# The Regulation of Point of View Surveillance:

# A Review of Australian Law

# 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 August 2012

#### **Abstract**

This paper presents the results of a review of contemporary regulatory controls on the use of Point of View Surveillance technologies under Australian law. Law enforcement agencies have considerable scope to apply them, whereas the rights of individuals are more circumscribed and less clear. Because of the technology's applicability to both sur- and sousveillance, a more balanced regulatory framework is necessary.

#### 1. Introduction

During the last century, a variety of surveillance technologies have arrived, have been deployed, and have had impacts on society, both significantly positive and seriously negative. After emerging only in the late 1980s, digital cameras have quickly developed into a means of creating high-quality images and video, have become inexpensive, and have become sufficiently small to be not merely carried but also worn.

The concept 'Point of View' has been of significance in film-making for decades. Reductions in the size and weight of devices that can record and/or transmit images and video has resulted in the notion migrating into many additional contexts. The term 'Point of View Surveillance (PoVS) technologies' has emerged as a means of distinguishing these capabilities from other forms of monitoring of people through their actions, their communications, and the data-trails that they leave behind them.

This paper commences with a brief background on the nature of PoVS technologies, sufficient to establish that they are in need of coherent regulation. The main body of the paper presents a survey of the legal context within one country, Australia. Because it is a national jurisdiction with eight, diverse sub-national (State and Territory) jurisdictions, Australia embodies a rich set of alternative approaches, preoccupations and prevarications. Prospects for the emergence of a more effective framework are discussed.

# 2. Nature and Impacts

The defining feature of PoVS is that the camera is human-borne, and points away from the human, generally following the orientation of the person's head, hence enabling capture of the scene in the person's line-of-sight, or from the person's point-of-view. This differentiates it from, for example, fixed installations. Although the term is of recent origin, the concept is not, being traceable to at least 1980, when Steve Mann applied the term 'wearable computing' in particular to wearable cameras and head-mounted displays (Mann 1996, 1997). See also Velger (1998).

Many commentators use the term with considerable looseness, with some discussions also encompassing the use of cameras attached to other parts of a person's body, clothing or equipment, the use of cameras held in a human hand irrespective of the position relative to the person's eyes, and even the use of cameras installed in other devices, such as motor-vehicles, drones, and 'telepresence robots'.

There is also considerable laxness in the current literature in relation to the functionality involved in PoVS. A device may merely display image or video, in which case it may display it to the person themselves, or to others, by using not only image-detection but also transmission capabilities. It may or may not include an audio-stream. The stream(s) may be recorded, in which case the storage may be local, or remote. The live and/or recorded stream(s) may be limited to use by the individual, or they may be intended for use by others, and/or disclosed to others. The live video-stream may be raw, or processed, e.g. through image-enhancement or by 'augmenting' it, i.e. by overlaying additional images or animations over the raw feed. Another distinction, of considerable consequence in some applications, is between a single point-of-view and correlation among multiple points-of-view.

A wide range of actual and potential applications exists. Education and training can take advantage of PoVS to provide vicarious but highly realistic experience. People preparing litigation or seeking to stimulate prosecutions can use it to gather evidence that may have higher value in the court-room than testimony based entirely on their memories. Law enforcement agencies are using it to record scenes as experienced by an individual employee (or, increasingly, contractor), and in some circumstances to monitor developments in real time. Members of the public are also using it to record, and in some cases transmit, their experiences in dealing with organisations, particularly law enforcement agencies. This changes individuals from 'usees' to 'users'. The term 'sousveillance' was coined in order to distinguish this form of inverted observation – surveillance, by those who are usually observed, of those who are usually the observers (Mann et al. 2003).

The question arises as to what extent the use of PoVS technologies is authorised, tolerated or prohibited by law. The question is an important one, for several reasons. Some applications of PoVS promise considerable benefits, both economic and social, for individuals, groups, organisations and societies. There will be inevitable side-effects, however. A regulatory framework is essential in order to authorise highly desirable uses, preclude highly undesirable uses, and ensure the balancing of interests and the mitigation of unnecessary harm. Further, use of the technology can give rise to strong feelings on the part of those being subjected to unwanted observation and recording, and hence there is a considerable risk of breaches of the peace. Finally, the democratisation of PoVS, as a result of the emergence of low-cost and readily hidden devices, is bringing about a degree of change in the politics of surveillance. Powerful organisations and individuals are used to imposing surveillance on others but are little-used to having others impose it on them. Contrary to the optimistic view expressed in Brin (1998), however, the powerful have considerable capacity to avoid being monitored.

