The Regulation of Civilian Drones' Applications to the Surveillance of People

Review Version of 9 January 2014

Roger Clarke **

This document is at http://www.rogerclarke.com/SOS/Drones-BP.html

This is the fourth in a series of papers on drones: 1, 2, 3, 4

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 identified, together with means whereby they may come into being.

Contents

---

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 adapting very slowly in comparison with the rapid progress in drone capabilities and economics, 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 constructs 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. Its excludes surveillance of people in war-zones - a topic that is already copiously addressed in the literature. Its scope is applications in civilian contexts, up to and including para-military uses by law enforcement and national security agencies, such as border protection and the observation of civil unrest. The paper's purpose is to examine the extent to which current regulatory regimes appear to cope with the use of drones to conduct such surveillance.

This paper 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-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 long standing, 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 & 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, 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 carry Automated Number Plate Recognition (ANPR) capability, and those that transmit real-time video of sufficient quality to enable a human operator to visually recogise their quarry and associate the recording with an identified individual. Near-future prospects include tracking of devices carrying RFID-chips, including lorries, anklets imposed on `open prisoners', and animals, including humans.

Some drone activities, above and beyond their real-time impact on behaviour, give rise to threats to individuals in the form of retrospective exposure. The threats involve:

- additional collection, storage, use and disclosure of data about individuals
- interception of data-flows, e.g. of surveillance video transmissions (Gorman et al. 2009)
- retention of data
- 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
- unauthorised access to stored data
- exploitation of the data in conjunction with other data
- increased access by law enforcement agencies, 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, as live feeds and real-time surveillance, and just-in-case

Since the 1970s, data protection laws (sometimes misleadingly referred to as privacy laws) have been enacted in most countries (Greenleaf 2013). Moderate protections exist in Europe, and various, generally weak protections exist in other countries. The inadequacies are exacerbated by drones. This was the focus of a previous article in Computer Law & Security Review (Finn & Wright 2012).

A close cousin to data privacy is privacy of personal communications, which relates to ephemeral rather than stored data. 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 about individuals such as facial images and emanations from implants, including physical identifiers - usefully referred to as `entifiers' (Clarke 2009a). However, it is the two remaining dimensions of privacy that are the primary focus in this paper, because they encompass the interests that are most directly impinged upon by 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. Like any other privacy interest, this is subject to a wide range of conflicts with other interests of the individual, and 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).

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 & 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 both behaviour in private places and 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.

Until recently, the four dimensions discussed above had provided a sufficient basis for analysis. However, the 21st century has brought technological change 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 electronically (through recording of 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.

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 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. The target may be an object, an area, or one or more people (Wigan & 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). There is a substantial literature on surveillance, but a considerable proportion of it is sociological in nature or heavily intellectualised and lacks analytical clarity, or is technical and highly specific.

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. Communications surveillance focusses on written communications, listening to conversations, and access to various kinds of electronic messaging. Data surveillance observes transactions and exploits stored data. Tracking is a specialised form, combining physical surveillance of individuals with data surveillance. Since the late twentieth century, tracking has become so intrusive and pervasive that it requires treatment in its own right (Clarke 1999, Clarke & Wigan 2011, Michael & Clarke 2013). Body surveillance involves monitoring of aspects of the person's physical self (Masters & Michael 2007).

