encompasses the individual's activities, movements, associations and preferences. Like any other privacy interest, this is subject to a wide range of conflicts with other interests of the individual, and with interests of other individuals, groups, and society as a whole. Privacy protection is always an exercise in balance.

Overt surveillance stifles behaviours, including (and desirably) illegal behaviours, but also behaviours that are discouraged by organisations with institutional or market power. Covert surveillance, on the other hand, gives rise to the 'panoptic' effect: individuals fear that they may be subject to observation at any time, and that many behaviours might be construed by the powerful to be undesirable. This results in a form of 'self-discipline' – a 'chilling effect' on a wide range of behaviours, and the stultification of freedoms of expression and of innovation (Gandy, 1993, but the literature on 'the panoptic effect' goes back to Bentham, 1791, and has multiplied since Foucault, 1975).

The interest in behavioural privacy encompasses all aspects of human behaviour, but some aspects are particularly sensitive, such as sexual activities, religious practices and political activities. The focus is commonly on psychological needs for 'seclusion' (Warren and Brandeis, 1890; Solove, 2006). However, societies and economies depend on innovative behaviour, which tends to be stifled by observation. Similarly, a healthy

polity depends on effective protections for the privacy of personal behaviour, because democratic freedoms are undermined by the chilling of political speech (Clarke, 2008b).

The need of individuals for seclusion encompasses behaviour in private places, but also in public places where reasonable expectation exists of private space. For example, a person in a quiet corner of a public park, or amidst a large and noisy audience at a sport or entertainment event, might well be included in a general photo of the park or in a 'crowd shot' at the venue; whereas they reasonably have a strong expectation that they will not be targeted with a zoom lens or a directional microphone. Even in the case of 'celebrities', 'notorieties' and others 'in the public eye', their status does not imply that their every movement and utterance in public places is fair game for any voyeur that can train their lens or microphone on them, whether for personal enjoyment, for exposure to others, or for commercial publication.

Technological development continually expands the capacity of other parties to invade personal space. There is a strong tendency among government agencies and corporations to invoke technological determinism ('if you can do it, you should do it'), and argue that the legitimate expectation of private space has been destroyed by new capabilities. Such arguments may superficially serve the interests of organisations, but they are hostile to human beings. The underlying human need for private space is far too important to be sacrificed to administrative convenience. Technological capability is not a relevant criterion when determining the reasonableness of the expectation of private space. This is evident in public demands for, and implementation of, 'pixellation' of facial images that are incidentally gathered in such contexts as streetscapes, and that are incidentally published in such contexts as CCTV footage of criminal acts.

Until recently, the four dimensions of privacy discussed above had provided a sufficient basis for analysis. However, the 21st century has brought technological change that is resulting in comprehensive monitoring of what people view (e.g. YouTube and subscription video), listen to (e.g. Apple iTunes), read (through the licensing of electronic copies rather than the sale of hard copies), look up in reference works (on the Web rather than in hard copies in personal collections and libraries), who they interact with (through 'call' records for telephony and 'metadata' for electronic communications such as email and chat traffic), and who they consort with physically (through geolocation of mobile devices). It is therefore now necessary to distinguish a fifth dimension – 'privacy of personal experience'. Surveillance using drones may come to make contributions to the monitoring of the experiences that a person accumulates, and that influence their attitudes and opinions. This falls short of surveillance of beliefs and thoughts, but it comes much closer than has previously been feasible.

To what extent are behavioural and experiential privacy affected by surveillance and to what extent will that impact be increased through the use of drones for surveillance?

## 3. Surveillance

This section commences by identifying key features of the surveillance of individuals, as it is currently practised. It then draws on earlier papers in the series in order to identify specific ways in which the application of drones to surveillance creates new issues or exacerbates existing problems.

### 3.1. *Contemporary surveillance*

Surveillance is systematic monitoring or investigation of some target. By monitoring is meant contemporaneous observation, whereas investigation refers to the retrospective study of recordings. There is a substantial literature on surveillance, but a considerable proportion of it is technical and highly specific, or sociological in nature or heavily intellectualised and lacking in analytical clarity.

A surveillance target may be an area, or one or more objects, including people (Wigan and Clarke, 2006). Personal surveillance is concerned with an identified person of interest, whereas mass surveillance is of an area or a group of people, in order to influence behaviour, or to detect particular behaviour and identify individuals of interest (Clarke, 1988).

Surveillance takes a variety of forms (Clarke, 2010). Physical surveillance includes aural and visual monitoring, but may also extend to sound beyond the human auditory range and to other parts of the electromagnetic spectrum, such as infra-red emanations. Physical surveillance has been becoming increasingly intrusive, to the extent that a category of body surveillance now needs to be recognised, involving monitoring of aspects of the person's physical self (Masters and Michael, 2007). Communications surveillance focusses on intercepting written communications, listening to conversations, and access to various kinds of electronic messaging. Dataveillance observes transactions and exploits stored data (Clarke, 1988).

The combination of physical surveillance with data surveillance enables the location of individuals. The acquisition of a succession of locations for a person constitutes tracking. By these means, inferences can be drawn about the individual's behaviour, and even about their intentions, enabling interventions with their activities. Since the late twentieth century, tracking has become so intrusive and pervasive that it requires treatment in its own right (Clarke, 1999; Wright et al. 2010; Clarke and Wigan, 2011; Michael and Clarke, 2013).

Society exhibits considerable differences in institutional and market power among organisations, and between organisations and individuals. The term surveillance was coined in France in the late eighteenth century to reflect the superior position of an organisation that has some kind of authority over individuals – 'sur' = 'above'. It has been commonly associated with the physical superiority of guards in watchtowers over individuals in institutions. As the forms of surveillance have proliferated, the notion of superiority has been applied in a metaphorical sense. Drones actually bring back the sense of physical superiority of the observation-point over ground-dwelling individuals.

Recent, substantial reductions in the costs of apparatus used to conduct monitoring have led to a degree of democratisation of observation and recording. The term 'sousveillance' – utilising the French word 'sous' = 'beneath' – was coined to describe the use of veillance techniques and technologies by the less powerful, usually individuals, against the more powerful, usually organisations (Mann et al., 2003;

Mann, 2005, 2009). The search for a suitable degree of balance between the two has been characterised as 'equiveillance' (Mann et al., 2006).

Visual surveillance of people is invasive of behavioural and possibly also experiential privacy. The nature of surveillance abuses and excesses, and of their impacts, depends to a considerable extent on the motivation underlying the activity. At least the following categories of institutions and motivations need to be distinguished:

- formal law enforcement
- informal law enforcement (vigilantes, 'neighbourhood watch')
- journalism, as performed by the professional investigative media, focused on 'the public interest'
- informal journalism and investigation, particularly for environmental and social purposes
- voyeurnalism, by 'tabloid media', focused on 'what the public is interested in' (Clarke, 2012c)
- voyeurism for personal pleasure
- self-entertainment and hobbyist activities

Visual surveillance technologies have become highly sophisticated. They include such forms as closed-circuit television (CCTV), automated number-plate recognition (ANPR), in-car video (ICV), and the wearcams that have enabled point of view surveillance (POVS) for two decades (Mann, 1994, 1997), and that are now being industrialised by various latecomers to the market such as Google Glass. Visual surveillance capabilities that are relevant in the new context of drones include the following:

- acquisition of images or video (possibly with synchronised audio)
- transmission of images or video (possibly with audio) to a remote location
- recording/archival of images or video (possibly with audio)
- fixed cameras with known positions and orientations
- mobile cameras with measured or computed positions and orientations
- cameras embodied in other artefacts such as a baton, a pistol, a mobile-phone
- triggering of transmission and/or recording by conscious human act, or automatically
- enhancement of line-of-sight vision with data, e.g. messages, GPS coordinates
- augmentation of line-of-sight vision with computed visual overlays, e.g. colouration, contours
- alternative or supplementary displays, e.g. infra-red image/'night-goggles'
- display of streams from multiple cameras
- action-replays, triggered in various ways

### 3.2. *The differences that drones make*

Much of the early use of drones has been for the purpose of visual surveillance. For example, virtually every one of the UAV operating certificates issued in Australia to date has been for this category of application (CASA, 2014). Some surveillance is simply observation, but much of it results in transmission, and in recording of image or video, mostly in the human-visible spectrum, but in some cases in the infra-red. Drones can also gather structured data such as vehicle registration numbers using Optical Character Recognition (OCR) and ANPR techniques. They can be applied to the gathering of other forms of signal as well, e.g. as a means of intercepting electronic messaging services. They can be readily applied to assist with location and tracking (e.g. by detecting identified transponders and hence the objects that the transponders are associated with, or by following infra-red signatures). They could, at least in principle, gather measurements from individuals' implants. Drones are therefore potentially valuable elements within all surveillance forms. The primary focus in this article is, however, on the use of drones to support visual surveillance.

Surveillance embodies a wide variety of threats to behavioural privacy. This article reflects existing surveillance threats, and regulatory responses to them, with attention paid primarily to the following additional and enhanced threats that arise from the application of drones to surveillance:

(1) Extensiveness

Low costs and ready accessibility, combined with strong incentives (including profit, the drive to compete, and voyeurism), result in more extensive monitoring of individuals, in the sense of observation in more places, more recording, and more publication. This is akin to harassment.

(2) Intensity

Individuals are subjected to scrutiny for longer periods, more closely, and in high-resolution. Observation that is frequent, continual and even continuous is deeply intrusive into personal space, and is akin to stalking. Further, rather than the scrutiny being limited to observation, images are likely to be retained and stored, and later re-discovered and re-cycled.

(3) 'Paparazzi aloft'

Drones enable barriers in the line of sight to be overcome, and imagery to be captured that would not be available if the camera were terrestrially-bound. Vertical and angled shots can be achieved, as can stereo and 3-D. Continuous monitoring can be undertaken of bottleneck locations, such as the target's front door, and exit-points from airports, possibly including auto-triggering. Tracking becomes much easier. As pursuits become more feasible, they will create the risk of stimulating avoidance manoeuvres that may be frantic and ill-judged. Beyond 'professional' paparazzi, these capabilities have become available to any voyeurist.

(4) 'The Panoptic aloft'

- Law enforcement agencies may apply military technologies, and may do so in ways not attuned to human rights
- Law enforcement agencies may gain authorisation incidentally, as an unforeseen consequence of existing legislation and policies. Insufficiently-controlled

police surveillance, including warrantless search and self-issued 'warrants', are a concern in many countries, and have been a focal point of much debate within the USA
- The potential retributional value of surveillance is entirely dependent on the availability and application of resources, sufficiently close to the relevant incident in both time and space, to identify, locate and bring to justice the perpetrators of each crime and misdemeanour
- Observation has a deterrent effect, but the deterrent value of surveillance may be very limited in relation to serious forms of misbehaviour, because:
  - habitual criminals, despite law enforcement agency monitoring, do what they do
  - organised crime regards countermeasures as 'a cost of doing business'
  - most crimes of violence are performed with little regard for the consequences
  - dangerous and anti-social behaviour by people in party mode happens anyway

  As a result, the deterrent effect on illegal behaviour is likely to be far less than the chilling effect on lawful social, economic, cultural and political behaviours
- Law enforcement agencies are able to pay more attention to petty crimes that were previously regulated informally: 'Nobody gets away with anything', 'forgiveness and forgetfulness become conveniences of the past' (Bear, 2010). See also Cullen and Gilbert (2013)
- Drones make it practicable and economic for vigilantes to mount an airborne form of 'neighbourhood watch', possibly on an intensive and extensive basis
- Drones may enable practicable and economic implementation of 'mobile nagging aunties', to detect activity and play recorded messages or transmit real-time voice. These may be operated by law enforcement agencies, but also by moral minorities within communities

(5) Errors

Much surveillance is conducted from a single perspective and with limited context, resulting in inferences that may be apparently reasonable, but are actually at least misconceived, and even simply wrong. Many cases of mistaken identity arise, fuelling rumours and innuendo. Refutation of unjustified accusations is very challenging, in the court of public opinion, and even in courts of law.