#### 3. Relevant Australian Laws

This section provides a brief survey of Australian law that does or may relate to PoVS. The analysis was undertaken by a non-lawyer, based on a mix of primary sources and readily-accessible and apparently credible secondary sources. Sources of particular value are Nemeth (2005-) and Arnold (2006). The analysis below inevitably includes some legal imprecisions. Given the extensiveness, complexity and uncertainty of the laws and their application, it is likely that it contains some misinterpretations and even errors. Its purpose is to assist in policy discussions not to be a source of advice.

The analysis commences with a consideration of how laws relating to private property affect access to it, and the use of PoVS devices while on it. The focus is on observation and capture of images, video and audio, with space-limitations precluding much attention being paid to subsequent use, disclosure and publication. The paper then identifies extant legislation whose specific purpose is to preclude some uses of surveillance devices and/or to authorise some other uses. The focus is then switched to the rather different provisions applying in public places. A further sub-section reviews laws that are designed to prevent sousveillance, or that have the effect of doing so.

### 3.1 PoVS in Private Places

Under the common law regarding real property, including leasehold, the lawful occupiers of land (i.e. owners or lessees) have a general right to prevent others from being on, or doing acts on, their land, even if an area is freely accessible to the public. That right exists for the nine Australian Crowns, as it does for any other owner. So government property requires no special legislation to create such a right. However, based on that law alone, the right may need to be exercised in order to declare that filming on the property is not permitted, and to be effective it may need to be communicated. It is far from clear whether the law prevents the use of recordings that were obtained without permission or in violation of a denial of consent or an instruction not to do so.

The rights attaching to real estate do not generally extend to preventing photos from being taken from outside the property. Government agencies and corporations sometimes act as though the law precludes such photography, but they are seldom able to quote any legal authority. There are some specific laws, however, such as that requiring authority to use a camera for commercial purposes in designated parts of the Sydney Harbour Foreshores (such as around the Opera House), under Regulation 4(1)(b). In the case of military establishments, the Defence Act (Cth) is relevant, incl. s.82. In the case of Commonwealth property more generally, the Crimes Act s.89 applies.

In various jurisdictions, statutes create specific authorisations and prohibitions relating to the use of visual surveillance devices on private

property. The Surveillance Devices Act (Cth) includes provisions that override the rights of real property owners and permit agencies to use a surveillance device on their land. The term 'surveillance device' includes a data surveillance device, a listening device, an optical surveillance device, a tracking device, and any combination of them.

Under ss. 1-27, any of a number law enforcement agencies can apply for a warrant from a judge or Administrative Appeals Tribunal member of their choice, from a select panel (as distinct from the agency having to take its chance as to who the duty judge might be). However, under ss. 28-36, the agency may in emergencies issue its own non-judicial warrants. This is subject to weak *ex post facto* controls. Warrantless surveillance is also authorised by ss. 37-40, under various circumstances, such as listening to or recording a conversation to which a law enforcement officer is a party. Under s. 37, entry to premises requires a warrant, but subjecting activities to surveillance from outside the premises does not. Under ss. 44-48, the surveillance activity can be not only surreptitious, but the fact that it was used can be subsequently suppressed.

The Act's purpose is to authorise activities by Commonwealth law enforcement agencies. It appears to be silent about uses by people other than law enforcement officers, and hence does not appear to affect the use of PoVS technologies by other organisations and individuals.

In the six States and two Territories, there have been two waves of legislation in relation to surveillance devices, and the situation differs greatly between jurisdictions. Four States have Surveillance Devices legislation, three passed over a decade ago and one more recently: Western Australia (1998) Victoria (1999), the Northern Territory (2000), and NSW (2007). Because of the differences and the complexities, general statements need to be expressed and interpreted cautiously; but, broadly, visual and/or aural surveillance of a private activity is likely to 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. However, the prohibition may not apply:

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

Hence it would seem likely, for example, that it is illegal for a third party to visually record a sex act in a toilet cubicle (e.g. DT 2007, involving two prominent sportspeople, Falzon and Williams), or for a third party to visually transmit a sex act between other parties (one interpretation of a 2010 incident at the Australian Defence Force Academy – ADFA). 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).

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', and guidance provided in the Queensland Courts Bench Handbook. Visual surveillance without consent is only precluded if the person would reasonably expect their actions to be private. However, the terms 'private act' and 'private place' are defined to restrict the terms' applicability to a very few, specific instances.

The other three jurisdictions have yet to regulate visual surveillance, but have remnant Listening Devices legislation – South Australia (1972), Tasmania (1991) and ACT (1992). 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. There is, however, a general prohibition on listening to or recording sounds generated by other people, again subject to various provisos.

