NSW LAW REFORM COMMISSION

REPORT 108

Surveillance: Final report

May 2005

New South Wales. Law Reform Commission.

Sydney 2005

ISSN 1030-0244 (Report)

National Library of Australia

Cataloguing-in-publication entry

New South Wales. Law Reform Commission.

Surveillance: final report.

Bibliography.

Includes index.

ISBN 0 7347 2613 9.

1. Privacy, Right of – New South Wales. 2. Electronics in criminal investigation – New South Wales. 3. Electronic surveillance – New South Wales. I. Title. (Series : Report (New South Wales. Law Reform Commission); 108).

345.944052

NEW SOUTH WALES LAW REFORM COMMISSION

Letter to the Attorney General

To the Honourable Bob Debus MLC
Attorney General for New South Wales

Dear Attorney

Surveillance: Final report

We make this Report pursuant to the reference to this Commission received October 1996.

The Hon Justice Michael Adams
Chairperson

The Hon Justice Michael Adams

Hon Gordon Samuels AC CVO QC

Associate Professor Jane Goodman-Delahunty

Acting Judge Michael Chesterman

Professor Michael Tilbury

May 2005

TABLE OF CONTENTS

Terms of Reference

In October 1996, the then Attorney General, the Hon JW Shaw, QC MLC, asked the Commission to inquire into and report on:

- the scope and operation of the *Listening Devices Act 1984* (NSW);
- the need to regulate the use of visual surveillance equipment; and
- any related matter.

In undertaking the reference, the Commission was to have regard to:

- the protection of individual privacy;
- the views and interests of users of surveillance technology, including law enforcement agencies, private investigators, and owners of private premises, such as banks, service stations and shops; and the use of surveillance technology in public places.

Participants

Pursuant to s 12A of the *Law Reform Commission Act 1967* (NSW) the Chairperson of the Commission constituted a Division for the purpose of conducting the reference. The members of the Division are:

The Hon Justice Michael Adams

Hon Gordon Samuels AC CVO QC

Associate Professor Jane Goodman-Delahunty

Acting Judge Michael Chesterman

Professor Michael Tilbury (Commissioner-in-Charge)

Officers of the Commission

Executive Director	Mr Peter Hennessy
Legal Research and Writing	Ms Donna Hayward
	Ms Judy Maynard
Librarian	Ms Anna Williams
Desktop Publishing	Mr Terence Stewart
Administrative Assistance	Ms Wendy Stokoe

RECOMMENDATIONS

Recommendation 1 – see page 70
The use of overt surveillance should be in accordance with the proposed Surveillance Act. For the purposes of the proposed Act the following are the Overt Surveillance Principles:

Overt Surveillance Principle 1:
Overt surveillance must only be undertaken for an acceptable purpose.

Overt Surveillance Principle 2:
Overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy.

Overt Surveillance Principle 3:
Overt surveillance must be conducted in a manner that is appropriate for purpose.

Overt Surveillance Principle 4:
Notice provisions shall identify the surveillance user.

Overt Surveillance Principle 5:
Surveillance users are accountable for their surveillance devices and the consequences of their use.

- Public sector surveillance users and private non-domestic surveillance users, as part of their compliance with this Principle, must maintain a register containing such details as the number, types and locations of all their overt surveillance devices. Regulations should specify the details required, together with criteria identifying private surveillance users to whom this requirement applies.
- News gathering equipment operated by media organisations is exempt from any requirement to be listed in a register of surveillance devices.

Overt Surveillance Principle 6:
Surveillance users must ensure all aspects of their surveillance system are secure.

- This does not apply to media organisations in the context of their news gathering activities.

Overt Surveillance Principle 7:
Material obtained through surveillance to be used in a fair manner and only for the purpose obtained.

Overt Surveillance Principle 8:
Material to be obtained through surveillance to be destroyed within specified period.

- Material obtained overtly and genuinely for media purposes is exempt from this Principle.