(6) Spurious authority

Image and video, particularly when recorded from above the object being observed, and especially when presented by government agencies, is invested with importance that it may or may not merit.

(7) Reduced natural controls

As discussed in the third paper in the context of public safety, drone pilots and operators of onboard facilities are remote from their target, and operate in the virtual reality created by their data-feeds. Their detachment from the physical reality of the individual in their sights tends to weaken the constraints of conscience, and loosens at least some of the psychological and social controls that apply 'in meatspace'. This gives rise to a risk of operators engaging in voyeurism, harassment, stalking, and even acts of gratuitous violence.

(8) Surreptitiousness

In some cases, drone surveillance is very apparent, due to engine-noise, drone-size and/or drone-movement. However, some drones are designed for covert use, and many circumstances may arise in which individuals are unaware that their behaviour is being observed and recorded, are unaware that records have come into existence, and/or are unaware of the basis on which judgements are made about them and their behaviour.

(9) Discrimination

Surveillance drone capabilities are likely to be applied, by organisations and individuals alike, to 'the usual suspects' and 'undesirables', such as sex offenders, 'gypsies', minority groups and adolescents. This further increases social alienation and distrust, and undermines social cohesion (Finn and Wright, 2012).

(10) Paranoia

The combination of automated monitoring, increasingly extensive monitoring approaching pervasiveness, and increasingly intensive monitoring approaching continuousness, creates the prospect that the sentiment 'they know all about you anyway' will become at least more credible, and perhaps even true. Among persons-at-risk, this is likely to result in hyper-vigilance. Among individuals who are prone to paranoia – in both its delusional and justified forms – the occurrence and intensity of psychological disturbance can be expected to increase.

### 3.3. *Conclusions*

The emergence of surveillance society (Lyon, 1994) has already stimulated considerable public concern. Negative impacts arise at the psychological level on individuals, at the social level on groups and societies, at the economic level on innovators, and at the political level on democracies. Drones exacerbate these concerns. It is very important that new balances be sought, in the new and rapidly evolving contexts in which highly-invasive surveillance technologies are imposed.

## 4. Current regulatory arrangements relevant to surveillance

This section assesses the extent to which existing regulatory arrangements already deal with the new phenomenon of inexpensive aerial monitoring. The topic draws on the

analysis of regulation presented in the third paper in this series. This identified natural controls, plus four regulatory forms – organisational self-regulation, industry self-regulation, co-regulation, and formal regulation, defined in Table 1 in that paper – and a set of criteria for effective regulatory schemes, defined in Table 2.

The questions addressed in this section are:

- To what extent are surveillance activities as a whole currently subject to effective regulation?
- To what extent does it appear that the current regulatory arrangements are effective when applied to surveillance activities conducted with the assistance of drones?
- How do the laws apply to sousveillance (i.e. performed by a person) in comparison with surveillance (in the sense of being performed by an 'authority' such as the State, and the corporations that are increasingly dominating human affairs)?

In order to make the greatest possible contribution to policy formation, it is highly desirable that the analysis of regulatory frameworks be generic, and reflect the industry practices and laws in multiple jurisdictions. This would ensure that insights were drawn from various contexts, and that the conclusions drawn had at least some degree of applicability throughout the world. The third paper endeavoured to adopt this approach in respect of drones' public safety impact. Adopting the same approach in relation to surveillance, however, has proven to be even more challenging. The aviation industry has operated for the last seven decades within the framework provided by an international convention, resulting in considerable similarities across almost the entire world. No such cohesive influence exists in the field of surveillance regulation. Practices, laws, and responses to the many challenges presented by surveillance technologies vary enormously among jurisdictions, and even among sub-jurisdictions within individual countries. The approach adopted in this paper has accordingly been to examine in some depth the practices and laws of a single nation, the author's country of domicile, Australia.

Although military applications of drones have attracted a considerable amount of attention in the legal and policy literatures as well as in media outlets, few articles have been located in the refereed literature that address the specific focus of this paper on surveillance in civilian contexts. See, however, Gogarty and Hagger (2008) and Finn and Wright (2012).

The section commences by reviewing natural controls, and self-, industry and co-regulatory forms, in order to identify ways in which surveillance by means of drones is subject to controls. It then considers a range of pre-existing laws that may represent constraints on behaviour, culminating in privacy laws and laws relating specifically to surveillance.

### 4.1. *Natural controls*

As discussed in the third article in this series, a number of natural controls might have some degree of effectiveness. This section considers technological limitations, physical danger, economics, reputation and countervailing power.

It is a common experience for technologies to promise a great deal, but deliver rather less and rather differently. Examples of areas in which drone-based visual surveillance may encounter challenges include drone operational reliability, image-quality, precision of drone control and of camera control, reliability of image-capture and -transmission, misidentification of surveillance targets, and robustness. As indicated in earlier papers in this series, reports to date identify multiple problems, but there continues to be considerable investment, suggesting that venture capitalists consider them to be surmountable. If so, then technological limitations will not be an effective control against unreasonable uses.

A range of physical threats affect all aircraft, including a variety of aspects of weather, disturbances of the atmosphere e.g. by volcanic eruptions and by other aircraft, physical congestion of airspace by terrestrial artefacts such as buildings, cranes and powerlines, and by mobile artefacts such as manned aircraft and other drones, and electronic congestion that may reduce the reliability of the drone's data- and control-feeds. Further physical threats arise from disaffected individuals and organisations that may seek to damage or destroy the drone, including individuals who perceive themselves to be subject to surveillance by the drone in question. Risk of loss of a valuable aircraft is a strong disincentive against the conduct of surveillance, and risk of even injury let alone loss of life is an even stronger one. On the other hand, small drones are inexpensive, and the pilot is remote rather than on board the aircraft. Physical dangers are therefore a far weaker natural control over drone usage than is the case with conventional aircraft.

Economic factors might be expected to act as a constraint. The conventional approach in the private sector is for a 'business case' to be presented. This technique is, however, easily manipulated to fit with the strategic intent of powerful players within executive teams. In addition, studies in such areas as data matching, biometrics and body scanning have located little evidence of cost/benefit analysis being undertaken (Clarke and Stevens, 1997). In any case, cost/benefit analysis has a very narrow perspective, in that it fails to take into account benefits and disbenefits to stakeholders other than the organisation making the investment, and often fails to address contingent disbenefits (risks) even to the sponsor, let alone to other parties (Clarke, 2008a). Because of the low financial investment involved, it is unlikely that cost-benefit analysis will be performed, and unlikely that economic factors will be a significant inhibitor of drone usage for surveillance purposes.

Harm to reputation may arise from it becoming known that an organisation conducts surveillance using drones. This may be a factor of consequence in the case of organisations that depend heavily on the support of the public or of a key customer that may be concerned about its behaviour. It will have far less impact, however, where the party conducting the surveillance has substantial institutional power (such as law enforcement agencies) or market power (such as media corporations), or has little regard for their reputation (such as paparazzi and voyeurs).

A further possibility is that countervailing power may be exercised by one or more categories of parties affected by the

process, perhaps acting collectively, or through the mass media, or by attracting support from a competitor or a celebrity. Given the imbalance of power between organisations and individuals, it may not be realistic to expect this factor to be of any great significance except in very particular circumstances, such as when the public as a whole is revulsed by serious abuse, perhaps in relation to children, or to a member of a royal family. Or might complaints, boycotts, demonstrations, civil disobedience, vigilante groups, physical attacks and cyber-attacks change the balance of power?

There will be some circumstances in which natural controls effect some degree of limitation on surveillance activities generally, or using drones in particular. In most circumstances, however, they are likely to have limited impact. The exercise of control over excessive and unreasonable use of drones for surveillance requires a regulatory regime.

### 4.2. *The 'soft' regulatory forms*

Formal regulation is inevitably inflexible. In a fluid environment, such as that arising from experimentation with drones, and innovative applications of them, there are potential benefits for all parties in sustaining a degree of flexibility during the pioneering phases, and relying on less formal mechanisms to protect the various parties' interests. Might such approaches offer sufficient protections at least in the short term, and enable the gathering of experience to inform the development of a formal regulatory regime that is balanced, effective and efficient?

#### 4.2.1. *Organisational self-regulation*

Organisations might exercise self-restraint. Such behaviour could be influenced by professional norms, or by an appreciation of the fragility of public confidence in its institutions. Some organisations may recognise the need to respect individuals' rights that have no legal basis but are regarded by the society as moral rights. Another possibility is that drone-using organisations might limit their use of the technologies because they recognise a corporate responsibility to do so, or perceive it to provide them with a strategic or competitive advantage.

The Privacy Impact Assessment process is well-understood, and readily applied by any organisation that adopts either a strategic or a risk management approach to the issues (Clarke, 2011; Wright and De Hert, 2012; Wright and Raab, 2012). However there is virtually no discussion in the literature about PIAs for drone surveillance. An exception is a suggestion by the Queensland Information Commissioner's Office that a PIA be performed, at least in relation to data privacy, but arguably more broadly (OIC, 2013).

Where an organisation does commit to self-restraint, it may be evidenced through the publication of a Customer Charter or an internal Code of Conduct. Most such organisational codes are, however, expressed in highly vague, 'motherhood' terms, and, to the extent that they are specific, go little beyond re-stating the organisation's legal obligations. A scan of a small sample of websites of drone providers and user organisations found no such document. Even a drone-operating service-provider that advertises "high definition close-range aerial filming", highalpha.com.au, offered no indication of any care applied to the visual surveillance it undertakes for its clients. Its portfolio at that stage contained no high definition close-range shots of individuals of the kind likely to threaten behavioural privacy; but that may say as much about the selection of the images as about the imagery that the organisation actually gathers.

At this stage, it may be too early to expect Customer Charters to refer to the use of drones. On the other hand, surveillance of various kinds is already widely used. A scan of Customer Charters found some – primarily transport operators – that promise more surveillance, as part of their security service. But it found no Customer Charters that made any commitments about exercising controls over the organisation's use of surveillance. One significant example of an organisation whose Charter could reasonably be expected to include such undertakings is that of Centrelink, the Australian government agency that manages all transfer payments. This includes 'Respect', but the operationalisation of the term fails to address surveillance (DHS, 2013). Another example is the Australian government agency that manages all taxation matters. Its Charter says "You can expect us to … treat you as being honest unless you act otherwise" (ATO, 2013), but includes nothing more that is relevant to its use of surveillance. Each agency effectively reserves the right to do whatever it likes with surveillance technologies, and with surveillance drones.