There are Workplace Surveillance laws in NSW (2005) – which replaced an earlier statute of 1998, and ACT (2011). However, these merely require that the surveillance be declared; or, if the surveillance is to be covert, it requires a good reason and a magistrate's approval. Some other States and Territories may preclude surveillance in toilets, bathrooms, and change-rooms, at least in workplace contexts.

## 3.2 PoVS in Public Places

The Surveillance Devices Act (Cth) s.37 authorises multiple law enforcement agencies to use optical surveillance devices, in public places, without a warrant, provided that "there is no entry to premises without permission and no interference with any vehicle or thing".

Across the States and Territories, visual surveillance in public places appears not to be subject to general prohibitions except under a small number of circumstances. The Surveillances Devices Acts of Victoria, WA and NT, for example, prohibit the use of visual and aural surveillance devices, but only if the person(s) whose behaviour is observed or recorded had a strong case for expecting that the behaviour would not be observed, transmitted or recorded. In NSW, visual and aural surveillance in a public place is only precluded if the person would reasonably expect their actions to be private, and if they are engaging in a private act. The term 'private act' is defined to include a very few, specific instances. In South Australia, Tasmania and the ACT, Listening Devices legislation contains no provisions in relation to video surveillance. There is, however, a general prohibition on listening to or recording other people, again subject to various provisos.

Censorship laws at Commonwealth, State and Territory levels place some limitations on acts that are permitted to be the subject of PoVS. 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 conequences emerged. A lead has been provided in this area by the Queensland Criminal Code in 2005, 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 provisions, 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 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.

Despite a great deal of moral breast-thumping from time to time about the recording of images of children, there appears to be no general prohibition on such activities. Similarly, copyright, trademark and defamation laws appear to have very limited practical impact on the use of PoVS technologies.

#### 3.3 Counter-PoVS Laws

Apart from the prohibitions discussed above, individuals who object to being subjected to surveillance have a few other potential avenues of protection, including the torts of trespass against property, confidence, negligence, nuisance, trespass against the person, harassment and stalking (Clarke 2012). All are, however, very limited in their application.

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: common assault, affray, threatening to destroy or damage property, aggravated assault, battery, coercion, malicious damage, destroying or damaging property, false imprisonment, and theft, robbery or stealing (Clarke 2012b). A person using PoVS technology, even if doing so in a unreasonable manner, has access to far more protections than the person who they are monitoring.

Consideration also needs to be given to the scope for organisations to prevent members of the public applying PoVS technologies for the purpose of sousveillance. Law enforcement agencies in particular may have the legal capacity to take action to prevent the use of PoVS equipment, interfere with PoVS equipment, or confiscate it and/or data deriving from its use. This document considers the constraints that arise from legal authority to seize devices that have functionality relevant to sousveillance. The focus is primarily on the powers of law enforcement agencies, but the scope exists for some other organisations and individuals to take similar actions, including national security agencies, other government agencies including local councils, corporations and not-for-profit associations, and even members of the public.

The scope of the analysis was restricted to the following set of possible constraints:

- powers to require that particular actions be taken by the person in relation to PoVS devices, including:
  - not using them to observe or record particular activities, or in particular places
  - the deletion of existing recordings of particular activities
- powers to take particular actions in relation to PoVS devices, including:
  - their seizure, i.e. the removal of them from the person's possession
  - the deletion of existing recordings of particular activities
  - their confiscation, i.e. retention of them indefinitely, or for a considerable period of time
  - the disablement of particular functionality
  - the infliction of damage to them
  - their destruction

The scope of the analysis did not extend to measures taken by someone subjected to sousveillance to obscure their activities, nor to powers to exclude people seeking to exercise sousveillance from the location of an activity, or to remove them from it.

A scatter of laws exists that do or may create constraints of these kinds in Australia. Some are Commonwealth laws, and others are State and Territory laws. Some derive from the common law, and others from statute. There is little coherence or consistency among them. This section is limited to the situation in NSW.

An array of such powers were granted to NSW Police in relation to a meeting of a regional body called the Asia Pacific Economic Cooperation (APEC) in 2007. These were contained in s.13 of the APEC Meeting (Police Powers) Act

2007 (NSW). It was speculated that the powers might be retained or extended (e.g. Clennell 2008), but the provisions were in fact restricted to a location and a time-period, and the Act was subsequently repealed.