Recommendation 2 – see page 72
With respect to the regulation of overt surveillance, the Privacy Commissioner should have the following powers and functions:

- promoting, and providing assistance (eg, educational) for, compliance with the Overt Surveillance Principles;
- assisting surveillance users in drafting codes of practice;
- appointing inspectors to investigate complaints, and to conduct both routine and random inspections of surveillance systems or devices to ascertain compliance with the proposed Act;
- right of entry to non-residential premises to inspect surveillance systems or devices to ascertain compliance with the proposed Act;
- educating the public on the acceptable use of surveillance devices.

Recommendation 3 – see page 92
Recommendation 54 should be amended to require the issuing authority to have due regard to the role of the media in upholding the public interest. The revised recommendation would read as follows:

In determining whether to grant an authorisation to conduct covert surveillance in the public interest, the issuing authority should have regard to:

- the nature of the issue in respect of which the authorisation is sought;
- the public interest (or interests) arising from the circumstances;
- the extent to which the privacy of any person is likely to be affected;
- whether measures other than covert surveillance have been used or may be more effective;
- the intended use of any information obtained as a result;
- the role played by the media in upholding the public interest; and
- whether the public interest (or interests) involved justifies the displacement of individual privacy in the circumstances.

Recommendation 4 – see page 92
The Commission recommends that an additional dot point should be added to Recommendation 81, clarifying that material obtained lawfully in accordance with the terms of a covert surveillance authorisation may be communicated, published or broadcast in accordance with that authorisation (See Recommendation 5 below).

Recommendation 5 – see page 92
The Commission recommends that Recommendation 82 should be amended to clarify that, where the applicant for a public interest authorisation is a media organisation, the authorisation should specify that the material may be broadcast or published at the discretion of the media organisation provided that it has been lawfully obtained within the terms of that authorisation.

1. Introduction

- Background to the reference
- Interim Report 98

BACKGROUND TO THE REFERENCE

Terms of Reference

1.1 In October 1996, the then Attorney General, the Hon JW Shaw, QC MLC, asked the Commission to inquire into and report on:

- the scope and operation of the *Listening Devices Act 1984* (NSW);
- the need to regulate the use of visual surveillance equipment; and
- any related matter.

1.2 In undertaking the reference, the Commission was to have regard to:

- the protection of individual privacy;

the views and interests of users of surveillance technology, including law enforcement agencies, private investigators, and owners of private premises, such as banks, service stations and shops; and

- the use of surveillance technology in public places.

Background to previous publications

1.3 In May 1997, the Commission released a short Issues Paper (IP 12) outlining what it considered to be the major issues at that time, and inviting responses from key surveillance users, privacy advocates and interested individuals. From the submissions received in response to IP 12, it became clear that the issues were far broader than first thought. Surveillance technology was developing rapidly, with the boundaries between the types of technology converging and becoming more difficult to distinguish. It was no longer feasible to look at specific devices in isolation, or particular users, since the technology was open to everyone. For example, video and sound recording were more frequently than not conducted by a single device; digital video and photography has resulted in images being easily stored on computers and transmitted through email systems and the internet; mobile phones have increasingly been used as tracking devices and cameras, and can also have internet capacity. Indeed, the boom in the use of the internet and email alone since 1996, while hugely advantageous to business and communications, has also presented significant threats to the privacy of those communications, particularly in the workplace. The global and amorphous nature of the internet has also created enormous challenges for those seeking to regulate its potential abuse.