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 watch-towers over individuals in institutions. As the forms of surveillance have proliferated, the notion of superiority has been applied in 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 `sousveiilance' - 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 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 ('neighbourhood watch')
- journalism, as performed by the investigative professional media, focussed on 'the public interest'
- informal journalism and investigation, particularly for environmental and social purposes
- voyeurnalism, as performed by `tabloid media', focussed 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) technology, 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 (and audio)
- fixed cameras with known positions and orientations
- mobile cameras with measured or computed positions and orientations
- cameras embodied in other artefactssuch as a baton, a pistol, a mobile-phone
- triggering of 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. 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 gather structured data (e.g. vehicle registration numbers). 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, 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, but the primary focus is on 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 and recording in more places, which is akin to harassment
2. **Intensity**
   Individuals are subjected to scrutiny for longer periods, more closely, and in high-resolution, which is akin to stalking. Observation that is frequent, continual and even continuous is deeply intrusive into personal space. 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
   - Stereo and 3-D shots can be achieved
   - 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
   - Pursuits stimulate avoidance manoeuvres that may be frantic and ill-judged
4. **'The Panoptic Aloft'**
   - Law enforcement agencies apply military technologies, in ways not attuned to human rights
   - 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 & Gilbert (2013)
   - Drones make it practicable and economic for vigilantes to mount an intensive and extensive 'neighbourhood watch'
   - Drones enable practicable and economic implementation of 'mobile nagging aunties', which 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
   - The deterrent value in relation to serious forms of misbehaviour is limited, 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 primary deterrent effect that is likely to be achieved is the chilling of lawful social, economic, cultural and political behaviours
   - The potential retributional value of surveillance is entirely dependent on the availability and application of resources, close to the relevant incident in both time and space, to identify, locate and bring to justice the perpetrators of each crime and misdemeanour
5. **Errors**
   Much surveillance is conducted from a single perspective and with limited context, resulting in inferences that are apparently reasonable, but 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 Intrinsic Controls**
   Drones empower pilots and/or operators of onboard facilities to engage in voyeurism, harassment, stalking, and even acts of gratuitous violence. In addition, they are remote from the target, and are in the virtual reality created by their data-feeds. Their detachment from physical reality weakens the constraints of conscience, and loosens at least some of the psychological and social constraints that apply 'in meatspace'
8. **Surreptitiousness**
   In many circumstances, 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 & 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.

Questions that need to be addressed include:

- To what extent is surveillance 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 (from below, performed by a person) in comparison with surveillance (i.e. from above, 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, proved 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, all 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 & Hagger (2008) and Finn & Wright (2012).

The section commences by reviewing natural controls, 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, including aviation regulations, but narrowing in on privacy laws and on 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 image-quality, precision of drone control and of camera control, reliability of image-capture and -transmission, mis-identification 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 beset all aircraft, including a variety of aspects of weather, disturbances of the atmosphere in particular by volcanic eruptions, physical congestion of airspace by terrestrial artefacts such as buildings, cranes and powerlines, and by mobile artefacts such as 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. Risk of loss of a valuable aircraft is a strong disincentive to conducting surveillance, and risk of even injury let alone loss of life 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 easily manipulated to fit with the strategic intent of powerful players within executive teams, however. In addition, studies in such areas as data matching, biometrics and body scanning have located little evidence of cost/benefit analysis being undertaken (Clarke & 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 fails to address 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 is 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 just doesn't care about 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 regulatory agency, 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. Generally, 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 in the short term, and enable the gathering of experience to inform the development of a formal regulatory regime that is both effective and efficient?

(1) Organisational Self-Regulation

Organisations might exercise self-restraint. This could be influenced by professional norms, or by an appreciation of the delicacy 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.

Organisational self-restraint may be evidenced through the publication of a Customer Charter or a Code of Conduct. Most such company 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 more 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 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. The 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 most comprehensive and the most protective of the interests of people subjected to media attention (Clarke 2012a).

Unfortunately, that was where the warm glow came to an end, because it was comprehensively demonstrated that the 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, 2011b, 2011c, 2011d).

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.

(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 association of Australian Certified UAV Operators (ACUO), formed in 2009-10, has no Code of any kind; and the US association's Code 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.

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. However, no substantial collective of drone users was located.

A specialist group in the law enforcement field, the International Association of Chiefs of Police, has published an unenforceable set of `Recommended Guidelines' (IACP 2012). They are unenforceable, and hence have no direct bearing on operations. 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". In addition, 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 on-going 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"

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.

