Surveillance & Society

Article

Surveillance by the Australian Media, and its Regulation

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra, Australia | Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney, Australia | Visiting Professor in Computer Science, ANU, Canberra, Australia
Roger.Clarke@xamax.com.au

Abstract

The print and broadcast media make extensive use of surveillance in order to gather information for publication. It is vital to democracy that they do so. A proportion of the media's surveillance practices are, however, excessive and abusive of individuals' needs and reasonable expectations. An examination of Australian law shows that it provides almost no recourse against these excesses and abuses. Substantial change is necessary to create a regulatory environment in which balance is achieved.

1. Introduction

A free, effective and professional media has been a critical element within modern democracies. Considerable freedoms are, and must be, provided to the media to enable them to play a central role in the discovery of information, and in the provision of that information to the public.

On the other hand, the media has a substantial impact on the members of the public about whom it reports, and about whom it gathers information. As each new form of surveillance technology has emerged and matured, media organisations have considered the potential of the technology to assist in the media's functions. A variety of surveillance practices are used, such as ambush, pursuit and stake-out; and a variety of technologies have been adopted, including telephoto lenses, directional microphones, video-recording and auto-triggering devices.

The term 'the media' is used in this paper to refer to organisations that publish frequently, variously through print and broadcast channels and during the last decade increasingly also through telecommunications networks. The term also encompasses the employees and agents of media organisations, particularly reporters and photographers. A great deal of valuable investigative work is undertaken by parts of the media that are referred to by such positive terms as 'the broadsheets', 'quality journalism', 'news and current affairs' and 'documentaries'. Surveillance by investigative journalists doubtless gives rise to heartache on the part of the individuals subjected to it; but the professionalism is such that significant public disquiet seldom arises about the intrusions involved.

The same cannot be said for the use of surveillance by other media outlets. This paper uses the term 'tabloid media' to encompass newspapers, magazines, radio, television and electronic media that are much more concerned about 'what the public is interested in' than 'what is in the public interest'. The terms 'yellow press' and 'yellow journalism' were used in the USA a century ago, and the term 'sensationalist

Clarke, R. 2014. Surveillance by the Australian Media, and Its Regulation. *Surveillance & Society* 12(1): 89-107. http://www.surveillance-and-society.org | ISSN: 1477-7487

media' is used in the UK. The word 'voyeurnalism' is a concoction by this author, used in other publications arising from the same research project (Clarke 2012c). During the current decade, the UK has provided a great deal of evidence of inappropriate behaviour by tabloid media, documented in Leveson (2012).

The primary focus of the analysis is on 'official media'—the categories of individual who are issued passes to political, entertainment and sports events. On the other hand, the 'unofficial media' of bloggers and posters of videos needs to be considered as well. Sousveillance, used by the (hitherto) less powerful against the powerful, borders on surveillance by unofficial media. It appears very likely that limitations that are applicable to official media will need to be applied to unofficial media as well.

This paper is not concerned with the publication phase of media work, but only with the media's data-gathering activities, and in particular with its use of surveillance technologies. Little appears to have been published examining the regulation of media organisations' use of surveillance techniques and technologies. For example, nothing at all has been located in the first 11 volumes of *Surveillance & Society*. This paper sets out to fill that gap. It reports on part of a broader study that has been undertaken on 'privacy and the media' in Australia (Clarke 2012c).

The paper commences by defining a small empirical base to inform the analysis of the nature of surveillance undertaken by the media. It then reviews the current regulatory environment within which the media works, specifically within Australia, but with occasional observations about other jurisdictions. It finds that protections for the public against unjustifiable practices by the media are sorely lacking. The final section applies a set of general principles for the regulation of surveillance in order to articulate specific principles and standards. These provide a basis for the protection of members of the public, balanced against the legitimate needs of a free press.

2. Media Surveillance Practices

Several somewhat separate surveillance literatures exist. Technical disciplines are concerned with technologies that enable surveillance. Engineering disciplines are concerned with the surveillance of objects, including the use of RFID-tags on items moving through supply chains. Epidemiology tracks diseases and disease vectors, primary industries track livestock, and various environmental sciences track wildlife and monitor pollutants. Branches of the computing sciences focus on data collection and data mining, but also on de-identification and anonymity. A range of social sciences observe the effects of observation on psychological, social, economic and political behaviours. Historians study surveillance in past settings. The performing arts consider cultural impacts and opportunities. The archives of *Surveillance & Society* journal evidence many of these, but with a primary emphasis on the social sciences and a stated interest in transdisciplinary work.

This paper is concerned with the use of surveillance for the specific purpose of gathering data about people (rather than objects or locations), for publication in media outlets. Its primary concern is with physical surveillance of sight and sound, although other forms have relevance in particular circumstances. It is expressly instrumentalist in orientation, with a focus on existing regulation of media uses of surveillance. Because of the wide range of regulatory forms, the study is of necessity of a single country.

The remainder of this section presents the results of a survey of the use of surveillance by the media. The research method comprised the search for, and documentation and analysis of, a small set of cases that provide an empirical basis for the analysis. These are outlined in the first subsection. The second subsection then presents an evaluation of media behaviour, within an analytical framework previously developed by this author.

2.1 Empirical Approach

A search was undertaken of reports in Australian news media, between 2005 and 2011, in order to identify a manageably small but diverse set of instances of media surveillance. The search was performed on archives of media reports on privacy that are maintained by the Australian Privacy Foundation, complemented by reviews of the databases of the Australian Press Council (APC 2013; AustLII 2013) and the Australian Communications and Media Authority (ACMA 2013a). Google News is an ineffective search-tool for this purpose because almost every web-page contains the string 'privacy'. On the other hand, it was valuable as a means of identifying a range of media articles on each specific case. Table 1 lists the cases and key aspects of the practices and technologies involved. Descriptions and citations for these seven cases are in Clarke (2012c: s.3.2). No claims are made, or can be made, about randomness or comprehensiveness. The purpose was to enable the analytical component of the research to be undertaken with a sufficiently rich set of issues in view.