1.4 Research and consultation following IP 12 also challenged the traditionally held view that surveillance of “public” activity was acceptable, but monitoring of activity conducted in private needed more stringent controls. The sophistication of the technology has increased the capacity to penetrate what once would have been considered to be the “private” sphere, without the need to trespass or to alert those under observation in any way. This has made many of the common

law remedies for such activity inapplicable, or at least toothless. The proliferation of surveillance devices in places such as shopping centres, railway stations, and in and on public transport, has heightened public expectation that activities will be electronically recorded, whereas ten or fifteen years ago this would not have occurred to most people. The increased availability and affordability of surveillance devices has also meant that anyone may conduct surveillance of the most intrusive nature, once regarded the domain of law enforcers or private investigators. While all of these developments have brought undisputed benefits, privacy advocates worry that the line between public and private worlds has become so blurred and easily crossed, that the concept of a private life is ceasing to have any significance. In the Commission's view, the regulation of surveillance could not continue to be viewed in terms of public or private places or uses.[1]

1.5 The Commission's attention was also focussed on the type of activity that constituted surveillance. A watershed moment occurred in 1997 with the death of Diana, Princess of Wales, while being pursued by paparazzi, which challenged the traditional views of what constituted surveillance. This sparked a storm of controversy over the role of the media in conducting surveillance, the adequacy or otherwise of the regulation of media surveillance, and their responsibility for its end product.

1.6 It was against this background that the Commission developed the recommendations in Interim Report 98. What was most starkly apparent to the Commission when undertaking research for its Interim Report was the complete inadequacy of the current piecemeal, device-specific legislative models to meet the issues presented by modern and developing technology. At the time of writing Report 98, legislation in NSW regulated only the use of listening devices,[2] of video surveillance in the workplace, and the use of surveillance by some government agencies (excluding the police) to collect personal information.[3] The Commission considered that expanding the existing model to add devices would be equally inadequate. What was needed was an approach as broad and flexible as the technology it purported to regulate.

INTERIM REPORT 98

1.7 In February 2001, the Commission delivered Interim Report 98 to the Attorney General, the Hon Bob Debus, MP. The decision to release an Interim Report rather than a Discussion Paper was made because the Commission had developed fairly firm recommendations. However, since the scope of material covered was so much broader than that in the Issues Paper, the Commission was of the view that an Interim rather than a Final Report was more appropriate, considering that it may be desirable to conduct further consultation.

1. The Commission discusses the erosion of the distinction between public and private spaces in New South Wales Law Reform Commission, *Surveillance: An Interim Report* (Report 98, 2001) Chapter 2.
2. Including listening devices with video or tracking capacity: see *Listening Devices Act 1984* (NSW) s 3(1A).
3. That situation is largely unchanged. See ch 2 for a discussion of legislative changes or proposals since 2001.

Major recommendations

1.8 In Report 98, the Commission recommended a broad legislative approach to regulating surveillance conducted both overtly and covertly, through the use of any type of surveillance device, and by any surveillance user. A comprehensive overview of the Commission's recommended framework can be found in Report 98 at Chapters 1 and 2. The Commission recommended that "surveillance device" be defined to mean "any instrument, apparatus or equipment used either alone, or in conjunction with other equipment, which is being used to conduct surveillance".[4] Surveillance should be defined as "the use of a surveillance device in circumstances where there is a deliberate intention to monitor a person, a group of people, a place or an object for the purpose of obtaining information about a person who is the subject of the surveillance".[5] Those definitions are deliberately circular so as to exclude the use of a surveillance device for purposes other than conducting surveillance (for example, recreational photography or filming a wedding or child's birthday party).[6] The definitions also exclude surveillance conducted only by the human senses, without the use of a surveillance device.

1.9 Since overt and covert surveillance both raise privacy issues, the Commission recommended that they should both be regulated under the proposed legislation. However, because different policy questions arise depending on whether surveillance is conducted overtly or covertly, the Commission recommended two different regulatory schemes. As such, distinguishing between overt and covert surveillance is crucial, since that will determine which system of regulation would apply. According to the Commission's recommendations, surveillance would be considered to be overt in circumstances where the subject of the surveillance had notice that the surveillance was occurring. Surveillance conducted in all other circumstances would be considered covert. Adequate notice would be proven to be given through any of the following or similar means:

- signs which are clearly visible and widely understood (for example, by people from non-English speaking backgrounds and people with a disability); or
- other warnings of the type of surveillance occurring, such as audio announcements or written notification (where practicable); and
- surveillance equipment which is clearly visible and recognisable.[7]