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 assocation 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, 2012c) show how far short the APC's Code (APC 2011a, 2011b) falls of a meaningful form of protection. 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 also 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 includes 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 related user organisations in drone usage, 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-regulative behaviour that would ensure protection of the interests of individuals.

(3) Co-Regulation

As described in the third paper in this series, co-regulation involves one or more Codes negotiated between a regulator and industry, 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.

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 privacy (Clarke 2012a, pp. 184-185), to the extent that even media commentators have expressed derision (e.g. Ackland 2011).

(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.

(1) Trespass

The lawful occupiers of land (i.e. owners or lessees) have a general right to prevent laws from being on their land, and from doing particular acts on their land, even if an area is freely accessible to 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 by 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 may be effective 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, nor from the air, whether by means of a piloted aircraft or a drone.

In any case, the interests of the aviation industry have been prioritised over those of citizens and consumers. Trespass and nuisance by aircraft are not actionable in at least NSW and Victoria, by virtue of the Civil Liability Act (NSW) s.72 and the Wrongs Act (Vic) s.30, provided that the aircraft's height is reasonable in the circumstances and in accordance with the Air Navigation Regulations (Cth). Similar provisions may exist in other Australian jurisdictions.

(2) Other Torts

Several other tortious remedies might have relevance in particular circumstances:

- nuisance (interference with a real estate occupant's quiet enjoyment of their property)
- 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 could be inferred)

However, all of these torts are very narrowly defined, and actions have to navigate minefields of arcane and ambiguous interpretations based on precedents whose facts are very different from those arising from drone surveillance. For example, the tort of nuisance cannot be used to deal with media to 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.

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 appears 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 & 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" (Clarke P.A. 2013).

(3) 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 a range of deficiencies. However, in 2007, the

AVO enabling provisions were moved from Part 15A of the Crimes Act to the Crimes (Domestic And Personal Violence) Act, which 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', stalking will seldom be able to be demonstrated by a litigant 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 exclude mainstream surveillance activities. 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) 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 seldom sufficiently specific to represent constraints on other parties' use of visual surveillance. Finn & Wright (2012, pp. 192-193) did, however, conclude 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.

In many countries, human rights are at best constitutionally implicit, but for the most part are merely matters of public policy. In Australia, 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.

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', but 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.

(5) 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 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 the terms of the relevant 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 forces 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 International Convention, 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. As a result, aviation laws contain little or no

protection against aerial surveillance, and concerns such as privacy are out-of-scope for the regulatory agency.

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:
    - disablement of the drone, causing it, or parts of its wreckage, to hit something else
    - a projectile aimed at the drone hitting something else

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 extended its Test Site Program beyond safety issues to encompass privacy concerns (FAA 2013). 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).

In Europe, JAA (2004) was exclusively concerned with safety aspects of drones, 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.

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

4.5 Privacy Law

A great many `privacy laws' have been enacted since 1970, throughout the world. They are, however, constrained by the `fair information practices' (FIPs) model, which 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 `behavioural privacy'.

Data protection laws could 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 2013 - which states solely that "personal data must be [collected] fairly" (EU 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 following:

- within the set of Information Privacy Principles (IPP 1988), which has been applicable to government agencies from 1989 to 2014 (emphases added):
  - IPP1.2 states that "Personal information shall not be collected by a collector by ... unfair means"
  - 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
- within the set of National Privacy Principles (NPP 2000), which has been applicable to many organisations in the private sector from 2001 to 2014 (emphases added):
  - NPP1.2 states that "An organisation must collect personal information only by ...fair means and not in an unreasonably intrusive way"

Data privacy protections in Australia were greatly weakened by amendments in 2012, which take effect in March 2014. In drafting the Act, 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 5,000-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 is encompassed by the Principles. Some functions, on the other hand, relate to privacy more generally, such as "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 functions. Quite simply, the use of drones for surveillance by Australian government agencies and corporations is not subject to any formal privacy law, and the Privacy Commissioner acts as though such the topics were outside his purview.