An exception came to light during associated research on media corporations' codes of conduct. The Murdoch stable of newspapers in Australia are grouped under the holding company News Limited. That company has had a Professional Conduct Policy for some years (News Ltd, 2006). During the preparation of a normative Code for the Media (Clarke, 2012e), analysis was undertaken of all such Codes published by Australian media organisations. Contrary to widespread expectations, the News Limited Code was clearly the one that was most comprehensive and that appeared to afford the most protection for the interests of people subjected to media attention (Clarke, 2012a).

Unfortunately, that was where the warm glow came to an end, because it has been comprehensively demonstrated that News Ltd's Professional Conduct Policy had not been drawn to the attention of staff at any of the newspapers that the Chief Executive claimed were subject to it, and it had not been used when decisions were made either about the surveillance of people of interest or about publication of personal data (Simons, 2011a,b,c,d).

News Limited's and a few other media organisations' somewhat weaker Codes have at least some potential to address problems identified in this paper. However, no evidence has been located of such codes being actually applied by the organisations themselves or otherwise having any impact on the behaviour of their employees and contractors. In the absence of any evidence of commitments by organisations in relation to responsible use of surveillance technologies, it is difficult to see organisational self-regulation playing any role in the control of drone surveillance.

#### 4.2.2. *Industry self-regulation*

Organisations may recognise the need for an industry-level commitment. A conventional approach to such a

commitment is an Industry Code of Conduct. However the Code of the most apparently relevant US association says merely that "We will respect the privacy of individuals [and] the concerns of the public as they relate to unmanned aircraft operations" (AUVSI, 2012, 2013). Added to that, there is a complete absence of any commitment by members to the Code, and of any enforcement mechanisms. The same problems exist with other organisations, including the Australian Association for Unmanned Systems (AAUS).

Drone providers primarily sell or lease to users, and hence it can be reasonably argued that the major responsibility lies with user organisations. During the twentieth century, it was common for separate industry collectives to exist on both the provider and user sides. No substantial international collective of drone users was located. In Australia, the association of Australian Certified UAV Operators (ACUO), formed in 2009, has processes in place to develop a code, but as yet no Code.

A specialist group in the law enforcement field, the International Association of Chiefs of Police, has published a set of 'Recommended Guidelines' (IACP, 2012). They are unenforceable, and hence have no direct bearing on operations, although they may have some 'moral suasion' value. The Guidelines make a number of substantive contributions relevant to surveillance and privacy:

- "[Agencies should] engage their community early in the planning process, including their governing body and civil liberties advocates"
- "The community should be provided an opportunity to review and comment on agency procedures as they are being drafted. Where appropriate, recommendations should be considered for adoption in the policy"
- "Unless required as evidence of a crime, as part of an ongoing investigation, for training, or required by law, images captured by a UA should not be retained by the agency"
- "Unless exempt by law, retained images should be open for public inspection"

However, the Guidelines were motivated by the observation that "concerns about privacy threaten to overshadow the benefits this technology promises to bring to public safety", and the Association reached the conclusion that "privacy concerns are an issue that must be dealt with effectively if a law enforcement agency expects the public to support the use of UA by their police". It remains to be seen whether these sentiments are intended as anything more than window-dressing, and, if so, whether they will have any impact on the actual practices of law enforcement agencies, and, if so, whether any such positive impact will last beyond the initial phases of drone implementation. In Australia, for example, no evidence has been seen of any of the multiple law enforcement agencies that have used drones taking any notice of any of the exhortations listed in the IACP document.

Industry self-regulation in the media field provides further examples of window-dressing rather than any substantive contribution to the regulation of surveillance activities. The Code of Ethics of the professional association of journalists in Australia contains nothing more than the statement that journalists should "Respect private grief and personal privacy. Journalists have the right to resist compulsion to intrude" (MEAA, 1996). In any case, no evidence has been found of any procedure whereby the Code might be applied. Meanwhile, a draft Code of Ethics for Drone Journalists contains only a short line on privacy, which appears to deny an undefined category of 'public figures' any protections whatsoever (PSDJ, 2013).

A more substantial example exists. The Australian Press Council (APC) was formed in 1976 specifically as a means of holding the line against regulatory action by providing the appearance of self-regulation. The analyses in Clarke (2012a,c) show how far short of being a meaningful form of protection the APC's Code (APC, 2011a,b) falls. The Australian Law Reform Commission observed that "Such sanctions for breach as exist provide few, if any, real remedies for individuals whose privacy rights have been seriously affected" (ALRC, 2008a, at 42.24). The Finkelstein Inquiry into the Media and Media Regulation in Australia was in no doubt that serious problems exist and that the existing mechanisms "are not sufficient to achieve the degree of accountability desirable in a democracy" and "the problems … are inherent, and cannot be easily remedied by piecemeal measures" (Finkelstein, 2012, Executive Summary, paras. 6 and 7). In the UK, the Leveson Inquiry reached similar conclusions about that country's Press Council (Leveson, 2012).

During the second half of the twentieth century, industry associations comprised corporations that provided comparable goods and services. In the IT industry, it was common for associations of user organisations to exist as well, to represent the interests of purchasers of particular categories of IT goods and services. Since late last century, however, there has been an increasing incidence of associations whose membership comprises organisations along the whole value-chain, including producers, distributors and consultants, up to and including end-users. In such areas as biometrics, alliances of vendors and user organisations have conspired to generate favourable test results and to suppress the conduct and reporting of genuinely independent tests. Far from regulating themselves with 'the greater public good' in mind, longitudinally-integrated industry chains manipulate publicly-available information in order to overcome impediments to adoption of technologies that are at best unproven, perhaps ineffective, and even fraudulent. This is a highly unhealthy 21st century form of collusion, but regulators and parliaments have ignored it. Given the current dominance of 'national security' overtones among many drone-using organisations, collusive 'industry' associations would appear very likely to emerge in this area as well. This would augur very badly for a balanced outcome that takes behavioural privacy needs into account.

Very little evidence has been found to suggest that industry self-regulation will contribute much at all to controlling the inevitable excesses of drone surveillance. Moreover, there is a real risk of a contrary development, with 'industry value-chain' associations exercising their power to avoid effective regulation, and hence having very little incentive to sponsor industry self-regulatory behaviour that would ensure protection of the interests of individuals. Hayes et al. (2014) identify precisely such developments in Europe.

#### 4.2.3. *Co-regulation*

As described in the third paper in this series, co-regulation involves one or more Codes negotiated among stakeholders, with the Code then being subject to enforcement. For co-

regulation to be effective, industry needs to have significant input to the requirements, but other stakeholders need to have sufficient influence to ensure that their interests are reflected, and the outcome needs to sit within a statutory context, including enforcement mechanisms and graduated sanctions.

No evidence was found of any co-regulatory process emerging in relation to drone surveillance, or indeed of any involvement of stakeholders outside the drone industry. Further, such case studies as can be found in related fields provide little confidence that an adequate outcome might be achieved. For example, a nominally co-regulatory scheme exists in the commercial broadcast media in Australia, administered by the Australian Communications and Media Authority (ACMA). The scheme applies only to the publication of information, not to the practices that give rise to it, and hence Australian broadcast media are completely free of any regulation in relation to their use of surveillance technologies. In any case, ACMA has comprehensively demonstrated that the arrangements are completely ineffective in relation to the protection of data privacy (Clarke, 2012a, pp. 184–185), to the extent that even media commentators have expressed derision (e.g. Ackland, 2011).

#### 4.2.4. *Conclusions*

None of the soft regulatory forms make any significant contribution towards satisfying the criteria for effective regulation outlined in Table 2 of the third paper in this series. They provide virtually no protections against unjustified, disproportionate and unsafe surveillance. The protection of behavioural privacy against undue surveillance is therefore entirely dependent on formal regulatory arrangements.

### 4.3. *Pre-existing generic laws*

A variety of longstanding laws may have applicability to surveillance activities, particularly those that balance rights among parties. In common-law countries, particular common law and statutory torts may represent constraints on the use of drones. In the US context, Vallesenor (2013) considers trespass, intrusion upon seclusion, publication of private facts, and stalking and harassment. Because the laws in particular jurisdictions exhibit so much diversity, the analysis here is limited to the Australian context. This was originally derivative from the law of the UK of the nineteenth century. Since then, it has developed in parallel and separately from British law, but frequently draws on and references decisions of senior courts throughout the common-law world.

This section considers in turn land-related and other torts, recently-emerged statutory provisions, and human rights laws.

#### 4.3.1. *Trespass*

The lawful occupiers of land (i.e. owners or lessees) have a general right to prevent other parties from being on their land, and from doing particular acts on their land, even if an area is readily accessible by the public. A breach of this right is the tortious wrong of trespass. The tort is of sufficient significance that the rights of real property owners to prevent the use of surveillance devices within their property are expressly overridden by the Surveillance Devices Act (Cth), and by parallel legislation in each sub-jurisdiction, in order to permit law enforcement agencies to seek warrants from a hand-selected panel of judges, and even to issue their own extra-judicial warrants, e.g. in emergencies.

The tort of trespass might have some effectiveness in preventing other parties from conducting visual surveillance if they could only do so by entering the property, e.g. because the intended object of the surveillance is too far from the boundary of the property to be seen, or is shielded from view from outside the property. However, trespass is not effective in preventing images captured from outside the property. This includes capture from the air, whether by means of a piloted aircraft or a drone.

The interests of the aviation industry have been prioritised over those of citizens and consumers in that trespass by aircraft is not actionable, in at least NSW by virtue of the Civil Liability Act (NSW) s.72 and Victoria under the Wrongs Act (Vic) s.30, provided that the aircraft's height is reasonable in the circumstances (a notion that appears not to have been clarified by the courts) and in accordance with the Air Navigation Regulations (Cth). Similar provisions may exist in other Australian jurisdictions.

#### 4.3.2. *Nuisance*

The tort of nuisance deals with interference with a real estate occupant's quiet enjoyment of their property. In an NSW case in 1995, where a neighbour "had installed video equipment and lighting which was activated by movement or noise", the plaintiff was able to "establish a cause of action in nuisance giving grounds for an interlocutory injunction to restrain a nuisance, both on the way the lights were activated and the video equipment used" (Gaudin, 1996). This is positive, but expensive actions in the Supreme Court are not a cost-effective approach to such problems, and are entirely inaccessible for all but the most well-off members of the public.

The tort of nuisance cannot be used to deal with media stake-outs at locations such as parliaments or court-houses, nor to pursuits. In principle, it might be applicable to stake-outs at a celebrity's home, but the fact that it appears not to have been used for this purpose strongly suggests that celebrities' legal advisers consider that it is not an effective cause of action.

In any case, the entire aviation industry is relieved of its obligations under the tort of nuisance by the same provisions noted in the previous section in relation to trespass. Drone surveillance, possibly by accident but possibly intentionally, enjoys a statutory exemption from the tort of nuisance.