4. See Report 98, Recommendation 1 at para 2.36.
5. See Report 98, Recommendation 2 at para 2.39. The Report recommends that "monitor" be defined as listening to, watching, recording, or collecting (or enhancing the ability to listen to, watch, record or collect) words, images, signals, data, movement, behaviour or activity: Recommendation 3 at para 2.39.
6. Since this activity is not conducted for the purpose of monitoring, but as an electronic keepsake: see Report 98 para 2.65-2.67, and para 3.4-3.8 of this Report for further explanation.
7. See Report 98, Recommendation 10 at para 2.79. Due to the more specific rights and responsibilities owed to employers and employees, additional notice requirements are recommended for surveillance conducted in the workplace: see Report 98, Recommendations 11 and 12 at para 2.80-2.82. Also, the Commission recognised the difficulty that the notice requirements may pose for the media, and consequently

1.10 Examples of overt surveillance are CCTV cameras in shopping centres or railway stations, etc. The Commission recommended that overt surveillance should be regulated by a series of principles set out in the legislation (similar to the Information Protection Principles in the *Privacy and Personal Information Act 1998* (NSW)), to be supplemented by Codes of Practice. The eight principles developed by the Commission were:

1. Overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy.

2. Overt surveillance must only be undertaken for an acceptable purpose.

3. Overt surveillance must be conducted in a manner which is appropriate for purpose.

4. Notice provisions shall identify the surveillance user.

5. Surveillance users are accountable for their surveillance device and the consequences of their use.

6. Surveillance users must ensure all aspects of their surveillance system are secure.

7. Material obtained through surveillance to be used in a fair manner and only for the purpose obtained.

8. Material obtained through surveillance to be destroyed within a specified period.[8]

1.11 Under the Commission's recommendations, failure to comply with the principles would be an offence. The recommendations concerning the regulation of overt surveillance are discussed in detail in Chapters 3-4 of Report 98.

1.12 Since covert surveillance represents a more significant invasion of individual privacy than surveillance conducted overtly, the Commission recommended a more stringent system of prior authorisation by an independent arbiter before it may be conducted, based on the models currently in the *Listening Devices Act 1984* (NSW) and the *Workplace Video Surveillance Act 1998* (NSW). Accordingly, the Commission recommended that anyone wanting to use a surveillance device without the knowledge of the subject of the surveillance needs to obtain prior authorisation, based on affidavit evidence demonstrating the need for the surveillance. The type of authorisation required, and the body from which it should be obtained, would depend on whether the surveillance was being conducted by a law enforcement officer, in an employment

---

recommended that, in certain cases, surveillance will be deemed to be overt even if the notice requirements are not met: see Recommendation 18.

8. See Report 98, para 4.38-4.66.

context or in the public interest.[9] In an emergency situation, where prior authorisation is not possible or practicable, the Commission recommended that authorisation should be available retrospectively.

1.13 The Commission also recommended a series of measures designed to promote accountability for the conduct of covert surveillance and the use of the material obtained as a result. Breach of the provisions regarding covert surveillance would amount to a criminal offence. This is consistent with the current LDA and WVSA.

1.14 In addition, the Commission recommended that a civil action for damages should be available in certain circumstances where a breach of the proposed legislation has occurred. It is envisaged that this would operate in a similar way to the complaints and review mechanisms under the *Anti-Discrimination Act 1977* (NSW).[10]

Reasons for the Commission's approach

1.15 The rationale for the nature and scope of the recommendations made by the Commission are detailed in Chapter 2 of Report 98. In that Chapter, the Commission explains:

- the reasons for adopting a broad, inclusive, non-device specific approach;[11]
- what activity is and is not included within the scope of the recommendations;[12]
- why the regulatory scheme is based on the distinction between overt and covert surveillance and not on the public/private distinction favoured in other surveillance legislation;[13]
- why the media have not been exempted from the scope of the Commission's recommendations;[14] and
- why the recommended legislation should have privacy as its paramount concern.[15]

Some of these issues are revisited and clarified in Chapter 3 of this Report.