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. 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 Victorian government agencies will shortly conduct a campaign to remove the protections that have been nominally afforded by Victorian law.

A similar analysis of the privacy Principles applicable in every one of the hundred countries and many scores of subsidiary jurisdictions throughout the world might well 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.

This section commences by considering Australian statutes that have `surveillance' in their titles. Brief reviews are also provided of formal regulatory arrangements in relation to surveillance by the media, by law enforcement agencies, and finally by individuals.

(1) Surveillance Devices Laws

This section considers statutes that have `surveillance' or a similar term in the title, such as `Surveillance Devices Act', `Workplace Surveillance Act', or `Listening Devices Act'. It 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 reference 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 various protections, in various but in all cases tightly-defined circumstances. Broadly, visual and/or aural surveillance of a `private activity' is likely to be illegal. However, activity is `private activity' only in a very limited set of circumstances. 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 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 create 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 broadcast to colleagues video of a sex act performed with another cadet who was unaware of the

filming and transmission. Such behaviour appears to be generally regarded 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. 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.

(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 that, at least in Australia and the UK, the collection activities of the tabloid media are subject to seriously inadequate natural controls and self-regulatory, industry self-regulatory and co-regulatory regimes. Unfortunately, there appear to be virtually no formal regulatory arrangements in place to make up for that shortfall.

The Australian private sector is about to be 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 Privacy Act (Cth). The Australian Law Reform Commission recognised that a problem existed, and recommended the creation of a statutory tort, or 'privacy cause of action' (ALRC 2008b), but failed to recommend any material change to Privacy Act exemption (ALRC 2008a). 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).

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.

(3) Law Enforcement Use of Surveillance Devices

There will without doubt be many law enforcement uses of drones 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 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 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 that "there is no entry to premises without permission and no interference with any vehicle or thing"
- 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, and warrants 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 2011 `counter-terrorism' statutes, almost none of which have been justified, but none of which have yet been repealed
- all State and Territory jurisdictions have empowered their own law enforcement agencies to use surveillance and tracking devices

There is serious concern about the lack of meaningful and transparent evaluation of proposals, and of pre- and post-controls over the applications and the exercise of authorisation power. 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) 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 variety 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. 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). 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, posted the footage captured from the flight, and identified himself to the NSW Police, who returned the drone wreckage to him (NineMSN 2013). No report of a prosecution has been located.

More generally, government agencies have an interest in denying the public the right to apply visual surveillance against them. Such laws have not merely been mooted, drafted and implemented for short periods in relation to specific events such as G8 and APEC meetings, but have even been granted to law enforcement agencies 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 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.

(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 signficance 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 2010). The Victorian Parliament has either failed to notice, or chosen to ignore, Recommendations on the subject by its own Law Reform Commission (VLRC 2005). 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 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. It could well be accidentally applied 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 & 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, UK, Germany, Switzerland, Canada, 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 of people is invasive of behavioural privacy and experiential privacy. Drones greatly increase the invasiveness of visual surveillance, and with it the level of the privacy threat. 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 is not in evidence, and in principle 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 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 focussed 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 even empowered to contribute meaningfully to policy development in this area. Laws addressing surveillance specifically are largely intended to authorise surveillance by law enforcement agencies, and such privacy protections 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 the agency deems it to be inconvenient to them.

A rational approach to the problem is of course realiy specified. In order to address drone surveillance threats, proposals need to be subjected to prior evaluation and justification. The evaluations need 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, 2009b) and Wright & Raab (2012). Designs need to be proportionate and to incorporate mitigating 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 and educative value. 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 12.