Table 1: Case Studies in Media Surveillance

- **Kidman** — January 2005
  Film star harassed by paparazzi, at her home, on the move, and in a park with her child
  Stake-out, listening device, still-image photography, car pursuit, ineffective injunction

- **Falzon & Williams** — April 2007
  Well-known sports stars photographed in a tryst in a toilet cubicle
  Visual recording, non-public place, covert, unconsented, unofficial media

- **Elliott** — May 2008
  Distraught boat-owner filmed immediately after the boat's engine exploded, killing his parents
  Visual recording, public place, vulnerable person, overt, persistent, consent denied

- **Splatt** — June, 2009
  Mother of swine flu victim subjected to unwelcome media attention and disclosure of distressing details
  Persistent, consent denied, vulnerable people

- **Campbell** — May 2010
  Cabinet Minister filmed leaving gay club
  Stake-out, covert, visual recording, unconsented, no public interest

- **Pulver** — August 2011
  17-year-old girl subjected to fake collar-bomb in an attempt at extortion, then subjected to relentless media attention
  Stake-out, visual recording, persistent, overt, consent denied, pursuit

- **Boy in Bali** — October 2011
  14-year-old boy charged with a drug offence in Bali, en route to and from the court, subjected to media stampedes and microphones thrust in his face
  Stake-out, visual recording, consent denied, persistent, culturally risky

2.2 Analytical Approach

This section documents Australian media organisations' surveillance practices in a structured manner, by applying a framework for the analysis of surveillance developed by the author for such purposes (Clarke 2009). The framework has three elements. The first is definitions of key terms. Most centrally, surveillance is the systematic investigation or monitoring of the actions or communications of an area, a location or one or more objects, most relevantly for this analysis, people. Other notions of significance include the distinction between overt and covert surveillance.

The second element is a seven-dimension categorisation of the nature of a surveillance activity, addressing the questions of: 'of What? for Whom? by Whom? Why? How? Where? and When?' The framework arranges answers to the questions in ascending scales, relative to the degree of intrusiveness of the surveillance, and hence the strength of justification needed for it to be reasonably imposed. For example, surveillance is more intrusive if it is frequent rather than once-only, continuous rather than ephemeral, and involves recording rather than mere observation.

When addressing the question of 'Where?', the distinction is commonly made between a 'public place' and a 'private place'. Interpretations of the boundaries between them vary, and so do inferences about the significance of the difference between them. 'Where?' and 'What?' may also become intertwined. Analysts refer to 'private space', and courts and legislatures to 'private activity'. A private place will commonly provide a person with private space in which to conduct private activity; but that is not always the case because activity may be readily visible from nearby, e.g. because a door is ajar, or curtains are left open. On the other hand, despite the frequently made suggestion that individuals can have no expectation of privacy in a public place, a public place does not necessarily deny privacy. A broom cupboard in a public museum, or a secluded corner of a park or an alp, may give rise to a reasonable expectation of private space and the scope to conduct private activity. Similarly, a celebrity, in a public playground with partner and children, is not 'fair game' for paparazzi, because a reasonable expectation of privacy exists. An appearance on the red carpet outside an awards ceremony, on the other hand, involves no implication of private behaviour.

The third element of the framework distinguishes forms of surveillance and the technologies that underlie each form. The remainder of this section surveys those forms. Surveillance impinges on all of the dimensions of privacy (Clarke 1997). Communications privacy is invaded by directional microphones and wire-taps. Data privacy is undermined by, for example, locating a person in physical or electronic space, and logging their locations over time. Individuals' physical privacy is affected by microphones and cameras thrust in their faces, and may in time be invaded by implants to facilitate tracking. The primary focus of this paper, however, is behavioural privacy. This is the interest that individuals have in being free to conduct themselves as they see fit, without unjustified surveillance. Particular concern arises in relation to sensitive matters such as sexual preferences and habits, religious practices and political activities. Some privacy analyses, particularly in Europe, extend this discussion to personal autonomy, liberty and the right of self-determination. Intrusions have a chilling effect on social, economic and political behaviour.

The form of surveillance most commonly conducted by the media has been, and continues to be, ***physical surveillance***. Some is unaided watching and listening with eyes and ears, but advantage is taken on occasions of various aids to the human faculties of sight, hearing and remembering. Telescopic lenses, directional microphones, and recording devices for image, sound and video have all been exploited. In the *Kidman v. Fawcett & McDonald* case in 2005, a triggering device was used.

In some cases, such as Falzon & Williams and Campbell, the surveillance is covert. Many instances of media surveillance, on the other hand, are overt. A common pattern involves many individual reporters, some with portable microphone and audio-recorder, crowding around their quarry, together with large numbers of cameramen carrying still-image- and video-recording and/or transmission equipment, thrust well inside the 'personal space' that is otherwise the norm in Australian society. Stake-outs are commonly used, particularly by paparazzi, but also by news reporters. These are most commonly at the home of the target, but 'doorstop' interviews are another example, in particular at Parliament Houses and outside court-houses.

Consent is seldom sought. Denials of consent are generally ignored. In the Pulver and the Boy in Bali cases, the hypocrisy was extraordinary in that much of the media coverage adopted the pretence that the denial of privacy was the story that was being reported. The ignoring of denials of consent extends to

enormous persistence in many cases. Persistence in denials of consent extends to pursuit, on foot and by car. In the Pulver case, the trail was followed to a school sports-ground. In the Kidman case, the pursuit was at risk of resembling the fatal attempted escape of Dodi Fayed and Princess Diana.

Point of View Surveillance (PoVS) technologies have gone through the pioneer phase (Mann 1997), are becoming mainstream, and may even be consumerised if products such as Google Glass gain traction (Clarke 2012b). Lightweight audio- and video-recording and -transmission capabilities are increasingly available. Drones are currently enabling additional angles of view to be inexpensively acquired. The intrusiveness of physical surveillance is currently going through a substantial growth-spurt, which will inevitably have many harmful impacts on individuals.

The term ***communications surveillance*** is associated in the public mind with the monitoring of electronic traffic and content, using techniques such as 'wire-taps' / interception, deep packet inspection (DPI), and access to email server content. Its scope also encompasses interception of the post and the surveillance of behaviour and experience such as web-trails, searches and purchases. There have been few credible reports of communications surveillance by Australian media. Further, there have been enthusiastic denials that Australian media practise unauthorised access to voicemails (misleadingly reported in the UK as 'mailbox hacking'), or to telephone, email or chat/IM traffic. On the other hand, there is abundant evidence of reporters gaining access to information about private conversations from people who were party to them, or were otherwise present at the time. In some cases, the information is disclosed willingly, and in other cases for inducements. In a number of cases, information is gained by the media about private conversations through deceit, using techniques discussed below.