Since 2002, however, the Law Enforcement (Powers & Responsibilities) Act has enabled NSW Police to self-authorise special powers in public places in the event of what it judges to be "public disorder". The powers include stop and search without warrant (s.21). Another power is to seize and detain, originally, a communication device, but since 2007 any "thing, if [its] seizure and detention ... will assist in preventing or controlling a public disorder" (s.87M). Nominally, the onus is on the NSW Police to justify the self-declaration of the special powers, but s.87D is very weak in this regard. Further, the onus is nominally on the individual policeman to justify their actions, but there is an apparent lack of any real controls.

Various powers are also asserted by law enforcement agencies to be available to them under the Anti-Terrorism Act. In one reported case in Kings Cross in Sydney, well-known identity Nick Holmes a Court had his camera-enabled Blackberry confiscated without apparent justification, and reports on the case suggested that previous instances had come to light (TW 2008, CM 2008). One possible authority is the offence of resisting or hindering a police officer in the execution of their duty, under s.546C of the NSW Crimes Act 1900. A further possibility is the Anti-Terrorism Act (No. 2) 2005 - Schedule 5. The plethora of anti-terrorism laws passed since 2001 are a veritable rat's nest of possibilities.

# 4. Prospects

This section briefly summarises deficiencies in existing laws, and identifies proposals for changes to Australian laws that have been put forward by law reform bodies, but ignored. A framework for a more effective regulatory framework is suggested.

#### 4.1 Deficiencies

The scatter of laws identified in the previous section evidence a range of deficiencies. It appears likely that deficiencies of these kinds exist in the regulatory framework for PoVS in many jurisdictions.

A general concern is that few jurisdictions have laws based on deep analyses and calm consideration of the many competing interests. As outlined in the following sub-section, for example, several Australian law reform commissions have conducted studies, but legislatures have shown little interest in their findings. The pace of technological change has been rapid, and this naturally poses challenges for the law. However, bureaucratic lawyers in many countries have sought to avoid performing the deep

analyses necessary to address the issues by inventing a 'technology-neutrality' mantra. This rests on the pretext that law can be blind to technology and still be effective.

In many jurisdictions, laws have been created to authorise some or all law enforcement agencies to apply PoVS technologies, frequently with little evidence in support of the measures, without open public debate prior to passage, and creating excessive powers with inadequate controls. These deficiencies have been particularly marked since September 2001, with many legislatures continuing to pass in panic any Bill that has the term 'national security' associated with it.

Another important problem is the difficulty for the public to understand what laws exist, and how they apply to the use of PoVS technologies. Guidance is signally lacking in relation both to use by organisations, and to use by individuals against organisations.

# 4.2 Past Proposals for Change

In Australia, several Law Reform Commissions (LRCs) perform studies and publish reports, which are in most cases entirely ignored by parliaments. In some cases, specific Recommendations may be lifted out of context and implemented, and in others, weakened versions may be enacted, sometimes many years after the Recommendations were made. The following LRC Reports are known to have been published:

- almost 30 years ago, the Australian Law Reform Commission appears to have addressed some aspects relevant to the issues (ALRC 1983, around para. 1125)
- in 1995, the then NSW Privacy Committee provided Recommendations in relation to surveillance in the workplace (NSWPC 1995). This gave rise to a statute in 1998, which was replaced in 2005 by one of wider scope but that is highly friendly to employers and contains very weak protections for employees
- in 2005, the Standing Committee of Attorneys-General issued a Discussion Paper relating to Unauthorised Photographs (SCAG 2005), and large numbers of submissions were made in response to it; but like most SCAG documents, nothing further happened after that
- in 2005, the NSW Law Reform Commission made Recommendations in relation to both Overt Surveillance (Appendix 1) and Covert Surveillance (Appendix 2) (NSWLRC 2005)
- in 2008, the Australian Law Reform Commission briefly discussed surveillance, but failed to make any Recommendations (ALRC 2008). However, Recommendation 74-1 re a Statutory Cause of Action lists as an example of a serious invasion of privacy: ... (b) where an individual has been subjected to unauthorised surveillance

• in 2010, the Victorian Law Reform Commission recommended a law and a set if guiding principles for the responsible use of surveillance devices in public places (Appendix 3) VLRC 2010)

#### 4.3 A Normative Framework

A broad set of principles is needed for the regulation of surveillance of all kinds. One such set was proposed in Clarke (2007), and subsequently applied specifically to visual surveillance (APF 2009).

