

# **Surveillance by the Australian Media, and Its Regulation**

Roger Clarke

Principal, Xamax Consultancy Pty Ltd, Canberra, Australia

Visiting Professor, Cyberspace Law & Policy Centre, UNSW, Sydney

Visiting Professor, Research School of Computer Science, ANU, Canberra

+61 2 6288 6916

Roger.Clarke@xamax.com.au

Version of 21 April 2012

## **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**

The term 'the media' is commonly used to refer to media 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 agents of media organisations, particularly reporters and photographers.

A free, effective and professional media has proven to be a critical element within modern democracies, and considerable freedoms are, and must be, provided to the media to enable them to play a central role in information discovery and information flows to the public.

But 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. Many surveillance technologies and associated practices have become central to the functioning of the media.

Little appears to have been published examining the regulation of media organisations' use of surveillance techniques and technologies, and nothing at all in the first 9 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 (2012a)). That project is not concerned with the publication phase of media work, but only with the media's data-gathering activities.

The paper uses both empirical and analytical approaches to identify and articulate a wide range of excesses. It then reviews the current regulatory environment within which the media works, and 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**

This section presents the results of a survey of the use of surveillance by the media. The research method comprised the search for, documentation and analysis of a small set of cases that provide an empirical basis for the analysis. These are outlined in the first sub-section. The second sub-section 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 media reports in Australia between 2005 and 2011, in order to identify a manageable small but diverse set of instances of media surveillance. Exhibit 1 lists the cases and their key elements. Clarke (2012a, s.3.2) provides, for each of the cases, a description and citations.

### Exhibit 1: Case Studies in Media Surveillance

- **Kidman** – January 2005  
Stake-out, listening device, still-image photography, car pursuit, AVOs granted
- **Falzon & Williams** – April 2007  
Visual recording, non-public place, covert, unconsented, unofficial media
- **Elliott** – May 2008  
Visual recording, public place, vulnerable person, overt, persistent, consent denied
- **Splatt** – June, 2009  
Persistent, consent denied, vulnerable people
- **Jackie O & Sandilands** – July 2009  
Coercion, vulnerable person, live-to-air
- **Campbell** – May 2010  
Stake-out, covert, visual recording, unconsented, no public interest
- **Pulver** – August 2011  
Stake-out, visual recording, persistent, overt, consent denied, pursuit
- **14yo Boy in Bali** – October 2011  
Stake-out, visual recording, consent denied, persistent, culturally risky

## 2.2 Analytical Approach

During a 25-year period studying aspects of surveillance, the author has developed a framework for the analysis of surveillance (Clarke 2009). It has three elements. The first is definitions of key terms. The second distinguishes forms of surveillance and the technologies that underlie each form. An overview is in Exhibit 2. The third element is a seven-dimension categorisation of the nature of a surveillance activity. An overview is in Exhibit 3.

## Exhibit 2: Forms of Surveillance – Overview

1. Physical Surveillance
2. Communications Surveillance
3. Dataveillance
4. Location and Tracking Surveillance
5. Body Surveillance
6. Überveillance

## Exhibit 3: Dimensions of a Surveillance Activity – Overview

1. Of What?
2. For Whom?
3. By Whom?
4. Why?
5. How?
6. Where?
7. When?

This section applies the above framework, in the sequence of Exhibit 2, and interleaving aspects arising from Exhibit 3. This enables Australian media organisations' surveillance practices to be documented in a structured manner. Informal assessment of media practices in other countries suggests that there are many commonalities, but also regional differences.

The majority of media surveillance has been, and continues to be, **physical surveillance**. Some has been unaided watching and listening with eyes and ears, but advantage has been taken of many 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 14 yo 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.

The behaviour of reporters and photographers is such that they appear to regard the 'public interest' constraint as being to some extent at least relevant to the question of publication, but not at all to the question of data collection.

Point of View Surveillance (PoVS) technologies have become mainstream (Mann 1997, Clarke 2012b). Official and unofficial media are increasingly wearing their own integrated audio- and video-recording and -transmission capabilities. 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** refers primarily to the monitoring of electronic traffic and content, and such as 'wire-tap' interception, deep packet inspection (DPI) and access to email server content. It is useful to define it more broadly to also encompass 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.

The term **dataveillance** refers to 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 loginid/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 interview. 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 'spooft', 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 14yo Boy in Bali the stake-out of a court-house. The Kidman and Pulver cases involved pursuit by vehicle, including in Kidman's case at considerable speed. Location and tracking can be supported by more sophisticated means than human observation and informers, including the planting of tracking devices in vehicles, although no documented instances of the use of such technologies by the media have come to light during the current research.

It is no longer far-fetched to consider the possibility of more direct location and tracking of targeted individuals by planting 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). 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, whose key features are omnipresence / 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 & Michael 2007, Clarke 2007b). 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. The country 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. Much of the analysis in this section is the result of original research. Nemeth (2011) was of considerable value, however.

This section 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, culminating in privacy law, which achieves precisely nothing, but does set the scene for a discussion of media codes. Because the laws are so utterly deficient, it is necessary to consider the scope for direct action by individuals who are set upon by the media.