Whereas communications surveillance intercepts messages in transit, another form is concerned with stored data. This is ***dataveillance***, the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons (Clarke 1988). A number of dataveillance techniques are routinely used by the media. Instances of unauthorised access have occurred, e.g. through the use of login-ID/password pairs that have come into the media organisation's possession. Much more common, however, is data disclosure achieved by means of the social engineering technique of pretexting (in the US) or blagging (a UK term for a very similar concept).

Pretexting / blagging is, informally, the tricking of a person into making a disclosure by misleading them about the nature of the interaction. More formally, it is deceit, injurious falsehood, or constructive misrepresentation of the purpose of a conversation, in order to gain access to information that would normally be protected. A special case of pretexting / blagging is masquerade, where the deceit is the pretence that the interviewer is a particular person, or a member of a particular category of people, to whom it is appropriate to disclose the information. Media staff sometimes masquerade as, or 'spoof', the person to whom the data relates. Both pretexting and masquerade appear to be quite common practices among Australian reporters, and to be at least tacitly approved by media organisations, at least in relation to stories that the organisations judge to be important.

In recent years, it has become necessary to distinguish a special category of dataveillance, usefully referred to as ***location and tracking surveillance*** (Clarke 1999). The Kidman and Pulver cases involved stake-out of the targets' homes, the Campbell case involved stake-out of a gay club, and the Boy in Bali the stake-out of a court-house. The Kidman and Pulver cases involved pursuit by vehicle. Pursuit by drones is imminent (Clarke 2014). Location and tracking surveillance can be supported by more sophisticated means than human observation, informers and remote-controlled cameras. However, no documented instances of media organisations planting tracking devices in vehicles came to light during the research.

It is no longer far-fetched to consider the possibility of more direct location and tracking surveillance of targeted individuals through the planting of tracking devices in personal accoutrements and on, or even in, the targeted person. The term ***body surveillance*** has been emergent for some time to refer to such activities (Lyon 2001a, 2001b; Michael and Michael 2009). These techniques are proliferating beyond house arrest, parole, remand and private investigations, and hence body surveillance might soon become part of media practices.

For completeness, the framework for the analysis of surveillance necessarily extends to comprehensive surveillance, which strives for pervasiveness and omniscience. It necessarily involves multiple surveillance techniques and technologies, used in an integrated manner. The term ***überveillance*** has been coined for this emergent phenomenon (Michael and Michael 2007; Clarke 2007). This might lie in the media's future, but not in its present.

The presumption is readily made that the most privacy-abusive and least justifiable of the practices noted in this section are the province of paparazzi, such as those involved in the Kidman case. A paparazzo / paparazza is usefully defined as a photographer or reporter who seeks sensational but essentially trivial material, with great persistence and in some cases with audacity. On the other hand, it takes very little adaptation to produce an appropriate definition of an investigative reporter: a reporter who seeks material relevant to a matter of public interest, with great persistence and in some cases with audacity. It is important that clarity exists about where the public interest does and does not lie, and that a legal framework provide civil law and criminal law controls over inappropriate media surveillance activities.

3. Contemporary Regulation of Media Surveillance

This section provides a brief survey of Australian law that does or may relate to surveillance undertaken by the media. Australia is a federation of six States and two Territories, with a national jurisdiction that is in some contexts superior to and in other contexts complementary too or overlapping with the sub-national jurisdictions. There is much in common between Australian law and the laws of other common law countries, including the UK, USA, Canada, South Africa and India. The degree of applicability of the analysis that follows is, however, of less direct relevance in civil code countries. The analysis was undertaken and written by a non-lawyer, based on a range of readily accessible and apparently credible secondary sources. Nemeth (2011) was of considerable value. Because the purpose is to assist in policy discussions, and it is not intended as a source of legal advice, the text may contain legal imprecisions and infelicities.

The analysis commences with a review of relevant torts. Statutes that specifically deal with particular kinds of surveillance are then considered. A number of other statutes are then outlined, in particular human rights law and privacy law. These are shown to provide no protections, but they do set the scene for a discussion of media codes. Because the laws are deficient, and some individuals become very angry when subjected to persistent media attention, it is also necessary to consider the scope for direct action by individuals who are set upon by the media.

3.1 Tort Law

A tort is a civil wrong that can give rise to a claim before the courts. Most torts are common law arising from an accumulation of cases. Some have been codified by statute, changed by statute, or even extinguished by statute. A small number have been created by statute. A privacy tort has been recognised in both the US and the UK, although in both countries it is of limited scope and effectiveness. No privacy tort has been recognised by Australian courts, however. Moreover, a common law tort appears to be highly unlikely to emerge, and the prospect of a statutory tort being created has been suppressed by means of strenuous opposition by media organisations.

A range of specific torts are discussed below, as they relate respectively to interference with real estate, with a person, and with a person's emotional state. A final subsection considers torts relevant to deceitful behaviour. With a few exceptions, torts are generally venerable and arcane, they change enormously slowly, and their interest to lawyers is far greater than their usefulness to people—as evidenced by the paucity of cases in which Australians have successfully used tort law to protect their behavioural privacy, or indeed any other aspect of their privacy.

- *Interference with Real Estate*

The tort of **Trespass to Land** is relevant to unauthorised entry to real estate of which the person is the lawful occupant. It can be invoked if a media person physically enters another person's property, but not if they stay outside it, even if their presence or activities interfere with the person. Many government agencies, schools and parliaments, and many industrial and commercial corporations, ban photography within their property. That may have some benefits for people endeavouring to avoid media harassment.

The tort of **Nuisance** involves interference with a lawful occupant's quiet enjoyment of their property. It appears unlikely that this tort encompasses image-capture from outside a property but pointing into it. It might conceivably be used to deal with stake-outs outside a home. On the other hand, that does not appear to have been attempted in either the Kidman or the Pulver cases. It is not applicable to stake-outs on other properties, however, such as parliaments or court-houses, nor to pursuits.

- *Interference with a Person*

To invoke the tort of **Trespass to the Person** in a public place, the onus in on the plaintiff to prove that an act by the respondent had a 'direct' and 'substantial' interference with their personal autonomy. Intent is not necessary, and hence negligent trespass is in principle actionable. It appears that the obscure tort of **False Imprisonment** may be an extended or applied form of Trespass to the Person. The tort of **Obstruction** involves interference with a person's freedom of movement or action. It would appear to have in-principle relevance to stake-outs, persistent reporters and photographers, and pursuit. The tort of **Assault** requires an act intended to cause the reasonable apprehension of an immediate harmful or offensive contact. It appears more likely to assist the media than their prey, but might have some application to acts of coercion. These three or four torts may have some in-principle applicability, but none of them appear to have been used successfully to rein in excessive media behaviour.