At present, Australia has no arrangements in place in relation to surveillance that warrant a name 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. (2011a) 'Muddle-headed watchdog leaves the privacy door ajar' Opinion, The Sydney Morning Herald, 18 February 2011, at http://www.smh.com.au/opinion/society-and-culture/muddleheaded-watchdog-leaves-the-privacy-door-ajar-20110217-1ay3h.html

ACLU (2011) '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 (2008a) '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

ALRC (2008b) '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

APC (2011a) 'General Statement of Principles', Australian Press Council, Date of Origin unclear, no prior versions visible, current version dated August 2011, at http://www.presscouncil.org.au/general-principles/

APC (2011b) 'Statement of Privacy Principles', Australian Press Council, Date of Origin unclear, no prior versions visible, current version dated August 2011, at http://www.presscouncil.org.au/privacy-principles/

APF (2009) 'APF Policy Statement re Visual Surveillance, incl. CCTV' Australian Privacy Foundation, original version of September 2009, at http://www.privacy.org.au/Papers/CCTV-1001.html

APF (2013) 'APF's Meta-Principles for Privacy Protection' Australian Privacy Foundation, March 2013, at http://www.privacy.org.au/Papers/PS-MetaP.html

APP (2012) `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

ATO (2013) `Taxpayers' charter' Australian Taxation Office, 2013, at http://www.ato.gov.au/About-ATO/Access,-accountability-and-reporting/Informing-the-community/Taxpayers--charter/

AUVSI (2012) 'Industry Code of Conduct' Association for Unmanned Aircraft System Operation, undated, but released July 2012, at http://www.auvsi.org/conduct

AUVSI (2013) `Unmanned Aircraft Systems Privacy Statement' Association for Unmanned Aircraft System Operation, undated, but apparently of 2013, at http://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/UnmannedAircraftSystemPrivacyStatementFinal.pdf

Bathurst T.F. (2013) `Opening Remarks' Proc. 32nd Conf. Annual Aviation Law Association of Australia & New Zealand (ALAANZ), Sydney, 6 May 2013, at http://www.supremecourt.lawlink.nsw.gov.au/agdbasev7wr/_assets/supremecourt/m6700011771004/bathurs

BBC (2013) 'Google chief urges action to regulate mini-drones' BBC News, 13 April 2013, at http://www.bbc.co.uk/news/technology-22134898

Bear G. (2010) 'Little Brother is Watching', Communications of the ACM 53, 9 (September 2010) 111-112

CASA (2013) "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

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

Clarke R. (1988) `Information Technology and Dataveillance' Comm. ACM 31,5 (May 1988) Re-published in C. Dunlop and R. Kling (Eds.), 'Controversies in Computing', Academic Press, 1991, at http://www.rogerclarke.com/DV/CACM88.html

Clarke R. (1997) `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. (1999) 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications' Proc. 21st International Conf. Privacy and Personal Data Protection, Hong Kong, September 1999. Revised version published in Info. Techno. & People 14, 1 (2001) 206-231, at http://www.rogerclarke.com/DV/PLT.html

Clarke R. (2000) '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. (2006) '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. (2007) 'The Regulation of Surveillance' Xamax Consultancy Pty Ltd, August 2007, at http://www.rogerclarke.com/DV/SReg.html

Clarke R. (2008a) 'Business Cases for Privacy-Enhancing Technologies' Chapter 7 in Subramanian R. (Ed.) 'Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions' IDEA Group, 2008, pp. 135-155, at http://www.rogerclarke.com/EC/PETsBusCase.html

Clarke R. (2008b) `Dissidentity: The Political Dimension of Identity and Privacy' Identity in the Information Society 1, 1 (December, 2008) 221-228, at http://www.rogerclarke.com/DV/Dissidentity.html

Clarke R. (2009a) 'A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation' Proc. IDIS 2009 - The 2nd Multidisciplinary Workshop on Identity in the Information Society, LSE, London, 5 June 2009, at http://www.rogerclarke.com/ID/IdModel-090605.html

Clarke R. (2009b) 'A Framework for Surveillance Analysis' Xamax Consultancy Pty Ltd, August 2009, at http://www.rogerclarke.com/DV/FSA.html