#### 4.3.3. *Other torts*

Several other tortious remedies might have relevance in particular circumstances:

- trespass to the person (direct and substantial interference with a person's autonomy), obstruction (interference with a person's freedom of movement or action), assault (an act intended to cause the reasonable apprehension of an immediate harmful or offensive contact) and false imprisonment
- stalking (persistent unwanted communications, approaches, pursuit and/or monitoring that creates apprehension or fear)

- misrepresentation, involving deceit, passing off or injurious falsehood
- negligence (to the extent that a duty of care may exist, e.g. to a child who is being interviewed or whose behaviour is being recorded)
- breach of confidence (to the extent that some kind of confidentiality is express or could be reasonably inferred)

However, all of these torts are very narrowly defined. They are also subject to statutory overrides, particularly in favour of law enforcement agencies and other government agencies. All tort actions have to navigate minefields of arcane and ambiguous interpretations based on precedents whose facts were very different from those arising from drone surveillance, and whose applicability will be determined by courts at first instance, but in many cases adjusted or reversed on appeal. Further issues are that cases proceed very slowly and expensively, and that copious opportunities exist for powerful, well-resourced organisations to cause further delays, to increase the litigant's costs, and hence to avoid or circumvent justice. Outcomes are far from certain, and subject to expensive and very slow appeal processes.

The legal system in Australia serves consumers and citizens very poorly in many areas. The chances of any of these laws providing any meaningful check on drone surveillance appear very slim: "Whilst some existing tortious laws, such as trespass, might prohibit UVs from entering private property, their ability to exclude unwelcome surveillance from outside the property is limited. … This leaves individuals with little in the way of actionable rights against UVs that are used to survey their private property. … [Drone] technology thus renders the traditional common-law assumption — that privacy can be protected by the individual — a fallacy" (Gogarty and Hagger, 2008); and "Common law protections are ineffective. It is not a trespass to fly over another's land and nuisance would be a difficult claim to sustain. Relying on breach of confidence is an option but quite an artificial way to approach the issue. It would require complex pleading" (P.A. Clarke, 2013).

#### 4.3.4. *Recently-enabled causes of action*

A number of new heads of law have emerged in recent decades. In NSW, a person may apply for an Apprehended Violence Order (AVO) against an individual whose behaviour is threatening to them. The mechanism has had some degree of effectiveness, but also demonstrated a range of deficiencies. Moreover, in 2007, the AVO enabling provisions were moved from Part 15A of the Crimes Act to the Crimes (Domestic and Personal Violence) Act, which appears to have greatly reduced the range of circumstances in which they can be applied for. For example, it appears that they cannot be used in actions against the media.

In Victoria, the Personal Safety Intervention Orders Act (Vic) created a similar mechanism in 2010. PSIOs are available for "victims of … harassment [and] stalking … ", where:

- "harassment means a course of conduct by a person towards another person that is demeaning, derogatory or intimidating … "
- "[stalking means] a course of conduct with the intention of causing physical or mental harm to the second person, including self-harm, or of arousing apprehension or fear in the second person for his or her own safety or that of any other person; and that includes any of … following …, contacting …, tracing …, entering or loitering …, [and] keeping … under surveillance …".

Despite the inclusion of the term 'keeping under surveillance', surveillance of any kind, including by drones, will seldom constitute stalking, because of the requirement of 'intention to cause harm'. Harassment may have some limited applicability, although 'demeaning, derogatory or intimidating conduct' again is likely to generally exclude mainstream surveillance activities. Hence even the most recently created causes of action appear highly unlikely to act as any meaningful constraint on unreasonable uses of drones for surveillance.

#### 4.3.5. *Human rights laws*

An international framework exists in the form of the International Covenant on Civil and Political Rights (ICCPR). In some countries, rights are embedded within the constitution, and in some others they are expressed in legislation. However, even where human rights instruments actually give rise to legal rights, those rights are frequently insufficiently specific to represent meaningful constraints on other parties' use of visual surveillance. Finn and Wright (2012, pp. 192–193) concluded, however, that there may be some limited scope for human rights law to be used to curb drone use in the USA and in European countries. Thompson (2013), on the other hand, suggests that the Fourth Amendment to the US Constitution may provide very little protection against drone surveillance.

In many countries, on the other hand, human rights are at best constitutionally implicit, and for the most part are merely matters of public policy. In Australia, for example, the proposal in the 1890s to embed a Bill of Rights in the Constitution was defeated, and the Constitution creates only five very specific human rights (such as the right to vote). The national Parliament has consistently refused to pass legislation of any kind (thereby breaching its obligations arising from accession to ICCPR).

Only two of Australia's eight subsidiary jurisdictions have human rights instruments, and both are mere statements of aspiration. The ACT and Victorian Acts merely replicate the vague wording of ICCPR 17.1: 'a person has the right not to have his or her privacy, family [or] home … unlawfully or arbitrarily interfered with', and fail to implement ICCPR 17.2 regarding 'the right to the protection of the law against such interference'. They are thereby entirely unenforceable. People in countries with such valueless laws have no recourse to human rights as a means of protecting themselves against privacy-abusive uses of drones.

#### 4.3.6. *Conclusions*

A range of pre-existing generic laws could in principle provide some regulatory impact on surveillance applications of drones. In practice, in Australia, any such effect appears to be at best very limited, because of the tight limitations on the

applicability of the causes of action that are imposed variously by the common law and by legislation. Significant changes would need to be enacted in order to overcome these deficiencies. Given the slow pace of legal reform, this appears unlikely, and hence regulatory mechanisms need to be sought elsewhere.

### 4.4. *Aviation law*

The third paper in this series considered aviation laws in some depth. The primary purposes of the Chicago Convention on International Civil Aviation, and of the international body the International Civil Aviation Organisation (ICAO), are the facilitation of air traffic, and public safety. In many countries, aviation laws and the functions of the national regulator mirror that focus – and do so with highly beneficial effect. On the other hand, aviation laws contain little or no protection against aerial surveillance, and concerns such as privacy are out-of-scope for most and possibly all regulatory agencies.

In Australia, for example, the Civil Aviation Safety Authority (CASA) limits its focus to safety: "Dealing with matters related to privacy … and environmental footprint, noise and gaseous emissions … [are] not part of CASA's role" (CASA, 2013). Privacy is unlikely to be addressed within the aviation context at all, unless some broadening of the scope of CASA's considerations is forced, and funded, e.g. through an argument along the lines of:

(1) aerial monitoring of individuals constitutes stalking and harassment
(2) stalking and harassment result in psychological and even physical harm to individuals
(3) retaliatory measures will be undertaken (T&D, 2012; Coffman, 2013)
(4) retaliatory measures will endanger drones
(5) retaliatory measures will result in collateral damage, from:
    (a) disablement of the drone, causing it, or parts of its wreckage, to hit something else
    (b) a projectile aimed at the drone hitting something else

On the other hand, the analysis in the third paper in this series demonstrated that CASA is very casual about the public safety implications of drones, and hence such a line of argument is unlikely to attract any attention from at least the Australian regulatory agency.

In the USA, "the FAA may, but need not, choose to consider elements other than air safety, such as privacy, when implementing regulations" (EPIC, 2012). ACLU (2011) called for safeguards in the areas of public participation in policy formation, limits on purposes and on data retention, abuse prevention, and accountability for abuse. Under pressure from privacy advocates, FAA stated that it would extend its Test Site Program beyond safety issues to encompass privacy concerns (FAA, 2013a). However, by the end of 2013 it was apparent that FAA is not giving any meaningful consideration to privacy issues in its 'near-term' 'Accommodation' phase 2013–2015. Its Roadmap suggests that it may pay some attention to "the privacy, security, and environmental implications of UAS operations" in its 'mid-term' 'Integration' phase, c. 2016–2018 (FAA, 2013b, p. 32). The Terms of Reference for its Trial Sites would appear not to contain anything that might even contribute to an understanding of behavioural privacy issues, let alone to the development of effective protections (FAA, 2013c).

In Europe, the Joint Aviation Authorities' concept document for UAV regulation was exclusively concerned with safety aspects of drones (JAA, 2004), and although EC (2013) recognised that the surveillance capabilities of drones make privacy an issue that needs to be addressed, the group regarded the problem as being outside its scope, and the responsibility of national data protection authorities rather than an EC matter. This is of course an inadequate response, because national 'data protection' agencies are for the most part constrained to 'data protection' and most cannot give any deep consideration to behavioural privacy.

There appears to be very little in aviation law that acts as a control over drone surveillance, and very little prospect of aviation law in any country ever being upgraded to address the problems that this paper has identified.

### 4.5. *Privacy law*

With rare and minor exceptions, the courts have not established any meaningful tort law protections for privacy. UK law has afforded some limited rights to celebrities. Under US law, however, there is "no reasonable expectation of privacy in public or from a public vantage point … [and] … it will be difficult under existing case law to find a reasonable expectation of privacy from unmanned aerial surveillance in navigable airspace" (Farber, 2014, pp. 18, 22).

A great many statutes have been enacted since 1970, throughout the world, many of them referred to as 'privacy laws'. They are, however, limited to, and severely constrained by, the 'fair information practices' (FIPs) model. This has a strong orientation towards ensuring minimal inconvenience to business and government rather than towards protecting individuals' rights (Clarke, 2000). These laws are in any case almost entirely 'data privacy' or 'data protection' laws. At best, they only incidentally address other dimensions, in particular behavioural privacy.

It might have been expected that data protection laws would provide some degree of behavioural privacy protection through constraints on unreasonable collection practices. However:

- the OECD Guidelines that underpin the FIPs model are extremely weak in this area, saying merely that "data should be obtained by … fair means" (OECD, 1980, Principle 7, paras. 50–52)
- so is the otherwise benchmark EU Directive of 1995 – which merely requires that "personal data be [collected] fairly" (EC, 1995, Article 6.1(a), unnumbered p. 10)
- so too is the Draft Regulation of 2012–2013 – which states solely that "personal data must be [collected] fairly" (EC, 2012, Article 5(a), p. 43)
- the Council of Europe's Convention 108 also merely declares that "Personal data shall be … obtained … fairly … " (CoE, 1981)

An example of the national impact of these extraordinarily weak provisions is that the UK lacks any controls over unreasonable collection practices, as evidenced by the oversight agency's incomplete and weak guidance on CCTV (ICO, 2008).

No evidence was found that either the Article 29 Working Party of EU data protection authorities or the European Data Protection Supervisor has to date considered drones. The scope of those organisations is in any case limited to data privacy, and hence a vacuum exists in Europe, with no supervisory agency having any responsibility for the protection of behavioural privacy against the harm arising from surveillance, including surveillance that utilises drones.

Australia is one example of a jurisdiction within which the relevant principle was for many years articulated a little more helpfully than the OECD, the EU and many European countries have ever achieved. The Privacy Act 1988 (Cth) contained the familiar but essentially empty provision about 'fair means', but also the following unusual feature:

- within the set of Information Privacy Principles (IPP, 1988), which was applicable to government agencies from 1989 to March 2014, IPP3(d) states that "[an agency] shall … ensure that, having regard to the purpose for which the information is collected, … the collection of the information does *not intrude to an unreasonable extent upon the personal affairs of the individual concerned*" (emphasis added)
- within the set of National Privacy Principles (NPP, 1988), which was applicable to many organisations in the private sector from 2001 to March 2014, NPP1.2 states that "An organisation must collect personal information … *not in an unreasonably intrusive way*" (emphasis added)

Data privacy protections in Australia were greatly weakened by amendments in 2012, which took effect in March 2014. In drafting these amendments, the Attorney-General's Department ignored many of the Australian Law Reform Commission's Recommendations, and most of the submissions by public interest advocacy organisations, and instead accepted the vigorous pleadings of government agencies and industry. These pleadings are reflected throughout the massively amended Privacy Act, and in the 5000-word set of Australian Privacy 'Principles' that replace the IPPs and NPPs (APP, 2012).