During recent decades, instruments have been created called in New South Wales (NSW) **Apprehended Violence Orders (AVOs)**. These address stalking, which is persistent unwanted communications, approaches, pursuit and/or monitoring that creates apprehension or fear. In 2005, Kidman gained AVOs against paparazzi Jamie Fawcett and Ben McDonald. However, they proved to be too narrow and were dropped. The NSW Government then removed AVOs from Part 15A of the Crimes Act, and put them in the Crimes (Domestic And Personal Violence) Act 2007. This may have had the effect of denying access to them in actions against the media, with the examples of stalkers mentioned in a NSW Police information page being 'a former intimate partner, acquaintance, stranger, relative, spouse, etc.'.

In Victoria, the **Personal Safety Intervention Orders** Act 2010 created **PSIOs**. These relate to '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 ...'. It may be that the scope is intended to be

> broader than in NSW, because the brochure describing the law mentions as examples 'neighbour, friend, work colleague, employer, employee, tenant, landlord, trader, or even a stranger'.

Since the abortive instance of 2005, no evidence was found of any attempts to convince a court to consider claims of harassment or stalking by the media.

- *Interference with a Person's Emotional State*

A variety of behaviours may generate anxiety in a person, such as:

- Stalking or Pursuit, i.e. the persistent following of a person within a physical or possibly also an electronic space
- Stake-Out, i.e. the surveillance of a space, with the intention of intercepting a person in that space
- Harassment, i.e. behaviour by one person that another finds threatening or disturbing.

There appear to be no torts that provide redress against media use of such behaviours. Even under the modern tort of stalking, in both NSW and Victoria actions will fail unless 'intent to cause fear of mental harm' can be demonstrated, and in NSW the context has to be 'domestic or personal violence'. In some jurisdictions, criminal provisions exist relating to stalking. However, under the Crimes Act (Vic) s.21A, for example, a defence is available if 'the course of conduct was engaged in without malice ... in the normal course of a lawful business, trade, profession or enterprise (including ... the publication, or arranging for the publication, of news or current affairs material)' (s.21(4A)(a)). So it would appear that, in Victoria, stalking by the media is only a criminal offence if the conduct is 'engaged in with malice', a term that is interpreted very narrowly by the courts. In some other jurisdictions, stalking is only a crime if it is done with the intent to cause harm of some kind, and the onus of proof lies on the prosecution.

The tort of **Negligence** arises from a failure to exercise a duty of care. It is unlikely to be of much value in relation to media behaviour, although it might have applicability where, for example, a child is being interviewed or their behaviour is being recorded.

- *Deceitful Behaviour*

The tort of **Misrepresentation** exists. It encompasses several rights of action. **Deceit** may be actionable where a person makes a factual misrepresentation, knowing that it is false (or having no belief in its truth and being reckless as to whether it is true) and intending it to be relied on by the recipient, and the recipient acts to his or her detriment in reliance on it. It appears that it can only be invoked by the person who is subjected to the trickery, not by a third party who is harmed by it. It is therefore only of benefit where the media use deceit to cause the person to expose personal data about themselves. It may also be limited to commercial contexts, in which case it would be useless in relation to most instances of deceit by the media.

Passing Off appears to have developed solely in commercial contexts, where a person misrepresents their goods or services as being those of another person, in order to gain an advantage or to disadvantage the other person. It does not appear that acts of impersonation, identify fraud or even the rare and extreme phenomenon of identity theft is encompassed within this tort, as it currently exists in Australia. These torts provide very limited scope for reining in the media's use of the various 'social engineering' techniques such as pretexting / blagging and masquerade.

3.2 Surveillance Statutes

A patchwork quilt of statutes exists in Australia that have represented responses to various perceived needs in various jurisdictions. In the first context examined, telecommunications, they appear to be

effective. Visual and aural surveillance is subject to some (at least partially ineffective) constraints in relation to private places, but far less in relation to public places.

- *Telecommunications*

Interference with physical mail is subject to **Postal Services offences** under the Crimes Act (Cth) Part VIIA, ss.85E-85ZA. The Commonwealth **Telecommunications (Interception and Access)** Act (TIAA) constrains abuse of wired and wireless message transmission—popularly referred to as 'wire-tapping'—and is backed up by complementary legislation in most States and Territories, and offences in ss. 473-475 of the Criminal Code (Cth).

There are also **computer offences** under ss. 476-478 of the Criminal Code (Cth), and in the various State and Territory criminal laws. There is also a plethora of so-called 'counter-terrorism' laws in this area. Although not specifically targeted at the media, these laws probably criminalise most acts by reporters that involve both exploitation of weak passwords and 'hacking'. For example, the actions of UK journalists from the now-defunct News of the World tabloid, which resulted in public furore, hearings by Parliamentary Committees and the Leveson Inquiry (Leveson 2012), if performed in Australia, would probably constitute an offence of unauthorised access to restricted data, under s.478.1, which is subject to a penalty of 2 years imprisonment. Australian media have argued that such behaviour is not indulged in by journalists of any kind in Australia, and no serious accusations have ever come to light.

- *Listening and Optical Surveillance Devices*

There have been two waves of legislation in relation to surveillance devices. The situation differs enormously across the eight State and Territory jurisdictions, and is complicated by the existence of a small Commonwealth jurisdiction of uncertain extent. In a 2010 case that involved video-surveillance of a private, consensual sex act in the dormitories of the Australian Defence Force Academy (ADFA), considerable uncertainty arose as to whether the surveillance activity was subject to the laws of the Commonwealth of Australia and/or of the Territory in which it occurred. It does not appear that any cause of action exists in the civil jurisdiction. However, the act was found to be the criminal offence of 'Using a carriage service to ... cause offence', under the Crimes Act (Cth) s.474.17.