9. See Report 98, Chapters 5-7 for detailed recommendations concerning the regulation of covert surveillance by law enforcement officers, in the public interest and in employment, respectively.
10. See Report 98, Chapter 10 for a discussion of the recommended methods of dealing with breaches of the proposed new legislation.
11. See Report 98, para 2.8-2.32 for a discussion of the scope of the Commission's recommendations.
12. See Report 98, para 2.40-2.76.
13. See Report 98, para 2.20-2.27.
14. See Report 98, para 2.56-2.61.
15. See Report 98, para 2.4-2.7.

Difficult or controversial aspects

1.16 Some of the recommendations in Report 98 contain difficult or controversial aspects that are either inherent in the subject matter of surveillance and the Commission's approach to its regulation, or have emerged through events occurring since the publication of the Report. In particular, the more difficult areas include:

- vehement objection by the media to its inclusion within the scope of the proposed legislation;[16]
- the need to regulate email and internet surveillance, yet the difficulty of doing so, both constitutionally and practically, at a State level;
- the increased prominence and acceptance of surveillance as an anti-terrorism measure post-September 11, and the corresponding decrease in sympathy for privacy arguments;
- resentment of the fact that, since surveillance technology has dramatically outpaced the law, the proposed legislation would be regulating activity that is currently unregulated; and
- apparent confusion over the practical implications of the recommendations, eg, what is or is not covered.

This Report

Developments since Report 98

1.17 The Attorney General tabled Report 98 in Parliament in December 2001. At the same time, he wrote to the Commission asking for further consultation to be conducted concerning the impact of the Commission's recommendations on media organisations, and asking the Commission to consider the effect of a High Court Decision involving media surveillance handed down in November 2001. The Commission has received submissions from a number of media organisations regarding their views on Report 98, and a meeting was held with those organisations in July 2002.

1.18 Due to other work commitments, only a watching brief was kept over the surveillance reference until December 2003 when research was recommenced. The current post-September 11 environment is vastly different from the one in which Report 98 was written. As a result, issues have emerged that need to be examined in addition to the ones directed to the Commission by the Attorney General. For example, the impact wrought by the changing attitudes and legislative responses to surveillance as a result of the focus on anti-terrorism, and the increasing pressure to regulate electronic communications in the workplace.

16. See Chapter 3-5 for a discussion of the issues raised in submissions from media organisations.

The Commission's approach in this Report

1.19 In the course of writing this Report, the Commission has conducted extensive research into technological, social and legal developments in the field of surveillance, and analysed the relevant policy issues. The Commission has also undertaken targeted consultation with, and received submissions from, various media organisations. In addition, submissions have been received from insurers, Commonwealth and NSW government organisations, including Privacy NSW, individual private investigators, and others involved in the manufacturing, installation and maintenance of surveillance equipment.

1.20 The regulation of surveillance activity is a huge issue, and was comprehensively dealt with in Report 98. The legislative framework developed by the Commission in that Report was made deliberately flexible to avoid having to be revised every few years. Consequently, many of the issues that have emerged since Report 98 could all be accommodated under the Commission's recommended legislative model, without the need to amend the legislation each time a new device, or use for a device, emerged. For example, issues such as the proliferation of cameras in mobile phones, the desire of police to make more use of video surveillance, and the regulation of email surveillance in the workplace, could all be regulated under the recommendations in Report 98.

1.21 Hence, the Commission is of the view that it is unnecessary in this Report to revise every aspect of Report 98 since the overall framework and the great majority of recommendations made in the Interim Report remain sound. This Report discusses only those issues that need clarification or amendment as a result of legal or other developments that have occurred since 2001, or have been incorporated as a result of suggestions made in submissions. Hence, this Report cannot be read as a stand-alone document, and needs to be read in conjunction with Report 98.