This section is written by a non-lawyer, based on a range of readily accessible and apparently credible secondary sources. It is accordingly riddled with legal imprecisions and infelicities, and is doubtless sprinkled with errors. Its purpose is to assist in policy discussions not to be a source of advice.

#### **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. With a few exceptions, torts are venerable and arcane, they change enormously slowly, and their interest to lawyers is far greater than their usefulness to people. Torts are identified that relate respectively to interference with real estate, with a person, and with a

person's emotional state. A final sub-section considers torts relevant to deceitful behaviour.

- **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.

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.

Many government agencies, schools and parliaments, and many commercial and industrial premises ban photography within their property. That may have some benefits for people endeavouring to avoid media harassment.

- **Interference with a Person**

To invoke the tort of **Trespass to the Person** in a public place, the onus is 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 they do not appear to have been used successfully to rein in excessive media behaviour.

During recent decades, instruments have been created called in NSW **Apprehended Violence Orders (AVOs)**. 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, which appears to have had the effect of denying access to them in actions against the media.

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 ...", and "[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 appears that the scope is intended to be broad because the brochure describing the law mentions as examples "neighbour, friend, work colleague, employer, employee, tenant, landlord, trader, or even a stranger".

As shown below, stalking would be difficult to invoke against the media. Harassment may be more tenable, but it remains to be seen whether the courts will consider awarding PSIOs against the media.

- **Interference with a Person's Emotional State**

There appear to be no torts that address behaviour that generates anxiety in a person, in particular:

- Pursuit, i.e. the persistent following of a person
- 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 is one area in which laws do exist, however. In NSW, **Stalking** is persistent unwanted communications, approaches, pursuit and/or monitoring that creates apprehension or fear. On the other hand, the NSW statute is limited to actions in the context of domestic violence, and to actions taken 'with intent to cause fear of physical or mental harm'. It would appear unlikely that a reporter or media organisation could be demonstrated to intend mental harm to any of the individuals in the case studies, so, in NSW at least, stalking laws appear to be useless as a means of controlling media behaviour.

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 the media, 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 themselves expose personal data. 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.

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, 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 wire-tapping and 'hacking'.

- **Aural and Visual Surveillance Devices**

There have been two waves of legislation in relation to surveillance devices, and 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 involved video-surveillance of a private, consensual sex act in the dormitories of the Australian Defence

Force Academy (ADFA), considerable uncertainty arose in as to whether the surveillance activity was subject to the laws of the Commonwealth of Australia and/or the Territory in which it occurred.

Victoria, Western Australia and the Northern Territory passed Surveillance Devices legislation in the 1998-2000 timeframe, and NSW in 2007. These apply to both visual and aural surveillance devices. Because of the differences and the complexities, general statements need to be expressed and interpreted cautiously.

Broadly, in these jurisdictions, visual and/or aural 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

- 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 is illegal 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 (the other interpretation of the ADFA incident). Further, it would be less likely to be illegal if the act was conducted in private, but brazenly (e.g. with the door open).

In public places, on the other hand, visual surveillance will generally not attract any protection unless there is a strong case for expecting that the behaviour would not be observed, transmitted or recorded.

Queensland has taken a similar but 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 visual surveillance, but have remnant Listening Devices legislation from 1972, 1991 and 1992 respectively. There is no general prohibition against taking photographs or videos of people without their consent, not even in private. There may be, however, laws applying in particular contexts. On the other hand, there is a general prohibition on listening to or recording voice where the person making the recording is not a party to the conversation, again subject to various provisos.

- **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, create 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 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 any of the following:

- copyright law
- trademarks law
- human rights law (ACT and Victoria only)
- media law

It would be reasonable to expect that privacy law would be relevant. However, what are commonly referred to as privacy laws are mere data protection laws, and affect surveillance only indirectly, through collection, use and disclosure principles. They exist in six of the nine jurisdictions, the exceptions being Western Australia, South Australia and (with a tiny qualification) Tasmania.

The most relevant statute is that of the Commonwealth. The desperately weak private sector provisions of the Privacy Act were legislated in 1999. But they include an extraordinarily audacious exemption for the media, which 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. Naturally, all media organisations were happy to comply with this embarrassingly pro-business, anti-consumer provision.

The ALRC conducted a study of the operation of the Act, reporting in 2008. Its Report was guilty of abject cowardice in its handling of this aspect of privacy law, merely recommending that the word 'adequately' should be inserted into the expression 'deal with privacy'.

People who are subjected to media surveillance can find almost nothing to assist them in the nation's privacy laws.

### 3.4 Media Codes

A range of 'codes' exist, which are generally in the form of vague 'statements of aspiration' rather than specific, operationalised guidance that lends itself to the resolution of disputes. Many 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) sub-sets of codes with broader scope than just privacy.

Print media are 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 handle complaints about breaches of those codes. The codes are written by the media, for the media, so it is uncommon for complainants to get any form of satisfaction from such processes.