Clarke R. (2010) 'What is Überveillance? (And What Should Be Done About It?)' IEEE Technology and Society 29, 2 (Summer 2010) 17-25, at http://www.rogerclarke.com/DV/RNSA07.html

Clarke R. (2012a) `Privacy and the Media: Extracts from Media Organisation Codes of Conduct' Xamax Consultancy Pty Ltd, January 2012, at http://www.rogerclarke.com/DV/PandM-Codes.html

Clarke R. (2012b) `Surveillance by the Australian Media, and Its Regulation' Xamax Consultancy Pty Ltd, March 2012, at http://www.rogerclarke.com/DV/MSR.html

Clarke R. (2012c) `Privacy and the Media - A Platform for Change?' Uni of WA Law Review 36, 1 (June 2012) 158-198, at http://www.rogerclarke.com/DV/PandM.html

Clarke R. (2012d) 'The Regulation of Point of View Surveillance: A Review of Australian Law' Working Paper, Xamax Consultancy Pty Ltd, August 2012, at http://www.rogerclarke.com/DV/POVSRA.html

Clarke R. (2012e) `Privacy and the Media - A Normative Analysis' Xamax Consultancy Pty Ltd, December 2012, at http://www.rogerclarke.com/DV/PMN.html

Clarke R. & Stevens K. (1997) `Evaluation Or Justification? The Application Of Cost/Benefit Analysis To ?Computer Matching Schemes' Proc. European Conference in Information Systems (ECIS'97), Cork, Ireland, 19-21 June 1997, at http://www.rogerclarke.com/SOS/ECIS97.html

Clarke R. & Wigan M.R. (2011) 'You Are Where You've Been: The Privacy Implications of Location and Tracking Technologies' Journal of Location Based Services 5, 3-4 (December 2011) 138-155, at http://www.rogerclarke.com/DV/YAWYB-CWP.html

CoE (1981) `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. (2013) '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. (2012) 'Drone journalism takes off' ABC News, 21 February 2012, at http://www.abc.net.au/news/2012-02-21/drone-journalism-takes-off/3840616

Cullen F.T. & Gilbert K.E. (2013) `Reaffirming Rehabilitation' Anderson Publishing, 2013

DHS (2013) `Our Service Commitments' [Australian] Department of Human Services, 2013, at http://www.humanservices.gov.au/corporate/about-us/service-commitments/#sc-respect

EC (1995) `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' European Commission, October 1995, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF

EC (2012) `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 (2013) '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 (2005) 'Unmanned Planes Offer New Opportunities for Clandestine Government Tracking' Electronic Privacy Information Center, August 2005, at http://epic.org/privacy/surveillance/spotlight/0805/

EPIC (2012) 'FAA to Assess Safety of Drones in US Airspace' EPIC Alert 19.03, 16 February 16 2012, at http://www.epic.org/alert/epic_alert_1903.html

FAA (2013a) 'Unmanned Aircraft System Test Site Program - Proposed Rule Document' Federal Aviation Administration, 14 February 2013, at http://www.regulations.gov/#!documentDetail;D=FAA-2013-0061-0001

FAA (2013b) 'Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap' Federal Aviation Administration, 7 November 2013, at http://www.faa.gov/about/initiatives/uas/media/UAS_Roadmap_2013.pdf

Finkelstein (2012) '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 R.L. & Wright D. (2012) 'Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications' Computer Law & Security Review 28, 2 (April 2012) 184-194

Gandy O.H. (1993) 'The Panoptic Sort: Critical Studies in Communication and in the Cultural Industries' Westview, Boulder CO, 1993

Goldberg D., Corcoran M. & Picard R.G. (2013) 'Remotely Piloted Aircraft Systems & Journalism: Opportunities and Challenges of Drones in News Gathering' Reuters Institire for the Study of Journalism, June 2013 , at https://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/Working_Papers/Remotely_Pilot