1.22 In this Report, the Commission provides an update of the way in which surveillance activity is currently regulated at a State and Commonwealth level, and outlines some of the major legal developments that have occurred since the release of Report 98 that either result from, or impact upon, the Commission's recommendations.[17] The Commission has also carefully considered all views raised in submissions and consultations, and discusses any changes to our recommendations provoked as a result in Chapters 4 and 5.

1.23 The major focus of this Report is to consider the impact of the recommendations made in Report 98 on the activities of the media, as requested by the Attorney General. Submissions from media organisations were highly critical of the Commission's approach, both overall and with regard to specific recommendations. The Commission has examined all of the issues raised, and separated them into two categories: those which represent philosophical differences of opinion on broad issues such as the nature of privacy and surveillance;[18] and those relating to particular recommendations that may cause some practical difficulty.[19]

17. See ch 2.
18. These issues are discussed in ch 3.
19. Recommendations relating to overt surveillance are discussed in ch 4, while recommendations concerning covert surveillance are discussed in ch 5.

2. Recent legal developments

- Current regulation of surveillance
- Other legal developments since Report 98

CURRENT REGULATION OF SURVEILLANCE

2.1 Surveillance activity in Australia is regulated by a complex and, at times, confusing web of Commonwealth, State and Territory laws dealing variously with telephone intercepts and the use of surveillance devices. The coverage offered by each of these legislative schemes is currently piecemeal and inconsistent, and is largely geared towards the use of surveillance devices by law enforcement agencies. The Commonwealth and some States also have privacy statutes establishing principles regarding the collection, storage and use of personal information, which can include material obtained as a result of surveillance.

2.2 The Commission discussed the regulation of surveillance by statute and common law in detail in Chapter 1 of Report 98. The following section updates that information and focuses on two major developments: the struggle at Commonwealth level to find an appropriate means of regulating the interception of electronic communications, such as email; and the High Court decision concerning surveillance by the media in *Australian Broadcasting Company v Lenah Game Meats Pty Ltd*.[1]

Division of legislative responsibility between the Commonwealth and the States and Territories

Interception of telecommunications

2.3 The Commonwealth Constitution gives the Commonwealth Government the power to regulate "postal, telegraphic, telephonic and other like services".[2] This power is not exclusive to the Commonwealth, and co-exists with the residual powers of the States.[3] The Commonwealth has used this power to enact the *Telecommunications (Interception) Act 1979* (Cth) ("the Interception Act"), which prohibits, except where specifically authorised, the interception of communications passing over a telecommunication system.[4] The Interception Act was originally introduced to prohibit unauthorised telephone tapping. In the intervening years, other communications, such as email and telephone text messages, may be transmitted through telephone lines, and so the scope of communications covered by the Interception Act has been extended to include conversations or messages in the form of speech, music or other sounds, data, text, visual images or signals, or in any other form or combination of forms.[5] So far as telephone interceptions are concerned, it has been held that the Interception Act is intended to cover the field, thus displacing, by virtue of section 109 of the Constitution, any State legislation which might otherwise be applicable.[6] The situation with the interception of other

1. (2001) 208 CLR 199.
2. *Constitution Act* s 51(v).
3. *Constitution Act 1902* (NSW) s 5.
4. *Telecommunications (Interception) Act 1979* (Cth) ("Interception Act") s 7.
5. Interception Act s 5. However, the definition of "interception" refers only to "listening to or recording" such communications: s 6. See further discussion at para 2.11 below.
6. *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222 at 230; *Miller v Miller* (1978) 141 CLR 269.

communications is less clear, but the safe assumption is that any communication intercepted during its passage across a telecommunications system would be regulated exclusively by Commonwealth law.