The IPPs and NPPs quoted above have been replaced by APP 3.5, which requires only that "An APP entity must *collect personal information* only *by … fair means*" (emphasis added). From March 2014, the Privacy Act (Cth) accordingly ceases to constrain any Australian organisation from gathering personal data "in an unreasonably intrusive way".

In any case, the Australian Privacy Commissioner's role is very weak, and is very meekly administered. The previous and current Commissioners have steadfastly avoided taking any action against government agencies or corporations in relation to surveillance matters. Some of the Commissioner's functions are explicitly limited to the administration of behaviour by organisations that are encompassed by the IPPs and NPPs, and now the APPs. Some functions, on the other hand, relate to privacy generally rather than merely to interferences with data privacy as defined by the Principles. These generic functions include "to undertake research into, and to monitor developments in, data processing and computer technology … to ensure that any adverse effects of such developments on the privacy of individuals are minimised" (Privacy Act, s.27(1)(c)), but also the preparation and publication of guidelines (s.27(1)(ea)), education (s.27(1)(m)), and reports and recommendations (s.27(1)(r)). The Commissioners for the last decade have actively ignored these generic policy functions and limited themselves to administrative activities.

Quite simply, the use of drones for surveillance by Australian government agencies and corporations is not subject to any formal privacy law. The Privacy Commissioner has suggested to the Attorney-General that "it may be timely to review the current regulatory framework", and an Australian Law Reform Commission study has drones as one small element within a much broader brief it is addressing during 2013–2014.

State government agencies are not subject to Commonwealth law. NSW has always avoided imposts on its agencies, in that nothing in its data protection statute prevents even collection by unfair means let alone collection in an unreasonably intrusive manner. Queensland government agencies are also subject to no controls over collection in an unreasonably intrusive manner, although they are supposed to be precluded from collection in a way that is unfair. As noted, however, the Queensland Commissioner has issued a brief paper on drones which includes the suggestion that agencies "may find [PIAs] very useful" (OIC, 2013).

The Victorian Act at this stage still stipulates that "An organisation must collect personal information only by … fair means and not in an unreasonably intrusive way" (VIPP, 2000, Principle 1.2). However, the Commonwealth's APPs were expressly intended to achieve nationwide harmonisation, i.e. to ratchet down already-weak privacy protections to the lowest available common denominator. So it can be reasonably expected that Victorian government agencies will shortly conduct a campaign to remove the 'unreasonably intrusive collection practice' protections that have been nominally afforded by Victorian law.

A similar analysis of the data protection principles applicable in every one of the hundred countries and many scores of subsidiary jurisdictions throughout the world might locate a small number of circumstances in which some limited controls exist over intrusive visual surveillance. However, even in those cases, it is highly unlikely that any such provisions represent an effective regulatory mechanism over visual surveillance generally, or surveillance involving drones.

### 4.6. *Surveillance laws*

In most jurisdictions, various laws exist that explicitly regulate surveillance – although each generally relates to surveillance only of a specific kind, and in specific circumstances, and often the primary purpose is to empower organisations rather than to protect individuals. Such laws tend to exhibit considerable differences across jurisdictions. The approach adopted here limits the focus to a single country, but one in which differences exist among the country's sub-jurisdictions that exemplify the challenges involved in appreciating how laws affect the use of drones for surveillance.

The section commences by considering Australian surveillance statutes. Brief reviews are also provided of formal regulatory arrangements in relation to surveillance by the media, by law enforcement agencies, and finally by individuals.

#### 4.6.1. *Surveillance devices laws*

Relevant laws in Australian jurisdictions have titles such as 'Surveillance Devices Act', 'Workplace Surveillance Act' and 'Listening Devices Act'. This section builds on prior research that assessed Australian laws relating to media use of visual surveillance (Clarke, 2012b), and to 'point of view' surveillance using wearcams (Clarke, 2012d). That research in turn drew on a longstanding source relating to photography in the State of N.S.W. (Nemeth, 2005).

Surveillance devices legislation is largely a matter for the States and Territories. Five of the eight have laws with general effect relating to the use of 'optical surveillance devices'. Four (WA, Vic, NT, NSW) have Surveillance Devices Acts from the period 1998–2007, and the other (Queensland) has a provision in its Criminal Code. These provide varying but very limited protections. Broadly, visual and/or aural surveillance of a 'private activity' is likely to be illegal, but 'private activity' is defined extremely narrowly. The term does not apply to activity outside a building (although in NSW it does include activity in a car), nor does it apply where it is reasonable to assume the parties to it did not care whether they were seen by others, nor if they could not have reasonably expected that it would not be seen by others, and nor does it apply to someone who is a party to the activity. There appear to be few prosecutions under these laws.

The other three jurisdictions (SA, Tas, ACT) have Listening Devices legislation dating to the period 1970–1990, but have never extended them to visual surveillance. Two jurisdictions (NSW and ACT) also have statutes authorising employers to conduct visual surveillance in the workplace. In the case of overt surveillance it is merely necessary to declare that they conduct surveillance. Some conditions apply to the conduct of covert surveillance. In those jurisdictions and in Victoria, surveillance is prohibited in toilet facilities and similar areas.

A number of additional statutes exist that have the character of visual surveillance laws. During various periods of moral panic, States and Territories have enacted legislation relating to 'peeping-tom', 'upskirting' and 'downblousing' activities. Many of these laws have had to be withdrawn or amended when cases reached the courts and anomalies and unintended consequences emerged. An apparently more effective and enforceable formulation is in the Queensland Criminal Code, which criminalises observation or visual recording made for the purpose of observing or visually recording another person's genital or anal region (s.227A) and distributing prohibited visual recordings (s.227B). In NSW, Division 15B of the Crimes Act 1900 ss.91I–91M contain voyeurism offence provisions, relating to photographs of a sexual and voyeuristic nature, usually of a person's "private parts", if they are taken without consent, and taken in places where a "reasonable person would reasonably expect to be afforded privacy" (such as toilets and showers, and possibly changing rooms, but also conceivably in enclosed backyards).

Two recent cases, both involving the Australian Defence Force Academy, demonstrated the ineffectiveness of the current mish-mash of laws. In one, a case against a cadet accused of "secretly filming a fellow cadet while she was showering" was dismissed because of a technical deficiency in the ACT surveillance legislation (Nairn, 2012). In the other (R v McDonald and Deblaquiere, 2012–13), a cadet transmitted video to colleagues of a sex act performed with another cadet who was unaware of the filming and transmission. Such behaviour appears to be generally regarded by the public as inappropriate, and there is an expectation that it be subject to at least civil and perhaps also criminal procedures. It was found to break no military, no privacy, and no surveillance laws, and it is remains unclear whether it gave rise to any cause of action in the civil jurisdiction. It was, however, found to breach a vague provision that creates an offence of "using a carriage service to … cause offence … [by using it] in a way … that reasonable persons would regard as being, in all the circumstances, … offensive" (Criminal Code (Cth) s.474.17).

The recording of images of children in such places as schoolyards, swimming-pools and at the beach gives rise to a great deal of moral breast-thumping from time to time. There appear to be no general prohibitions on such activities, although, where the person filmed is "a child under the age of 16 years", the NSW Crimes Act treats that fact as a 'circumstance of aggravation' in the crimes outlined above, resulting in an increase of the maximum penalty from 2 to 5 years imprisonment.

There are a few circumstances in which surveillance is subject to formal law, but the circumstances are almost entirely limited to highly private behaviour, primarily of a sexual nature or otherwise involving sex organs.

#### 4.6.2. *Media use of surveillance devices*

Drones clearly provide considerable benefits to the media, but bring with them many challenges to achieve a fair balance against other interests (Moses, 2012, 2013; Goldberg et al., 2013). It was noted earlier in this paper that, at least in Australia and the UK, the collection activities of the tabloid media are subject to seriously inadequate natural controls and seriously inadequate self-regulatory regimes. Unfortunately, there appear to be virtually no formal regulatory arrangements in place to make up for that shortfall.

As noted above, the Australian private sector has just been relieved of the limitations on gathering personal data in an unreasonably intrusive manner that have nominally applied during the period 2001–2014. But the media industry was never subject to that constraint, because it has always enjoyed complete exemption from the provisions of the Australian Privacy Act. Although the Australian Law Reform Commission recognised that a problem existed, it failed to recommend any material change to Privacy Act exemption (ALRC, 2008a). On the other hand, it recommended the creation of a statutory tort, or 'privacy cause of action' (ALRC, 2008b), intended to be of general applicability across all sectors and all dimensions of privacy. Successive Australian governments have demonstrated unwillingness to confront the media industry and impose any regulatory scheme, despite the weakening of the industry's power as a result of the revelations about the Murdoch media's abuses in the UK,

and the haemorrhaging of advertising revenue since Google snatched control of Internet-based advertising (Clarke, 2012c). The then Government made a half-hearted attempt in 2012–2013 to implement a statutory cause of action, but the new Government clearly has no intention of bringing forward any such legislation.

No other formal regulatory provisions have been identified that represent significant checks on the use by the Australian media of surveillance devices, nor of drone-based surveillance. The sole source of limitations would appear to be provisions in aviation law relating to public safety (Corcoran, 2012). That leaves the media free to use drone surveillance in a very wide range of circumstances – which is highly desirable from the viewpoint of news-gathering and democracy – but without protections for behavioural privacy.

#### 4.6.3. *Law enforcement agency use of surveillance devices*

There will without doubt be many law enforcement uses of drones for surveillance that will attract very considerable and widespread support. On the other hand, concerns have been expressed from the outset about use that is intended to generate suspicion rather than to investigate suspicious circumstances, use that is surreptitious, and use that is uncontrolled (e.g. EPIC, 2005).

Various law enforcement agencies have stated their intentions to use drones, in such applications as reconnaissance and pursuits, and perhaps as a means of managing crowds (e.g. Kyriacou, 2012; Hyland, 2012). In some cases, funding is likely to be available for military-derived technologies (e.g. prior to major meetings of world leaders, and for events like the World Cup and the Olympic Games), whereas in other circumstances police may only be able to afford inexpensive commercial and/or cheap consumer devices.

In Australia, law enforcement agencies have access to a veritable flotilla of authorisations for visual surveillance:

- the Surveillance Devices Act (Cth) s.37 authorises a large raft of national law enforcement agencies to use optical surveillance devices, in public places, without a warrant, provided only that "there is no entry to premises without permission and no interference with any vehicle or thing". There is no need for any justification to be demonstrated, or even proportionality; there are no mitigating measures needed, and there are no effective controls over use of the power
- surveillance involving entry to premises or 'interference' requires a warrant. However, these are available under permissive arrangements specified in ss.10–27
- the need for a judicial warrant can be avoided, because warrants can be self-authorised by the law enforcement agency itself merely by invoking the uncontrolled emergency provisions of s.28–36
- there are also many powers provided within the c. 60 post-September 2001 'counter-terrorism' statutes, almost none of which have been justified, but none of which have yet been repealed
- State and Territory jurisdictions have empowered their own law enforcement agencies to use surveillance and tracking devices, generally with highly inadequate controls

There is serious concern about the lack of meaningful and transparent evaluation of proposals, and of pre- and post-controls over the applications, and about the exercise of authorisation powers. Given the enormous freedom of action granted to law enforcement agencies in a great many countries, it appears likely that the Australian situation may be broadly representative.