Gogarty B. & Hagger M. (2008) `The Laws of Man Over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air' Journal of Law, Information and Science 5, 19 (2008) 73, at http://www.austlii.edu.au/au/journals/JlLawInfoSci/2008/5.html

Gorman S., Dreazen Y.J. & Cole A. (2009) ' Insurgents Hack U.S. Drones' Wall Street Journal, 17 December 2009, at http://online.wsj.com/news/articles/SB126102247889095011

Greenleaf G. (2013) `Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' Journal of Law, Information & Science (2013), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877#%23

HoL (2009) `Surveillance: Citizens and the State' [UK] House of Lords Constitution Committee - Second Report, January 2009, at http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm

Hyland T. (2012) `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 (2012) '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 (2008) `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_Pro

IPP (1988) `Information Privacy Principles', embodied in s.14 of the Privacy Act (Cth), at http://www.austlii.edu.au/au/legis/cth/consol%5fact/pa1988108/s14.html

JAA (2004) `Joint JAA/EUROCONTROL Initiative on UAV/ROAs: Final Report' 11 May 2004, at http://www.easa.europa.eu/rulemaking/docs/npa/2005/16-2005/NPA_16_2005_Appendix.pdf

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

Kyriacou K. (2012) `Queensland Police to trial hi-tech surveillance drones to chase criminals' The Courier -Mail, 14 March 2012, at http://www.news.com.au/technology/attack-of-the-drones/story-e6frfro0-1226298835589

Leveson (2012) 'An inquiry into the culture, practices and ethics of the press: report' The Leveson Inquiry, UK Official Document No 0780 2012-13, 29 November 2012, at http://www.official-documents.gov.uk/document/hc1213/hc07/0780/0780.asp

Lyon D. (1994) `The Electronic Eye: The Rise of Surveillance Society' Polity Press, 1994

Mann S. (1994) `Wearable,Tetherless, Computer-Mediated Reality (with possible future applications to the disabled)' Technical Reporti #260, M.I.T. Medial Lab Perceptual Computing Section, Cambridge, Massachusetts, 1994, at http://wearcam.org/mr.html

Mann S. (1997) 'An historical account of the 'WearComp' and 'WearCam' inventions developed for applications in 'Personal Imaging" Proc. ISWC, 13-14 October 1997, Cambridge, Massachusetts, pp. 66-73, at http://www.wearcam.org/historical/

Mann S. (2005) 'Equiveillance: The equilibrium between Sur-veillance and Sous-veillance' Opening Address, Computers, Freedom and Privacy, 2005, at http://wearcam.org/anonequity.htm

Mann S. (2009) 'Sousveillance: Wearable Computing and Citizen 'Undersight' - Watching from Below Rather Than Above' h+ Magazine, 10 July 2009, at http://www.hplusmagazine.com/articles/politics/sousveillance-wearable-computing-and-citizen-undersight

Mann S., Fung J. & Lo R. (2006) `Cyborglogging with camera phones: Steps toward equiveillance ` Proc. 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

Mann S., Nolan J. & Wellman B. (2003) 'Sousveillance: Inventing and Using Wearable Computing Devices...' Surveillance & Society 1, 3 (2003) 331-355, at http://www.surveillance-and-society.org/articles1(3)/sousveillance.pdf

Masters A. & Michael K. (2007) `Lend me your arms: the use and implications of humancentric RFID' Electronic Commerce Research and Applications 6, 1 (Spring 2007) 29-39

MEAA (1996) 'Media Alliance Code of Ethics' Media Entertainment and Arts Alliance, undated but apparently of November 1996, at http://pda.alliance.org.au/code-of-ethics.html

Michael K. & Clarke R. (2013) 'Location and Tracking of Mobile Devices: Überveillance Stalks the Streets' Computer Law & Security Review 29, 3 (June 2013) 216-228, at http://www.rogerclarke.com/DV/LTMD.html