For the vast majority of the press, the mechanism is a very weak form of 'industry self-regulation' by means of the industry's own body, the **Australian Press Council (APC)**. The APC documents declare the Principle 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".

On the other hand, 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" – and 'public interest' is defined enormously widely, to include matters 'capable of affecting the people at large so they might be legitimately interested in' them.

Moreover, the grossly excessive claim is made that "Public figures necessarily sacrifice their right to privacy, where public scrutiny is in the public interest",

with the inadequate saving clause that "However, public figures do not forfeit their right to privacy altogether".

The apparently strong statement that "Members of the public caught up in newsworthy events should not be exploited" appears to be 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". This does not apply the protective anglo-australian concept of 'consent', but rather 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.

Radio and TV Broadcasters are subject to what is nominally a 'co-regulatory' scheme, but the nominal regulator, the **Australian Communications and Media Authority (ACMA)**, is merely a registrar of codes negotiated between ACMA and the industry. 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 illogic argument in order to do so.

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 provides no control whatsoever over media surveillance by the broadcast media.

### **3.5 Direct Action**

The patchwork quilt of laws identified in the preceding sections abjectly fails the need for controls over media surveillance practices. It is therefore very important 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 appear 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 readily actionable in the courts, than protections for people who are subjected to unreasonable media behaviour.

---

#### **4. Prospective Regulation of Media Surveillance**

The following section presents a normative scheme whereby the vast shortfall in protections for people set upon by the media can be made good. The first section enunciates a general set of principles. The second section then applies the general principles to the specific context of media surveillance. The third section examines the critical concept of 'the public interest'.

##### **4.1 General Principles for the Regulation of Surveillance**

The specific proposals in this paper were developed within the context of a broad set of principles for the regulation of surveillance of all kinds, listed in Exhibit 4, documented in Clarke (2007a), and applied to visual surveillance generally in APF (2010).

## **Exhibit 4: Regulatory Principles – Overview**

1. Justification
2. Proportionality
3. Openness
4. Access Security
5. Controlled Use
6. Controlled Disclosure
7. Controlled Publication
8. Non-Retention and Rapid Destruction
9. Review
10. Withdrawal

### **4.2 Principles for the Regulation of Media Surveillance**

In Clarke (2012a), 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 proposed in Exhibit 5.

### **Exhibit 5: A Specific Principle for Media Information-Gathering**

After Clarke (2012a)

- 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. Exhibit 6 suggests how the articulation can be expressed.

### **Exhibit 6: Standards for Media Information-Gathering**

The following data-gathering activities breach the 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, and 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

### 4.3 The Public Interest

The above statement and articulation of the Principle 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, as a means of circumventing or subverting the public interest test. A regulatory regime for the media should deny the legitimacy of the concept, and require all behaviour and publication to 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 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 previous 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. These are:

- 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

Discussion of each of those categories is provided in APF (2009, 2011) and Clarke (2012). 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. Regulatory change is essential now. The need will become even more pressing due to the increasing availability of inexpensive means of conducting surveillance, the increased revenue pressures that media organisations are being subjected to as a result of networked media and hence the even greater importance of frequent 'scoops', and the democratisation of both surveillance and media publishing. This paper has proposed what needs to be done, and how to do it.

---

## References

- 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>
- Clarke R. (1988) 'Information Technology and Dataveillance' *Commun. ACM* 31,5 (May 1988) 498-512, and 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. (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. Revised version in *Information Technology & People* 14, 2 (Summer 2001) 206-231, at <http://www.rogerclarke.com/DV/PLT.html>
- Clarke R. (2007a) 'The Regulation of Surveillance' Xamax Consultancy Pty Ltd, August 2007, at <http://www.rogerclarke.com/DV/SReg.html>
- Clarke R. (2007b) '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. Revised version published as '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. (2007c) 'Surveillance Vignettes' Xamax Consultancy Pty Ltd, September 2007, at <http://www.rogerclarke.com/DV/SurvVign.html>
- 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 - A Platform for Change?' Xamax Consultancy Pty Ltd, Working Paper, January 2012, at <http://www.rogerclarke.com/DV/PandM.html>
- Clarke R. (2012b) 'Point-of-View Surveillance' Xamax Consultancy Pty Ltd, Working Paper, February 2012, at <http://www.rogerclarke.com/DV/PoVS.html>
- Lyon D. (2001a) 'Under My Skin: From Identification Papers to Body Surveillance' Chapter 16 of Caplan J. & Torpey J. (Eds.) (2001) 'Documenting Individual Identity: The Development of State Practices in the Modern World', pp. 291-310
- Lyon D. (2001b) 'Surveillance society: Monitoring everyday life' Open University Press, 2001

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

Michael M.G. & Michael K. (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](http://www.privacyconference2007.gc.ca/Terra_Incognita_program_E.html)

Nemeth A. (2011) 'Australian Street Photography: Legal Issues' Andrew Nemeth, 2000-, at <http://4020.net/words/photorights.php>

---

### **Acknowledgements**

An earlier version of this paper was presented at a Conference on Surveillance and/in Everyday Life, University of Sydney, 20-21 February 2012.

---