#### 4.6.4. *Constraints on sousveillance devices*

In contrast to the freedoms enjoyed by law enforcement agencies to conduct visual surveillance, the general public is subject to a wide array of constraints. For example, the Defence Act (Cth) at s.82 proscribes the filming of military establishments. In the case of Commonwealth property more generally, the Crimes Act (Cth) s.89 applies. There are also statutes relating to specific areas and locations, such as the Sydney Harbour Foreshores in the vicinity of the Opera House. However, it appears that this particular legislation, like the Air Traffic Regulations, is largely ignored by law enforcement agencies. The drone that collided with the Sydney Harbour Bridge was reported to have carried an SLR camera which was running during its flight (Kontominas, 2013; LL, 2013). This may have been in breach of Sydney Harbour Foreshore Authority Regulation 4(1)(b) (NSW), which prohibits use of a camera for a commercial purpose in the area in which the drone was flying, unless authority is obtained. The pilot, a visitor from the UK, identified himself to the NSW Police, who were reported as having returned the drone wreckage to him, after which he posted the footage captured from the flight (NineMSN, 2013). No report of a prosecution has been located, and in early 2014 CASA was vague about whether the matter was open or closed.

Government agencies generally have an interest in denying the public the right to apply visual surveillance against them. Beyond the premises-related bans on filming, law enforcement agencies have had broad powers granted to them, for short periods in relation to specific events such as G8 and APEC meetings, and even on a permanent basis. Since 2002, the Law Enforcement (Powers & Responsibilities) Act has enabled NSW Police to self-authorise special powers in public places in the event of what it judges to be "public disorder". The powers include stop and search without warrant and without reasonable grounds for suspicion, and seizing and detaining, originally, a communication device, but since 2007 any "thing, if [its] seizure and detention … will assist in preventing or controlling a public disorder" (s.87M). Nominally, the onus is on the NSW Police to justify the self-declaration of the special powers, but s.87D is very weak in this regard. Further, the onus is nominally on the individual policeman to justify their actions, but there is an apparent lack of any real controls. In short, NSW Police can readily prevent the use of visual surveillance equipment by a member of the public, can interfere with such equipment, and can confiscate such equipment and/or data deriving from its use.

Powers to give orders and to confiscate have also been asserted by law enforcement agencies to be available to them under counter-terrorism legislation, although no specific authority has come to light. One possible authority is the offence of resisting or hindering a police officer in the execution of their duty, e.g. under s.546 of the Crimes Act (NSW). Another

possibility is the Anti-Terrorism Act (Cth) Schedule 5. The plethora of anti-terrorism laws passed since 2001 represent a veritable rat's nest of possibilities.

In the Australian context, it would appear that the sole context in which inappropriate use of drone surveillance is subject to effective controls is where a law enforcement agency perceives itself to be the victim, and is sufficiently energised to invoke real or pretended powers to give instructions to members of the public in relation to their use of such devices, to disable, seize, confiscate or destroy them, and/or to seize, confiscate or destroy image, video and sound recorded using them. Many reports exist of such behaviour by law enforcement agencies in the USA and Europe, but to date no analyses of formal powers have been located. In short, whereas surveillance is empowered, sousveillance is constrained.

#### 4.6.5. *Conclusions*

In Australia, the legal framework governing visual surveillance might be described as a patchwork quilt in which many patches are missing, and the rest are threadbare. The application of drones to surveillance appears set to exacerbate the chaos. This was expressed recently by a keynote speaker for the Annual Aviation Law Association of Australia & New Zealand, as follows: "Questions are … likely to be raised as to whether legislation such as the [NSW] Surveillance Devices Act applies to items like UAVs … [T]he frontiers of aviation will continue to raise novel issues that the law may not yet have addressed exhaustively" (Bathurst, 2013). The significance of the comment is vastly greater in that the speaker was the Chief Justice of NSW.

There is no sign of the NSW Parliament having registered that the head of its judiciary has declared, in the polite manner preferred by senior judges, that major problems exist. This is despite the existence of relevant and clear Recommendations by the NSW Law Reform Commission some years earlier (NSWLRC, 2005). The Victorian Parliament has either failed to notice, or chosen to ignore, Recommendations on the subject by its own Law Reform Commission (VLRC, 2010). In both cases, the Recommendations included extending the scope of the Privacy Commissioner to encompass surveillance. The British Government and Parliament have similarly ignored Recommendations of a House of Lords Committee (HoL, 2009).

One example of the problems that arise from such failures of the public's elected representatives is the application of the 'in plain view' dictum. The situation in New Zealand is readily presented. The Search and Surveillance Act 2012 (NZ) s.123 enables police to "*seize any item [that he or she] finds* in the course of carrying out [any lawful] search or *as a result of observations* at the place or in or on the vehicle, if the enforcement officer has reasonable grounds to believe that he or she could have seized the item or items under any search warrant that could have been obtained or any other search power" (emphases added). In short, any law enforcement officer can issue their own on-the-spot search warrant, at any time, in any place, but without so much as a responsibility to express the terms in written text, or to justify it.

Such powers in relation to items of interest 'in plain view' currently apply to individual law enforcement staff, using their own powers of observation. But it could well be applied – accidentally or intentionally, and surreptitiously or openly – to new contexts that involve surveillance apparatus, including apparatus that can observe for extended periods, can record, can convert to structured data through such means as optical character recognition applied to vehicle registration plates, and can take to the air.

If so, that would completely disrupt the delicate balance that currently exists between law enforcement powers and civil rights, and represent a further lurch away from civil society towards police state. Finn and Wright (2012, p. 192) considered the distinction between a policeman's 'naked-eye view' and technology-enhanced viewing, in the context of the US Fourth Amendment protections.

The state of laws relating to visual surveillance in Australia is important in its own right. It is also valuable as a case study. The federated nature of Australia gives rise to an overlay of complexity that some countries share (e.g. USA, Canada, UK, Germany, Switzerland, Russia, India), but many others do not. In all other respects, however, all countries are likely to face uncertainties, complexities and threats of a similar nature to those confronting Australians.

## 5. Conclusions

Visual surveillance may give rise to personal data, and the adequacy of data protection laws is in doubt, throughout the world. This paper, however, has focused on the more direct threat that visual surveillance represents to behavioural privacy and experiential privacy. Drones greatly increase not only the scope for visual surveillance to be undertaken, but also the degree of invasiveness of observation, transmission, recording, publication, location, tracking and the likelihood of interventions into the individual's behaviour by others. The need exists for a regulatory regime that protects behavioural privacy, while placing no greater constraints on the application of drones than is justified.

Natural controls appear to be far too weak to assist much at all in satisfying the need. Organisational and industry self-regulation are not in evidence, and in principle their potential impact is very limited anyway, and hence these forms are unlikely to contribute much towards a satisfactory regime. Co-regulation is an attractive idea; but it is difficult to find any relevant circumstances in which it has been applied in a manner that satisfies the criteria enunciated in the previous paper in this series. Hence, despite its theoretical promise, co-regulation too appears unlikely to satisfy the need. Formal regulation therefore appears to be essential. The frequency and intensity of media reports suggest that this sentiment may be gaining traction. Even a voice that has been consistently and stridently anti-privacy, that of Google Chair Eric Schmidt, has called for regulation of drones to protect privacy (BBC, 2013).

An examination of pre-existing laws shows them to be ill-fitted to the need, and capable of providing relief in only rare circumstances. Aviation law is focused specifically on operational needs and public safety, and is highly unlikely to be expanded to address surveillance and privacy. Data privacy laws are all-but irrelevant to behavioural privacy.

Indeed, data protection oversight agencies have such limited scope that few are empowered to contribute meaningfully to policy development in this area, while the Australian Privacy Commissioner has avoided fulfilling his statutory responsibility to do so. Laws that address surveillance specifically are largely intended to authorise surveillance by law enforcement agencies, and such privacy protections as they provide are incidental, incomplete, and very weak. Abuses by tabloid media are almost entirely unregulated. Meanwhile, law enforcement agencies have considerable powers at their disposal to preclude use by members of the public when agencies deem it to be inconvenient to them.

A rational approach to the problem is of course readily specified. In order to address drone surveillance threats, proposals need to be subjected to prior evaluation and justification. The evaluation needs to reflect the perspectives of all stakeholders, to take into account all forms of benefits and disbenefits, quantifiable and otherwise, and to extend to risk assessment in order to encompass contingent disbenefits. Frameworks for the evaluation of surveillance proposals are in Clarke (2007, 2009c) and Wright and Raab (2012). Detailed guidance on the conduct of impact assessments is available (Clarke, 2011; Wright and De Hert, 2012). Designs need to embody measures that are proportionate to the justification, and need to incorporate mitigation measures, operations need to be subject to controls, and deployments need to be reviewed (APF, 2009, 2013).

In the third paper in this series, in Table 2, a set of criteria was presented, as a means of evaluating a regulatory regime. The third cluster of criteria relate to the outcomes of the regulatory regime. In the case of surveillance by drones, the current circumstances, at least in Australia, are characterised by failure of oversight, of even enforceability let alone enforcement, and of review. The second cluster relate to the characteristics of the regulatory regime. Again the Australian situation fails on the fundamental requirement of comprehensiveness, but also on parsimony, articulation, educative value and appropriate generality and specificity. The first cluster of criteria relate to the process whereby the regulatory regime is established. To the limited extent that it might be claimed that a process exists, there is no clarity of aims and requirements, no transparency, no participation, and there is seriously inadequate reflection of stakeholders' interests. It is difficult to assign a score higher than zero out of 13.

At present, Australia has no arrangements in place in relation to surveillance that warrant a descriptor as grand as 'regulatory regime'. In many countries, a similar analysis would appear likely to reach a similar conclusion. Worse, even though deficiencies and their negative consequences are easily described, and despite the recommendations of Law Reform Commissions, there is virtually no momentum towards the creation of any such regulatory scheme. Drones will inevitably make the gap even more apparent than it already is. It is not clear, however, that public concerns will be sufficient to pierce the apathy of sleepy legislatures, or to overcome the lobbying of government agencies and corporations for freedom to implement surveillance technologies as they see fit.

It appears that a particular natural control will have to be invoked, in the form of countervailing power exercised with sufficient energy and inventiveness by enough members of the public. Activists can be reasonably expected to utilise the current freedoms. Parliamentarians and government and corporate executives who are subject to intrusive and unjustified surveillance, followed by media exposure, are likely to thereby learn what Eric Schmidt has already recognised – that behavioural privacy is very important, and that there is a need for a suitably balanced but effective regulatory regime.

## REFERENCES


Ackland R. Muddle-headed watchdog leaves the privacy door ajar. Opinion The Sydney Morning Herald. At:, http://www.smh.com.au/opinion/society-and-culture/muddleheaded-watchdog-leaves-the-privacy-door-ajar-20110217-1ay3h.html; 18 February 2011.

ACLU. Protecting privacy from aerial surveillance: recommendations for government use of drone aircraft. American Civil Liberties Union; December 2011. At: https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf.

ALRC. For your information: Australian privacy law and practice. Report 108, August 2008, Ch.42-Journalism Exemption, At: http://www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20%28ALRC%20Report%20108%29%20/42-journal; 2008a.

ALRC. For your information: Australian privacy law and practice. Report 108, August 2008, Ch.74-Protecting a Right to Personal Privacy, at: http://www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20%28ALRC%20Report%20108%29%20/74-protect; 2008b.