Victoria, Western Australia and the Northern Territory passed Surveillance Devices legislation in the 1998-2000 timeframe, and NSW in 2007. These apply to both listening and optical surveillance devices. Because of the differences and the complexities, general statements need to be expressed and interpreted cautiously. Broadly, in these jurisdictions, aural and/or optical surveillance of a private activity may well be illegal. A private activity is any activity inside a building performed in circumstances where it is reasonable to assume the parties to it did not want it to be seen by others, and reasonably expected that it would not be seen by others. In NSW at least, it includes activity inside a vehicle. The prohibition does not apply:

- to someone who is a party to the activity
- if the activity is happening outside
- if the circumstances indicate the parties do not care if they are seen

It would seem likely, for example, that it would be illegal in those jurisdictions for a third party to visually record a sex act in a toilet cubicle (the Falzon-Williams incident), or for a third party to visually transmit a sex act between other parties (one interpretation of the ADFA incident in 2010). However it is not illegal under such laws for a party to the act to transmit or record it (another interpretation of the ADFA incident). Further, it would be less likely to be illegal if the act was conducted in a private place, but brazenly (e.g. with the door open). In public places, on the other hand, aural and/or optical surveillance are generally not proscribed unless there is a strong case for expecting that the behaviour would not be observed, transmitted or recorded.

Queensland has taken a similar although highly restrictive approach, with the Criminal Code s.227A-227C relating to 'observations or [visual] recordings in breach of privacy', supported by guidance in the Queensland Courts Bench Handbook. South Australia, Tasmania and the ACT have yet to regulate optical surveillance. So in those jurisdictions there is no general prohibition against taking photographs or videos of people without their consent, not even in private.

On the other hand, even the three laggard jurisdictions have longstanding Listening Devices legislation, from 1972, 1991 and 1992 respectively. In all jurisdictions there are general prohibitions on listening to, or recording, voice where the person making the recording is not a party to the conversation, subject to provisos that vary across the jurisdictions. Parties to a conversation may, generally, record it, but they are subject to some (again, varying) constraints as to the purpose of the recording and/or the purpose of a communication or publication from the recording.

These are criminal matters, not causes of action in the civil jurisdiction, and hence they can in practice only be prosecuted by a law enforcement agency. No evidence came to light of any use of these provisions against the media. These laws would appear to provide individuals with scant protection against the use of surveillance devices by the media.

- *Pornography and Anti-Voyeurism Laws*

Censorship laws at Commonwealth, State and Territory levels may have some incidental value in protecting people against media harassment. In addition, various laws have been rammed through Parliaments during periods of moral panic relating to 'peeping-tom', 'upskirting' and 'downblousing' activities. Many have had to be withdrawn or amended when cases reached the courts and anomalies and unintended consequences emerged.

A lead was provided in this area by the Queensland Criminal Code, which criminalises observation or visual recording made for the purpose of observing or visually recording the other 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, creates voyeurism offences relating to:

(a) photographs of a sexual and voyeuristic nature, usually of a person's 'private parts'
(b) taken without consent, and
(c) taken in places where a 'reasonable person would reasonably expect to be afforded privacy' (such as toilets, showers, changing rooms, enclosed backyards, etc.)

Such laws would appear to represent controls over a narrow range of media abuses. On the other hand, the NSW law gives the appearance of criminalising the behaviour of the (unofficial media) photographer in the Falzon-Williams case, yet no record has been found of a prosecution.

3.3 Human Rights Laws

Human rights law also offers Australians no protections against media abuses. Despite a Bill of Rights being considered at the time of federation, the Australian Constitution created 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 declare the 'right not to have his or her privacy, family [or] home ... unlawfully or arbitrarily interfered with', but provide no enforceable protection for that right.

Some countries have human rights embedded in their Constitution, or in statute, and hence those countries' residents may have some protections against media intrusions under human rights laws. On the

other hand, many countries' instruments are vague and weak. As a result, residents in many countries may have little better protection than do Australians.

3.4 Privacy Laws

It would be reasonable to expect that privacy law would be relevant. However, what are commonly referred to as privacy laws are in almost all cases mere data protection laws, and affect surveillance either not at all or only very indirectly. Data protection laws exist in six of the nine Australian jurisdictions, the exceptions being Western Australia, South Australia and (with a tiny qualification) Tasmania.

The most relevant Australian statute is the Privacy Act (Cth). It contains very weak provisions relating to the private sector, which were legislated in 1999. But they include an exemption for the media that is reasonably described as audacious. It grants media organisations not only freedom from regulation, but also the freedom to set any 'standards' that they like, provided that those standards purport to 'deal with privacy', without any external standards or tests of credibility, or even consultation (s. 7B(4)). Naturally, all media organisations were happy to comply with this pro-business, anti-consumer provision.

During 2006-08, the ALRC conducted a study of the operation of the Act. Its Report noted the existence of a serious problem, but merely recommended that the word 'adequately' should be inserted into the expression 'deal with privacy' (ALRC 2008a). On the other hand, the ALRC recommended a carefully designed privacy right of action, which would apply generally, including to the media (ALRC 2008b). The Government of the day proposed to implement such a right of action, but, confronted by vitriolic media attacks led by the Murdoch press, failed to carry through on its undertakings.

A right of action of that kind would finally extend privacy protections beyond the narrow confines of data privacy, including to behavioural privacy. The existing Privacy Act, meanwhile, has been significantly weakened from 2014 by the Privacy Amendment (Enhancing Privacy Protection) Act 2012. Until March 2014, an at least nominal constraint existed, in that data collection was not to be conducted 'in an unreasonably intrusive way'. But the 2012 amendments omitted that requirement from the replacement Principle 3.5.

The Privacy Act is a solely data protection law, and a very weak one at that. Australians who are subjected to media surveillance find nothing to assist them in the nation's human rights and privacy laws, and there is currently little prospect of that changing. Presumptions are frequently made by authors that European data protection laws have some kind of impact on behavioural privacy as well. This is incorrect. The EU Directive of 1995, the EU Regulation that was debated 2012-13 (but appears to have been withdrawn following strong lobbying by US corporations), and national legislation such as the UK Data Protection Act, are concerned only with data privacy. Data collection activities are out-of-scope, and hence there are not even any incidental protections for behavioural privacy. The absence of privacy law protections against unreasonable surveillance by the media is not a solely Australian phenomenon.

3.5 Other Statutes

The tapestry of Australian law is complex, and a few other statutes may harbour protections for people set upon by the media. However, nothing of any value for these purposes is apparent in media law, copyright law, or trademark law.

3.6 Media Codes

A range of corporate and industry codes exist in the Australian media industry. For a compilation, see Clarke (2012a). Most are vague 'statements of aspiration' rather than specific, operationalised guidance that lends itself to the resolution of disputes. Many of them long pre-date the Privacy Act exhortation to have a code, but some were created in order to satisfy the exemption criterion. Many are (for good reasons) subsets of codes with broader scope than just privacy.