The following are proposed as the key requirements:

- 1. **Justification**. A clear explanation must be provided by the proponents, showing why the authorisations and prohibitions are needed. The explanation must be supported by evidence and systemic reasoning, and not merely rely on assertions. The well-established processes of Privacy Impact Assessment (PIA) must be applied
- 2. **Proportionality**. The positive benefits need to be sufficient to justify the privacy-intrusiveness involved, and the design must be no more invasive than is justified. Less privacy-invasive alternatives must have been considered, and their inadequacies documented. Unavoidable negative privacy impacts must be the subject of mitigation measures
- 3. **Openness / Transparency**. Sufficient information must be published in advance of the deliberations to enable meaningful debate. The law must be sufficiently clear that its implications can be understood, and explanatory material must be prepared and must be readily available
- 4. **Controls**. Authorisations must require judicial warrant, and must be subject to pre- and post-controls. The controls must relate to specific justification, and security safeguards in relation to collection, transmission, storage, use, disclosure, publication, retention and destruction
- 5. **Accountability**. Breaches must be subject to sanction, with arrangements in place to ensure enforcement. The regime as a whole must be subject to periodic review, and adapted or withdrawn depending on the findings made in relation to the need for the regime and its effectiveness

#### 5. Conclusions

It is entirely understandable that rapid technological development will undermine existing laws. What is not acceptable is that incoherent and unbalanced laws should remain in place. There is a considerable imbalance between authorisations for law enforcement agencies on the one hand, and public rights in relation to PoVS on the other. A framework is available within which the problems can be addressed, and specific recommendations

are available from a number of law reform agencies. Governments and legislatures need to rise from their torpor and address these issues.

#### References

ALRC (1983) 'Privacy' Australian Law Reform Commission, ALRC 22, 1983

ALRC (2008) 'Impact of Developing Technology on Privacy: Surveillance technologies' paras. 9.89-9.84, Australian Law Reform Commission, August 2008, at

http://www.alrc.gov.au/publications/9.%20Overview%3A%20Impact%20of%20Developing%20Technology%20on%20Privacy/surveillance-technologies

APF (2009) 'Policy Statement re Visual Surveillance, incl. CCTV' Australian Privacy Foundation, October 2009, at

http://www.privacy.org.au/Papers/CCTV-1001.html

Arnold B. (2006) 'Unauthorised Photos' Caslon Analytics, November 2006, at http://www.caslon.com.au/photonote.htm

Brin D. (1998) 'The Transparent Society' Addison-Wesley, 1998

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

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

Clennell A. (2008) 'Tough police powers outlive APEC' Sydney Morning Herald, 12 March 2008, at http://www.smh.com.au/news/national/tough-police-powers-outlive-apec/2008/03/11/1205125911459.html

CM (2008) 'BlackBerry seizure an 'abuse of police powers' The Courier-Mail, 25 December 2008, at http://www.couriermail.com.au/police-snatch-blackberry/story-fna7dq6e-1111118412772

DT (2007) 'Toilet tryst picture' The Daily Telegraph, 12 April 2007, at http://www.dailytelegraph.com.au/entertainment/toilet-tryst-picture/story-e6frewyr-1111113329395

Mann S. (1996) 'Smart Clothing: The Shift to Wearable Computing' Communications of the ACM 39, 8 (August 1996) 23-24, at http://www.eyetap.org/papers/docs/acm\_comm96.pdf

Mann S. (1997) 'An historical account of the 'WearComp' and 'WearCam' inventions developed for applications in 'Personal Imaging' Proc. ISWC, 13-

14 October 1997, Cambridge, Massachusetts, pp. 66-73, at http://www.wearcam.org/historical/

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

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

NSWLRC (2005) 'Surveillance' Report 108, NSW Law Reform Commission, 2005, at

http://www.lawlink.nsw.gov.au/lawlink/lrc/ll\_lrc.nsf/pages/LRC\_r108toc

NSWPC (1995) 'Invisible Eyes:Report on Video Surveillance in the Workplace' NSW Privacy Committee, August 1995, at http://www.austlii.edu.au/au/other/privacy/video/index.html

NSWLRC (2005) 'Surveillance' Report 108, NSW Law Reform Commission, 2005, at

http://www.lawlink.nsw.gov.au/lawlink/lrc/ll\_lrc.nsf/pages/LRC\_r108toc

NSWPC (1995) 'Invisible Eyes:Report on Video Surveillance in the Workplace' NSW Privacy Committee, August 1995, at http://www.austlii.edu.au/au/other/privacy/video/index.html

SCAG (2005) 'Unauthorised Photographs on the Internet and Ancillary Privacy Issues' Discussion Paper, Standing Committee of Attorneys-General, Canberra, 2005

Velger M. (1998) 'Helmet Mounted Displays and Sights' Artech House, 1998

### Acknowledgements

An earlier version of this paper was presented at the International Workshop on Point of View Technologies in Law Enforcement, Sydney University, 22 February 2012.