APC. General statement of principles. Australian Press Council; 2011a. Date of origin unclear, no prior versions visible, current version dated August 2011, At: http://www.presscouncil.org.au/general-principles/.

APC. Statement of privacy principles. Australian Press Council; 2011b. Date of origin unclear, no prior versions visible, current version dated August 2011, At: http://www.presscouncil.org.au/privacy-principles.

APF. APF policy statement re visual surveillance, incl. CCTV. Australian Privacy Foundation; 2009. Original version of September 2009, At: http://www.privacy.org.au/Papers/CCTV-1001.html.

APF. APF's meta-principles for privacy protection. Australian Privacy Foundation; March 2013. At: http://www.privacy.org.au/Papers/PS-MetaP.html.

APP. Australian privacy principles. Embodied in s.14 of the Privacy Act (Cth), At: http://www.austlii.edu.au/au/legis/cth/num_act/pappa2012466/sch1.html and http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles; 2012.

ATO. Taxpayers' charter. Australian Taxation Office; 2013. At: http://www.ato.gov.au/About-ATO/Access,-accountability-and-reporting/Informing-the-community/Taxpayers–charter/.

AUVSI. Industry code of conduct. Association for Unmanned Aircraft System Operation; 2012. Undated, but released July 2012, At: http://www.auvsi.org/conduct.

AUVSI. Unmanned aircraft systems privacy statement. Association for Unmanned Aircraft System Operation; 2013.

Undated, but apparently of 2013, at: http://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/UnmannedAircraftSystemPrivacyStatementFinal.pdf.

Bathurst TF. Opening remarks. In: Proceedings of the 32nd conference on annual Aviation Law Association of Australia & New Zealand (ALAANZ). Sydney, 6 May 2013, at: http://www.supremecourt.lawlink.nsw.gov.au/agdbasev7wr/_assets/supremecourt/m670001l771004/bathurst_130506.pdf; 2013.

BBC. Google chief urges action to regulate mini-drones. BBC News. At: http://www.bbc.co.uk/news/technology-22134898; 13 April 2013.

Bear G. Little brother is watching. Commun ACM September 2010;53(9):111–2.

Bentham J. Panopticon; or, the inspection house; 1791. London.

CASA. Development of UAS in civil airspace and challenges for CASA – Address to the Association for Unmanned Vehicle Systems Australia. Melbourne: Civil Aviation Safety Authority (Director of Aviation Safety John McCormick); 25 February 2013. At: http://www.casa.gov.au/scripts/nc.dll?WCMS:STANDARD::pc=PC_101374.

CASA. List of UAS operator certificate holders. Civil Aviation Safety Authority; 3 March 2014. http://www.casa.gov.au/scripts/nc.dll?WCMS:STANDARD::pc=PC_1009595.

Clarke PA. Drone journalism programs grounded in the USA. Illigitimi non carborundum, at: http://www.peteraclarke.com.au/2013/08/28/drone-journalism-programs-grounded-in-the-usa; 28 August 2013.

Clarke R. Information technology and dataveillance. Commun ACM May 1988;31(5). Re-published in Dunlop C, Kling R, editors. Controversies in computing. Academic Press; 1991, PrePrint at: http://www.rogerclarke.com/DV/CACM88.html.

Clarke R. Introduction to dataveillance and information privacy, and definitions of terms. Xamax Consultancy Pty Ltd; August 1997. At: http://www.rogerclarke.com/DV/Intro.html#Priv.

Clarke R. Person-location and person-tracking: technologies, risks and policy implications. In: Proceedings of the 21st international conference on privacy and personal data protection. Hong Kong, September 1999. Revised version published in Inf Technol People 2001;14(1):206–31, PrePrint at: http://www.rogerclarke.com/DV/PLT.html; 1999.

Clarke R. Beyond the OECD guidelines: privacy protection for the 21st century. Xamax Consultancy Pty Ltd; January 2000. At: http://www.rogerclarke.com/DV/PP21C.html.

Clarke R. What's 'privacy'?. Workshop presentation for the Australian Law Reform Commission. Xamax Consultancy Pty Ltd; July 2006. At: http://www.rogerclarke.com/DV/Privacy.html.

Clarke R. The regulation of surveillance. Xamax Consultancy Pty Ltd; August 2007. At: http://www.rogerclarke.com/DV/SReg.html.

Clarke R. Business cases for privacy-enhancing technologies [chapter 7]. In: Subramanian R, editor. Computer security, privacy and politics: current issues, challenges solutions. IDEA Group; 2008a. pp. 135–55. PrePrint at: http://www.rogerclarke.com/EC/PETsBusCase.html.

Clarke R. Dissidentity: the political dimension of identity and privacy. Identity Inf Soc 2008b;1(1):221–8. At: http://www.rogerclarke.com/DV/Dissidentity.html.

Clarke R. The covert implementation of mass vehicle surveillance in Australia. In: Proceedings of the 4th workshop on the social implications of national security: covert policing. ANU; 2009a. April 2009, PrePrint at: http://www.rogerclarke.com/DV/ANPR-Surv.html.

Clarke R. A sufficiently rich model of (id)entity, authentication and authorisation. In: Proceedings of the IDIS 2009 – the 2nd multidisciplinary workshop on identity in the information society. London: LSE; 2009b. 5 June 2009, at: http://www.rogerclarke.com/ID/IdModel-090605.html.

Clarke R. A framework for surveillance analysis. Xamax consultancy Pty Ltd; 2009c. August 2009, at: http://www.rogerclarke.com/DV/FSA.html.

Clarke R. What is überveillance? (and what should be done about it?). IEEE Technol Soc Summer 2010;29(2):17–25. PrePrint at: http://www.rogerclarke.com/DV/RNSA07.html.

Clarke R. An evaluation of privacy impact assessment guidance documents. Int Data Priv Law March 2011;1(2):111–20. PrePrint at: http://www.rogerclarke.com/DV/PIAG-Eval.html.

Clarke R. Privacy and the media: extracts from media organisation codes of conduct. Xamax Consultancy Pty Ltd; 2012a. January 2012, at: http://www.rogerclarke.com/DV/PandM-Codes.html.

Clarke R. Surveillance by the Australian media, and its regulation. Xamax Consultancy Pty Ltd; 2012b. March 2012, at, http://www.rogerclarke.com/DV/MSR.html.

Clarke R. Privacy and the media – a platform for change? Univ WA Law Rev 2012c;36(1):158–98. PrePrint at: http://www.rogerclarke.com/DV/PandM.html.

Clarke R. The regulation of point of view surveillance: a review of Australian law. Working paper. Xamax Consultancy Pty Ltd; 2012d. August 2012, at:, http://www.rogerclarke.com/DV/POVSRA.html.

Clarke R. Privacy and the media – a normative analysis. Xamax Consultancy Pty Ltd; 2012e. December 2012, at, http://www.rogerclarke.com/DV/PMN.html.

Clarke R, Stevens K. Evaluation or justification? The application of cost/benefit analysis to computer matching schemes. In: Proceedings of the European conference in information systems (ECIS'97). Cork, Ireland, 19–21 June 1997, at: http://www.rogerclarke.com/SOS/ECIS97.html; 1997.

Clarke R, Wigan MR. You are where you've been: the privacy implications of location and tracking technologies. J Locat Based Serv December 2011;5(3–4):138–55. http://www.rogerclarke.com/DV/YAWYB-CWP.html.

CoE. Convention for the protection of individuals with regard to automatic processing of personal data. Council of Europe; January 1981. At: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Coffman K. Don't like drones? Folks in deer trail, Colorado mull paying citizens to shoot them down. Fairfax Media; 18 July 2013. At: http://www.theage.com.au/technology/technology-news/dont-like-drones-folks-in-deer-trail-colorado-mull-paying-citizens-to-shoot-them-down-20130718-2q5rd.html.

Corcoran M. Drone journalism takes off. ABC News. At: http://www.abc.net.au/news/2012-02-21/drone-journalism-takes-off/3840616; 21 February 2012.

Cullen FT, Gilbert KE. Reaffirming rehabilitation. Anderson Publishing; 2013.

DHS. Our service commitments. Australian: Department of Human Services; 2013. At: http://www.humanservices.gov.au/corporate/about-us/service-commitments/#sc-respect.

EC. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Eur Comm. At: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF; October 1995.

EC. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation). European Commission; January 2012. At: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

EC. Roadmap for the integration of civil RPAS into the European aviation system. European RPAS Steering Group; 20 June 2013. At: http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap_en.pdf.

EPIC. Unmanned planes offer new opportunities for clandestine government tracking. Electronic Privacy Information Center; August 2005. At: http://epic.org/privacy/surveillance/spotlight/0805/.

EPIC. Privacy & human rights 2006. Electronic Privacy Information Center; 2006.

EPIC. FAA to assess safety of drones in US airspace. EPIC alert 19.03, At: http://www.epic.org/alert/epic_alert_1903.html; 16 February 2012.

FAA. Unmanned aircraft system test site program – proposed rule document. Federal Aviation Administration; 2013a. 14 February 2013, At: http://www.regulations.gov/#!documentDetail;D=FAA-2013-0061-0001.

FAA. Integration of civil unmanned aircraft systems (UAS) in the national airspace system (NAS) roadmap. Federal Aviation Administration; 2013b. 7 November 2013, At: http://www.faa.gov/about/initiatives/uas/media/UAS_Roadmap_2013.pdf.

FAA. FAA selects unmanned aircraft systems research and test sites. Federal Aviation Administration; 2013c. 30 December 2013, At: http://www.faa.gov/news/press_releases/news_story.cfm?newsId=15576.

Farber H. Eyes in the sky: constitutional and regulatory approaches to domestic drone deployment. Syracuse Law Rev 2014;64(1). PrePrint At: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2350421.

Finkelstein. Report of the inquiry into the media and media regulation. The Hon R Finkelstein QC assisted by Prof M Ricketson. Department of Broadband, Communications and the Digital Economy; 28 February 2012. At:, http://www.dbcde.gov.au/__data/assets/pdf_file/0006/146994/Report-of-the-Independent-Inquiry-into-the-Media-and-Media-Regulation-web.pdf.

Finn RL, Wright D. Unmanned aircraft systems: surveillance, ethics and privacy in civil applications. Comput Law Secur Rev April 2012;28(2):184–94.

Foucault M. Discipline and punish: the birth of the prison. Penguin; 1975. 1979.

Gandy OH. The panoptic sort: critical studies in communication and in the cultural industries. Boulder, CO: Westview; 1993.

Gaudin J. Raciti v Hughes (NSW). Priv Law Policy Rep September 1996;2(10):192.

Gogarty B, Hagger M. The laws of man over vehicles unmanned: the legal response to robotic revolution on sea, land and air. J Law Inf Sci 2008;5(19):73. At: http://www.austlii.edu.au/cgi-bin/sinodisp/au/journals/JlLawInfoSci/2008/5.html.

Goldberg D, Corcoran M, Picard RG. Remotely piloted aircraft systems & journalism: opportunities and challenges of drones in news gathering. Reuters Institute for the Study of Journalism; June 2013. At: https://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/Working_Papers/Remotely_Piloted_Aircraft_and_Journalism.pdf.

Gorman S, Dreazen YJ, Cole A. Insurgents hack U.S. drones. Wall Str J. At: http://online.wsj.com/news/articles/SB126102247889095011; 17 December 2009.