Print media are nominally subject to whatever code they use in order to trigger the Privacy Act exemption. Some newspapers, although mainly only the larger ones, have internal codes, and some may even have business processes for handling complaints about breaches of those codes. However, the codes are written by the media, for the media, and are applied by the media, for the media; so it is uncommon for complainants to get any form of satisfaction from such processes as actually exist.

A very weak form of 'industry self-regulation' applies to most of the press, in the form of the industry body, the **Australian Press Council**. The Council's documents (APC 2011a, 2011b) apply a 'public interest' test to publication, but not to data collection practices. The sole relevant statement of Principle is that 'journalists should not unduly intrude on the privacy of individuals and should show respect for the dignity and sensitivity of people encountered in the course of gathering news'. Moreover, the APC Code appears to actually approve of 'dishonesty and unfair means', in that publication of information obtained by dishonesty and unfair means is permitted provided that there is an 'over-riding public interest'.

A further concern is that the key term 'public interest' is defined enormously widely, to include matters 'capable of affecting the people at large so they might be legitimately interested in' them. The wide-ranging claim is made that 'Public figures necessarily sacrifice their right to privacy', qualified by the vague saving clause 'where public scrutiny is in the public interest', and the even vaguer sentence 'However, public figures do not forfeit their right to privacy altogether'. A later section of this paper examines the 'public interest' notion and proposes a formulation that appropriately balances the public and private interests.

The APC documents contain the apparently strong statement that 'Members of the public caught up in newsworthy events should not be exploited'. But this is weakened by the immediately following sentence: 'A victim or bereaved person has the right to refuse or terminate an interview or photographic session at any time'. Rather than applying the protective anglo-australian concept of 'consent', it implements only the permissive US concept of 'opt-out'.

The Council has limited powers and very limited sanctions, which are currently only to require publication of the Council's determination in relation to a complaint. Late in its life, the Labor Government of 2007-13 introduced the News Media (Self-regulation) Bill 2013. This would have forced the Australian Press Council's members to grant the APC remedial powers. But the Bill did not proceed, and the incoming Coalition Government, which is just as terrified of the power of the Murdoch media, but much better served by it, shows no sign of bringing about any changes that would advantage individuals against media surveillance.

Radio and TV Broadcasters are subject to what is presented as though it were a 'co-regulatory' scheme; but the nominal regulator, the **Australian Communications and Media Authority (ACMA)**, is merely a registrar of codes developed by the industry (ACMA 2013b). On the last workday before Christmas 2011, ACMA weakened still further its 'privacy guidelines for broadcasters', such that the tiny incidence of successful complaints is destined to fall still further.

In any case, none of the Codes registered with ACMA appear to contain any provisions whatsoever relating to the media's information-gathering behaviour. A complaint can only be made in respect of publication. The ACMA admitted its own failings in relation to the behaviour of TV stations in the Elliott case, and was widely criticised (including by many in the media) for condoning the TV Channel's behaviour in the Campbell case, and using a patently illogical argument in order to do so (Ackland 2011).

The APC provides a very limited, very weak and very weakly enforceable form of control over media surveillance by most of the print media. The ACMA-administered Codes are only nominally co-regulatory

because the agency has no powers, and in any case the scope does not extend to surveillance by the broadcast media. In the face of aggressive opposition by media organisations that continue to be perceived by politicians to be powerful, there is no prospect of either industry self-regulation or co-regulation acting as any kind of curb on unreasonable uses of surveillance by the media.

3.7 Direct Action

The substantial absence of protections exposed in the preceding sections makes it necessary to consider the scope for an individual to take direct, i.e. physical, action against members of the media who are subjecting them to surveillance.

There seem to be very few laws that provide individuals with any express rights to act against other people. The following are apparent:

- a person in possession of real estate can use 'reasonable force' to evict other people from the property
- some limited rights exist in relation to 'citizen arrest', but these apply only in respect of criminal behaviour, not behaviour that infringes civil rights

On the other hand, a person who fights back against media intrusions runs the risk of themselves infringing a wide array of provisions of both civil law and the criminal law. The following are apparent:

- a threat of violence, whether conveyed verbally or physically, may constitute the crimes of common assault, affray and/or threatening to destroy or damage property
- an act of violence may constitute aggravated assault and/or battery
- a threat of violence as a means of forcing, for example, deletion of images from a camera, may constitute coercion
- an act of violence against a person's possessions (such as a camera) may constitute battery or malicious damage or destroying or damaging property
- detaining a person may constitute false imprisonment
- seizing a person's equipment (such as a camera) may constitute theft, robbery or stealing

Clearly, media staff should be protected against unreasonable behaviour by people who they are gathering information from and about. It is significant, however, that protections for the media are far clearer and more comprehensive, and far more ready actionable in the courts, than protections for people who are subjected to unreasonable media behaviour.

This review of laws regulating media surveillance has shown that members of the public have very few protections, and such as do exist appear to be narrowly defined criminal laws that can be, at least in practice, prosecuted solely by law enforcement agencies, and cannot be pursued by the individual who has the grievance.

Important as it is for journalists to be able to pursue stories and unearth important facts, power that is unfettered to such a considerable extent is bound to be abused. From time to time, the abuse will be by over-exuberant investigative journalists, but the primary source will inevitably be the tabloid media. It is therefore important that a balance be established, in which the media are free to conduct surveillance in appropriate circumstances, but subject to effective sanctions when they do it without sufficient justification. The following section presents a normative scheme whereby the shortfall in protections for people set upon by the media can be made good.

4. Prospective Regulation of Media Surveillance

The specific proposals in this section were developed within the context of a broad set of principles for the regulation of surveillance of all kinds. These were developed by the public interest advocacy organisation, the Australian Privacy Foundation, and are listed in Table 2. An earlier application of the general principles, specifically to visual surveillance activities such as CCTV, is in APF (2010).

Table 2: Regulatory Principles for Surveillance
Extract from APF (2013)

1. Justification
All surveillance proposals that have the potential to harm privacy must be subjected to prior evaluation against appropriate privacy principles.

2. Consultation
All evaluation processes must feature consultation processes with the affected public and their representative and advocacy organisations.

3. Transparency
Sufficient information must be disclosed in advance to enable meaningful and consultative evaluation processes to take place.

4. Justification
All privacy-intrusive aspects must be demonstrated to be necessary pre-conditions for the achievement of specific positive outcomes.

5. Proportionality
The benefits arising from all privacy-intrusive aspects must be demonstrated to be commensurate with their financial and other costs, and the risks that they give rise to.