Morison W.L. (1973) 'Report on the Law of Privacy' University of Sydney, Sydney 1973

Moses A. (2012) '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. (2013) '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. (2012) `Curtain drawn on ADFA shower case' ABC News, 25 July 2012, at http://www.abc.net.au/news/2012-07-25/charges-dropped-against-adfa-cadet/4153292

Nemeth A. (2005) 'NSW Photo Rights: Australian Street Photography Legal Issues' Andrew Nemeth, at http://photorights.4020.net/

News Ltd (2006) `Professional Conduct Policy' News Limited, March 2006, at http://media.crikey.com.au/wp-content/uploads/2011/07/NewsLimited_ProfessionalCoC.pdf, mirrored at http://www.rogerclarke.com/DV/NewsLimited_ProfessionalCoC.pdf

NineMSN (2013) `Drone crashes into Sydney Harbour Bridge' NineMSN, 26 November 2013, at http://news.ninemsn.com.au/national/2013/11/26/18/26/drone-crashes-into-sydney-harbour-bridge

NPP (2000) `National Privacy Principles', embodied in Schedule 3 of the Privacy Act (Cth), at http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch3.html

NSWLRC (2005) '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 (1980) `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/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpers

PSDJ (2013) 'Code of Ethics' Professional Society of Drone Journalists, undated, but apparently of 2013, at http://www.dronejournalism.org/code-of-ethics

Simons M. (2011a) `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/

Simons M. (2011b) `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/

Simons M. (2011c) `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/

Simons M. (2011d) `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/

Solove D.J. (2006) 'A Taxonomy of Privacy' University of Pennsylvania Law Review 154, 3 (January 2006) 477-560

T&D (2012) '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

Vallesenor J. (2013) 'Observations From Above: Unmanned Aircraft Systems And Privacy ' Harvard Journal of Law & Public Policy 36, 2 (2013) 457-517

VIPP (1988) `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

VLRC (2010) 'Surveillance in public places: Final report' Victorian Law Reform Commission, August 2011, at http://www.lawreform.vic.gov.au/projects/surveillance-public-places/surveillance-public-places-final-report

Warren S. & Brandeis L.D. (1890) 'The Right to Privacy' 4 Harvard Law Review (1890) 193-220, at http://athena.louisville.edu/library/law/brandeis/privacy.html

Wigan M.R. & Clarke R. (2006) `Social Impacts of Transport Surveillance' Prometheus 24, 4 (December 2006) 389 - 403, at http://www.rogerclarke.com/DV/SITS-0604.html

Wright D., Friedewald M., Gutwirth S., Langheinrich M., Mordini E., Bellanova R., de Hert P., Wadhwa K. & Bigo D. (2010) 'Sorting out smart surveillance' Computer Law & Security Review 26, 4 (July 2010) 343-54

Wright D. & Raab C.D. (2012) 'Constructing a surveillance impact assessment' Computer Law & Security Review 28, 6 (December 2012) 613-626

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/

Criminal Code (Cth)
http://www.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html

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/au/cases/act/ACTSC/2013/122.html

Author Affiliations

Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra. He is also a Visiting Professor in the Cyberspace Law & Policy Centre at the University of N.S.W., and a Visiting Professor in the Research School of Computer Science at the Australian National University.

From the site's beginnings in August 1994 until February 2009, the infrastructure was provided by the Australian National University. During that time, the site accumulated close to 30 million hits. It passed 40 million by the end of 2012.

Sponsored by Bunhybee Grasslands, the extended Clarke Family, Knights of the Spatchcock and their drummer

ACN: 002 360 456
78 Sidaway St,
Chapman ACT
2611 AUSTRALIA
Tel: +61 2 6288 6916

Created: 16 August 2013 - Last Amended: 9 January 2014 by Roger Clarke - Site Last Verified: 15 February 2009
This document is at www.rogerclarke.com/SOS/Drones-BP.html