Greenleaf G. Sheherezade and the 101 data privacy laws: origins, significance and global trajectories. J Law Inf Sci. At: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877#%23; 2013.

Greenleaf G. Asian Data Privacy Laws: Trade and Human Rights Perspectives. Oxford University Press; 2014. forthcoming.

Hayes B, Jones C, Toepfer E. Eurodrones Inc. Statewatch; 2014. February 2014, At: http://www.statewatch.org/news/2014/feb/.

HoL. Surveillance: citizens and the state. Second report. UK: House of Lords Constitution Committee; January 2009. At:, http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm.

Hyland T. Police seek bigger picture in using drones but libertarians incensed. Fairfax Media; 13 May 2012. At: http://www.smh.com.au/technology/technology-news/police-seek-bigger-picture-in-using-drones-but-libertarians-incensed-20120512-1yjgy.html.

IACP. Recommended guidelines for the use of unmanned aircraft. International Association of Chiefs of Police; August 2012. At: http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf.

ICO. CCTV code of practice. UK: Information Commissioner's Office; 2008. At: http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf.

IPP. Information privacy principles. Embodied in s.14 of the Privacy Act (Cth); 1988. At: http://www.privacy.org.au/Resources/IPPs-140311.pdf.

JAA. Joint JAA/EUROCONTROL initiative on UAV/ROAs: final report. Joint Aviation Authorities; At: http://www.easa.europa.eu/rulemaking/docs/npa/2005/16-2005/NPA_16_2005_Appendix.pdf; 11 May 2004.

Kontominas B. Security scare as drone hits bridge. The Sydney Morning Herald. At: http://www.smh.com.au/nsw/mystery-drone-collides-with-sydney-harbour-bridge-20131004-2uzks.html; 5 October 2013.

Kyriacou K. Queensland police to trial hi-tech surveillance drones to chase criminals. The Courier-Mail. At: http://www.news.com.au/technology/attack-of-the-drones/story-e6frfro0-1226298835589; 14 March 2012.

Leveson. An inquiry into the culture, practices and ethics of the press: report. The Leveson Inquiry; 29 November 2012. UK official doc no. 0780 2012–2013, At: http://www.official-documents.gov.uk/document/hc1213/hc07/0780/0780.asp.

LL. Drone crash into Sydney Harbour Bridge causes security incident. Liveleak.com; 26 November 2013. At: http://www.liveleak.com/view?i=661_1385456831.

Lyon D. The electronic eye: the rise of surveillance society. Polity Press; 1994.

Mann S. Wearable, tetherless, computer-mediated reality (with possible future applications to the disabled). Technical report #260. Cambridge, Massachusetts: M.I.T. Medial Lab Perceptual Computing Section; 1994. At:, http://wearcam.org/mr.html.

Mann S. An historical account of the 'WearComp' and 'WearCam' inventions developed for applications in 'personal imaging'. In: Proceedings of the ISWC. pp. 66–73. 13–14 October 1997, Cambridge, Massachusetts. At: http://www.wearcam.org/historical/; 1997.

Mann S. Equiveillance: the equilibrium between sur-veillance and sous-veillance. Opening address. In: Computers, freedom and privacy. At:, http://wearcam.org/anonequity.htm; 2005.

Mann S. Sousveillance: wearable computing and citizen 'undersight' – watching from below rather than above. h+ Mag. At: http://www.hplusmagazine.com/articles/politics/sousveillance-wearable-computing-and-citizen-undersight; 10 July 2009.

Mann S, Nolan J, Wellman B. Sousveillance: Inventing and using wearable computing devices…. Surveil Soc 2003;1(3):331–55. At: http://www.surveillance-and-society.org/articles1(3)/sousveillance.pdf.

Mann S, Fung J, Lo R. Cyborglogging with camera phones: steps toward equiveillance. In: Proceedings of the MM'06. October 23–27, 2006, Santa Barbara, California, At: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.1418&rep=rep1&type=pdf; 2006.

Masters A, Michael K. Lend me your arms: the use and implications of humancentric RFID. Electron Commer Res Appl Spring 2007;6(1):29–39.
MEAA. Media alliance code of ethics. Media Entertainment and Arts Alliance; 1996. Undated but apparently of November 1996, At: http://pda.alliance.org.au/code-of-ethics.html.
Michael K, Clarke R. Location and tracking of mobile devices: überveillance stalks the streets. Comput Law Secur Rev June 2013;29(3):216–28. At: http://www.rogerclarke.com/DV/LTMD.html.
Morison WL. Report on the law of privacy. Sydney: University of Sydney; 1973.
Moses A. Privacy watchdog urges debate on aerial drones. Fairfax; 12 September 2012. At: http://www.smh.com.au/technology/technology-news/privacy-watchdog-urges-debate-on-aerial-drones-20120912-25ri4.html.
Moses A. Privacy fears as drones move into mainstream. Fairfax Media; 18 February 2013. At: http://www.theage.com.au/technology/technology-news/privacy-fears-as-drones-move-into-mainstream-20130217-2elcj.html.
Nairn J. Curtain drawn on ADFA shower case. ABC News. At: http://www.abc.net.au/news/2012-07-25/charges-dropped-against-adfa-cadet/4153292; 25 July 2012.
Nemeth A. NSW photo rights: Australian street photography legal issues. Andrew Nemeth; 2005. At: http://photorights.4020.net/.
News Ltd. Professional conduct policy. News Limited. At: http://media.crikey.com.au/wp-content/uploads/2011/07/NewsLimited_ProfessionalCoC.pdf, mirrored at: http://www.rogerclarke.com/DV/NewsLimited_ProfessionalCoC.pdf; March 2006.
NineMSN. Drone crashes into Sydney Harbour Bridge. NineMSN. At: http://news.ninemsn.com.au/national/2013/11/26/18/26/drone-crashes-into-sydney-harbour-bridge; 26 November 2013.
NPP. National privacy principles. Embodied in schedule 3 of the Privacy Act (Cth), 1988. At: http://www.privacy.org.au/Resources/NPPs-140311.pdf.
NSWLRC. Surveillance: final report. Report 108. NSW Law Reform Commission; May 2005. At:, http://www.lawreform.lawlink.nsw.gov.au/lrc/reportsmain/LRC_r108bib.html.
OECD. OECD guidelines on the protection of privacy and transborder flows of personal data. Organisation for Economic Cooperation and Development; 1980. At: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
OIC. Privacy and drone technology. Queensland: Office of the Information Commissioner; April 2013. At: http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-drone-technology.
PSDJ. Code of ethics. Professional Society of Drone Journalists; 2013. Undated, but apparently of 2013, At: http://www.dronejournalism.org/code-of-ethics.
Simons M. NotW: Hartigan weighs in … but more boots to drop, some of them here. Crikey. 8 July 2011, at: http://www.crikey.com.au/2011/07/08/notw-john-hartigan/; 2011a.
Simons M. More on the News Limited code of professional conduct, and knowledge of same. Crikey. 9 July 2011, At: http://blogs.crikey.com.au/contentmakers/2011/07/09/more-on-the-news-limited-code-of-professional-conduct-and-knowledge-of-same/; 2011b.
Simons M. Simons: News Ltd gets smart and lifts the code of silence. Crikey. 12 July 2011, At: http://www.crikey.com.au/2011/07/12/code-of-conduct-news-limited/; 2011c.
Simons M. Mastering a code of conduct means pushing it hard. Crikey. 26 July 2011, at: http://www.crikey.com.au/2011/07/26/simons-mastering-a-code-of-conduct-means-pushing-it-hard/; 2011d.
Solove DJ. A taxonomy of privacy. Univ Pa Law Rev January 2006;154(3):477–560.
T&D. Animal rights group says drone shot down. T&D; 14 February 2012. At: http://thetandd.com/animal-rights-group-says-drone-shot-down/article_017a720a-56ce-11e1-afc4-001871e3ce6c.html.
Thompson II R.M. Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses. US Congressional Research Service 7-5700, 3 April 2013, At: http://www.fas.org/sgp/crs/natsec/R42701.pdf; 2013.
Vallesenor J. Observations from above: unmanned aircraft systems and privacy. Harv J Law Public Policy 2013;36(2):457–517.
VIPP. Information privacy principles. Embodied in schedule 1 of the Information Privacy Act (Vic), At: http://www.austlii.edu.au/au/legis/vic/consol%5fact/ipa2000231/sch1.html; 2000.
VLRC. Surveillance in public places: final report. Victorian Law Reform Commission; 2010. August 2011, At: http://www.lawreform.vic.gov.au/projects/surveillance-public-places/surveillance-public-places-final-report.
Warren S, Brandeis LD. The right to privacy. Harv Law Rev 1890;4:193–220. At: http://athena.louisville.edu/library/law/brandeis/privacy.html.
Wigan MR, Clarke R. Social impacts of transport surveillance. Prometheus December 2006;24(4):389–403. At: http://www.rogerclarke.com/DV/SITS-0604.html.
Wright D, De Hert P, editors. Privacy impact assessments. Springer; 2012.
Wright D, Raab CD. Constructing a surveillance impact assessment. Comput Law Secur Rev December 2012;28(6):613–26.
Wright D, Friedewald M, Gutwirth S, Langheinrich M, Mordini E, Bellanova R, et al. Sorting out smart surveillance. Comput Law Secur Rev July 2010;26(4):343–54.

## TABLE OF STATUTES

### AUSTRALIA

Air Navigation Regulations 1947 (Cth). http://www.austlii.edu.au/au/legis/cth/consol_reg/anr1947257/.
Anti-Terrorism Act 2004 (Cth) http://www.austlii.edu.au/au/legis/cth/consol_act/aa2004187/.
Crimes Act 1914 (Cth) http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/.
Defence Act 1903 (Cth) http://www.austlii.edu.au/au/legis/cth/consol_act/da190356/.
Privacy Act 1988 (Cth) http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/.
Surveillance Devices Act 2004 (Cth) http://www.austlii.edu.au/au/legis/cth/consol_act/sda2004210/.

### NSW

Civil Liability Act 2002 (NSW) http://www.austlii.edu.au/au/legis/nsw/consol_act/cla2002161/.
Crimes Act 1900 (NSW) http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/index.html.
Crimes (Domestic And Personal Violence) Act 2007 (NSW) http://www.austlii.edu.au/au/legis/nsw/consol_act/capva2007347/.
Law Enforcement (Powers & Responsibilities) Act 2002 (NSW) http://www.austlii.edu.au/au/legis/nsw/consol_act/leara2002451/.

Sydney Harbour Foreshore Authority Regulation 2011 (NSW) http://www.austlii.edu.au/au/legis/nsw/consol_reg/shfar2011502/.
Surveillance Devices Act 2007 (NSW) http://www.austlii.edu.au/au/legis/nsw/consol_act/sda2007210/.

VICTORIA

Personal Safety Intervention Orders Act 2010 (Vic) http://www.austlii.edu.au/au/legis/vic/consol_act/psioa2010409/.
Wrongs Act 1958 (Vic) http://www.austlii.edu.au/au/legis/vic/consol_act/wa1958111/.

NEW ZEALAND

Search and Surveillance Act 2012 (NZ).

TABLE OF CASES

R v McDonald and Deblaquiere [2013] ACTSC 122 (27 June 2013) http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/act/ACTSC/2013/122.html.