6. Mitigation
Where privacy-intrusiveness cannot be avoided, mitigating measures must be conceived, implemented and sustained, in order to minimise the harm caused.

7. Controls
All privacy-intrusive aspects must be subject to controls, to ensure that practices reflect policies and procedures. Breaches must be subject to sanctions, and the sanctions must be applied.

8. Audit
All privacy-intrusive aspects and their associated justification, proportionality, transparency, mitigation measures and controls must be subject to review, periodically and when warranted.

The first section below applies the general principles to the specific context of media surveillance. The second section examines the critical concept of 'the public interest'.

4.1 Principles for the Regulation of Media Surveillance

In Clarke (2012c), a report was provided of a comprehensive study of privacy and the media in Australia. It included an analysis of the public's needs, and a proposed Code Template, against which each of the many codes that informs behaviour in the print and broadcast media can be assessed. This section extracts the aspects of those proposals that bear directly on the regulation of media surveillance behaviour.

It is particularly important that the Justification and Proportionality Principles outlined above be operationalised in ways that draw the line for both reporters and photographers on the one hand, and members of the public on the other. A more specific Principle is accordingly proposed in Table 3.

Table 3: A Specific Principle for Media Information-Gathering
After Clarke (2012c)

- The following practices must not be undertaken by or for a media organisation, unless a clear justification exists:
  - the seeking or gathering of personal data
  - the observation or recording of personal behaviour
- The justification for those practices must be based on one of the following:
  - consent by the person to whom the data relates
  - express legal authority; or
  - an over-riding public interest
- The nature of the activities, and their degree of intrusiveness:
  - must reflect the nature and extent of any consent provided
  - must reflect the nature and extent of any express legal authority; and
  - must be proportionate to the nature and significance of the public interest arising in the particular circumstances

The Principle then needs to be articulated into a form that supports the media in its work and provides a firm basis for the handling of complaints about media behaviour. Table 4 suggests how the articulation can be expressed.

Table 4: Standards for Media Information-Gathering

The following data-gathering activities breach the Media Information-Gathering Principle, unless they are the subject of express legal authority, or are justified by a public interest of sufficient significance to warrant the activity, taking into account relevant factors, in particular the sensitivity of the context and the degree of discomfort, anger or distress that the performance of the activity may give rise to:

1. activities that intrude into the person's private space
2. activities that intrude into the person's reasonable expectations of privacy, notwithstanding that the person is in a public space
3. activities that involve deception, such as the following:
   - masquerade as another person
   - misrepresentation or subterfuge intended to cause a person to provide information (sometimes called 'pretexting' or 'blagging')
   - observation or recording under circumstances in which the person would not reasonably expect observation or recording to be taking place
4. activities that exploit vulnerability, naiveté or ignorance about media organisations' collection practices. Particular concern arises in the case of children and people with limited mental capacity or experience
5. activities that intrude into the private space of people in sensitive situations, such as accident victims, witnesses to accidents, and the bereaved
6. activities that place pressure on a person to behave in a particular manner or to divulge sensitive data, such as conveying the implication that the person is under a legal or moral obligation, intimidation and excessive persistence
7. activities that the person reasonably perceives to constitute trespass, nuisance, obstruction, pursuit, harassment or stalking

4.2 The Public Interest

The Principle and Standards proposed above depend on a couple of key terms that need to be clearly explained as part of the framework.

The first necessary step is to recognise that the notion of a 'public figure' is used by the media to justify intrusive behaviour in relation to a person on the basis of who they are, in order to circumvent or subvert the public interest test. A regulatory regime for the media should deny the legitimacy of the concept 'public figure', and require that all behaviour and publication be based on the public interest test.

To the extent that the 'public figure' notion continues to be used, very different analyses need to be undertaken and very different approaches adopted in relation to at least the following categories:

- people with public appointments
- people with prominent roles in corporate and association life
- 'celebrities' and 'notorieties' (i.e. people famous for what they once did, or just for being famous)
- 'temporary celebrities' (i.e. people thrust into the limelight by events such as disasters and winning the lottery)
- persons-at-risk, whose safety is threatened by media exposure, including:
    - people who are in hiding from others, including victims of domestic violence, protected witnesses and undercover agents
    - wealthy people who may be subject to criminal activities such as burglary, extortion and kidnap
    - people who express views that are controversial or unpopular
    - people whose actions excite antipathy, such as convicted pederasts
- vulnerable people (i.e. whose state of mind may be harmed and/or who may not be currently capable of making informed judgements about their own best interests, including the young, the mentally-impaired, people with limited English language skills, accident victims, people otherwise caught up in an emergency or tragedy, and the bereaved)

The second requirement is that the public interest test be clarified and operationalised, and extraneous factors separated from it. The 'extraneous factor' problem is that the public interest emphatically does not contain any element of 'What the Public Is Interested In', far less 'What the Public May Be Able to Be Made Interested In'. The APC, and more recently the ACMA, have smuggled the idea in by means of a definition that includes the words '[matters that] people at large ... may be legitimately interested in'.

That wording derives from a UK judgement in *London Artists v Littler* (1969) 2 QB 375 at 391. Lord Denning, then Master of the Rolls, said that 'There is no definition in the books as to what is a matter of public interest. All we are given is a list of examples, coupled with the statement that it is for the Judge and not for the jury. I would not myself confine it within narrow limits. Whenever a matter is such as to affect *people at large*, so that they *may be legitimately interested in*, or concerned at, what is going on; or what may happen to them or to others; then it is *a matter of public interest* on which everyone is entitled to make fair comment' (emphases added).

This judgement is at best only indirectly relevant to the context of privacy and the media because Denning's words referred only to defamation law, and specifically to the defence of fair comment (which is dependent on the comment being made 'on a matter of public interest'). In the words of a sometime Australian Prime Minister, 'The public interest means publication or non-publication guided by what is in the interest of the public as a whole, not what readers or an audience might find interesting or titillating' (Keating 2010).

The notion of the public interest must be clearly defined so as to identify the specific categories of circumstance that justify a person's privacy interest being overridden. The following categories were identified and discussed in APF (2009, 2011) and Clarke (2012c):

- relevance to the performance of a public office
- relevance to the performance of a corporate or civil society function of significance
- relevance to the credibility of public statements
- relevance to arguably illegal, immoral or seriously anti-social behaviour
- relevance to public health or safety
- relevance to an event of significance

Those references also operationalise the term 'over-riding public interest', and discuss several additional factors that need to be taken into account when interests are being balanced.

5. Conclusions

Media use of surveillance is very important to society. Media responsibility in its use of surveillance is very important to individuals. The analysis conducted in this paper has shown that the contemporary regulatory framework in Australia evidences serious imbalance. The problem is set to worsen, with surveillance technologies becoming not only less expensive, but also more aerial, through the application of drones.

The need will become even more pressing due to the increased revenue pressures that media organisations are being subjected to as a result of networked media, Google's dominant position in the advertising supply chain, and hence the even greater importance of frequent 'scoops'. Another driving force is the democratisation of both surveillance and media publishing. Anyone who has the urge can now conduct surveillance, and can publish. Until now, paparazzi have been part of the media industry and have needed resources, formal publication channels, and commercial arrangements to enable them to spend the considerable amount of time and money involved. The prospect now arises of 'hobby paparazzi' and 'neighbourhood paparazzi'.

The absence of protections against media abuses has been problematical, but it is becoming much more serious. The media industry has missed the opportunity to 'take the moral high ground' and distinguish itself from amateur media by means of quality standards for the process of journalism. Regulatory change is now essential. There will shortly be public clamour for controls over the use of surveillance by amateur and professional media alike.

The final section of this paper has proposed a framework for balanced regulation of media surveillance activities. The proposal reflects the interests of watchers, the watched and the general public, is based on general principles, articulates the general to specific principles, and identifies specific activities that require legal authority or justification based on a defined notion of the public interest.

The analysis has focussed almost entirely on the Australian context, both as regards media practices and regulation of them. Care is needed in making generalisations to other countries because media practices, laws, and social and political values vary considerably. It is clear, however, that unjustified and harmful use of surveillance by the media, and particularly by the 'tabloid media', is not limited to Australia. Moreover, even where some scope exists for court action against the media, as is the case in the UK, the remedy may only be effective for individuals who have considerable resources to expend on the action, without any real prospect of the costs being recovered. This suggests that the Principles and Standards proposed in this paper may be of relevance well beyond Australia.

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

ACMA. 2013a. 'Broadcasting investigation reports' Australian Communications and Media Authority, 2013, at HTTP://archive.acma.gov.au/WEB/STANDARD/pc=PC_300384

ACMA. 2013b. 'Broadcasting Codes Index' Australian Communications and Media Authority, 2013, at http://archive.acma.gov.au/WEB/STANDARD/1001/pc=IND_REG_CODES_BCAST

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/

APC. 2013. 'Adjudications and other outcomes' Australian Press Council, 2013, at http://www.presscouncil.org.au/adjudications-other-outcomes/

APF. 2009. 'Policy Statement re Privacy and the Media' Australian Privacy Foundation, March 2009, at http://www.privacy.org.au/Papers/Media-0903.html

APF. 2010. 'Policy Statement re Visual Surveillance, incl. CCTV' Australian Privacy Foundation, January 2010, at http://www.privacy.org.au/Papers/CCTV-1001.html

APF. 2011. 'An Appropriate Public Regulatory Body' Submission to the Independent Media Inquiry, Australian Privacy Foundation, November 2011, at http://www.privacy.org.au/Papers/MediaInq-Sub-111118.pdf

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

AustLII. 2013. 'Australian Press Council Adjudications' Australasian Legal Information Institute, 2013, at http://www.austlii.edu.au/au/other/apc/

Clarke, R. 1988. 'Information Technology and Dataveillance' Commun. *ACM* 31:5 498-512.

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

Clarke, R. 1999. 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications' Proc. 21st International Conference on Privacy and Personal Data Protection, pp.131-150, Hong Kong, September 1999.

Clarke, R. 2007. 'What 'Überveillance' Is, and What To Do About It' Invited Keynote, 2nd RNSA Workshop on the Social Implications of National Security - From Dataveillance to Überveillance ..., 29 October 2007, University of Wollongong.

Clarke, R. 2009. 'A Framework for Surveillance Analysis' Xamax Consultancy Pty Ltd, Working Paper, August 2009, at http://www.rogerclarke.com/DV/FSA.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. 'Point-of-View Surveillance' Xamax Consultancy Pty Ltd, Working Paper, February 2012, at http://www.rogerclarke.com/DV/PoVS.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. 2014. 'The Regulation of Civilian Drones' Applications to the Surveillance of People' Forthcoming, *Computer Law & Security Review*, PrePrint at http://www.rogerclarke.com/SOS/Drones-BP.html

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. 2001a. 'Under My Skin: From Identification Papers to Body Surveillance'. In: *Documenting Individual Identity: The Development of State Practices in the Modern World*, eds. J. Caplan and J. Torpey, 291-310. Princeton, NJ: Princeton University Press.

Lyon, D. 2001b. *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.

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/

Michael, M.G. and K. Michael. 2007. 'Überveillance: 24/7 x 365 People Tracking and Monitoring' Proc. 29th International Conference of Data Protection and Privacy Commissioner, at http://www.privacyconference2007.gc.ca/Terra_Incognita_program_E.html

Michael, K. and M.G. Michael. 2009. 'Innovative automatic identification and location-based services: from bar codes to chip implants' IGI Global.
Nemeth, A. 2011. 'Australian Street Photography: Legal Issues' Andrew Nemeth, 2000-, at http://4020.net/words/photorights.php

Statutes

Crimes Act 1914 (Cth)
http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/
Crimes Act 1900 (NSW)
http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/index.html
Crimes Act 1958 (Vic)
http://www.austlii.edu.au/au/legis/vic/consol_act/ca195882/
Crimes (Domestic And Personal Violence) Act 2007(NSW)
http://www.austlii.edu.au/au/legis/nsw/consol_act/capva2007347/
Criminal Code Act 1995 (Cth)
http://www.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html
Criminal Code Act 1899 (Qld)
http://www.austlii.edu.au/au/legis/qld/consol_act/cc189994/
Human Rights Act 2004 (ACT)
http://www.austlii.edu.au//au/legis/act/consol_act/hra2004148/
Personal Safety Intervention Orders Act 2010 (Vic)
http://www.austlii.edu.au/au/legis/vic/consol_act/psioa2010409/
Privacy Act 1988 (Cth)
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/
Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
http://www.austlii.edu.au/au/legis/cth/num_act/pappa2012466/
Surveillance Devices Act 2007 (NSW)
http://www.austlii.edu.au/au/legis/nsw/consol_act/sda2007210/
Telecommunications (Interception and Access) Act 1979 (Cth)
http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/s7.html

Cases

London Artists v Littler (1969) 2 QB 375