2.4 The Interception Act applies only to covert communications,[7] and only to "live" communications intercepted whilst in transit. Thus, should a telephone conversation be recorded through the use of a tape recorder placed at the telephone receiver, this would be regulated by State or other Commonwealth surveillance laws since the surveillance of the communication occurred after it had completed its passage across the telecommunications system.[8] Similarly, surveillance of delayed access message services, such as voicemail, once they have reached the inbox of, and/or have been stored on equipment operated by, the recipient, are not currently regulated by the Interception Act.[9]

Regulation of surveillance devices

2.5 The Commonwealth and each State and Territory has surveillance laws covering various devices and activity. Certain Commonwealth laws regulate the use of listening devices by specific Commonwealth organisations, such as the Australian Federal Police ("AFP"), customs officials, and the Australian Security Intelligence Organisation ("ASIO").[10] Recently, the *Surveillance Devices Act 2004* (Cth) was passed by Commonwealth Parliament.[11] That Act incorporates and updates the surveillance provisions in the *Australian Federal Police Act 1979* (Cth) and the *Customs Act 1901* (Cth), described as being "outdated and inadequate in the face of progressively complex and covert criminal activity".[12] The Act regulates the covert use of data and optical surveillance devices, as well as listening and tracking devices, and applies to authorised employees of the AFP, the Australian Crime Commission ("ACC"), and State and Territory Police investigating certain Commonwealth offences,[13] or to the AFP and the ACC

7. This allows overt interception to occur without the need for a warrant. Organisations such the Australian Stock Exchange, Telstra and the 000 emergency line, routinely monitor calls overtly for the purpose of improving service quality or having a record of conversations in case of future allegations of improper conduct or coronial inquiries, etc: see Sydney Futures Exchange, *Submission* at 2; F Wood, "Your telephone calls: recording and monitoring" (1996) 3(1) *Privacy Law and Police Reporter* 14; and A Henderson and A McDonough, "Call monitoring – legalities and regulation" (February 1999) 2(8) *TeleMedia* 97 at 99.
8. See *T v Medical Board (SA)* (1992) 58 SASR 382.
9. This is discussed in more detail at para 2.11 and para 2.13-2.23 below.
10. The use of aural surveillance devices by Commonwealth agencies in the investigation of Commonwealth drug importation offences is regulated by the *Customs Act 1901* (Cth) s 219A-219K; the use of aural surveillance devices by the Australian Federal Police in the investigation of certain non-narcotics Commonwealth offences is regulated by the *Australian Federal Police Act 1979* (Cth) s 12B-12L; the use of aural, optical and computer surveillance devices by members of the Australian Security Intelligence Organisation is regulated by the *Australian Security Intelligence Organisation Act 1979* (Cth) s 25A-s 26C.
11. The *Surveillance Devices Act 2004* (Cth) came into effect on 15 December 2004.
12. *Surveillance Devices Bill 2004* (Cth) *Explanatory Memorandum* at 1.
13. See *Surveillance Devices Act 2004* (Cth) s 6.

investigating State offences with a federal aspect.[14] The Act does not affect the operation of State and Territory surveillance laws.

2.6 Originally, all States and Territories had legislation which regulated the use of listening devices, generally by prohibiting their use unless authorised under a judicial warrant or exempted from the need to obtain a warrant. Gradually, as technology developed, most of those listening device laws were amended to include other devices.[15] For example, South Australia recently expanded the ambit of its Listening Devices Act to become the *Listening and Surveillance Devices Act 1972* (SA), covering visual and tracking devices in addition to listening devices. Queensland has legislation which regulates the use of listening, tracking and visual surveillance devices by the police.[16] Western Australia, Victoria and the Northern Territory have replaced their listening devices laws with broader surveillance legislation. The *Surveillance Devices Act 1998* (WA) regulates listening devices, optical surveillance devices and tracking devices.[17] In Victoria, the *Surveillance Devices Act 1999* (Vic)[18] regulates the same devices as its Western Australian counterpart, but also covers data surveillance devices (defined as those that are capable of being used to record or monitor the input of information into or the output of information from a computer), when used by law enforcement officers.[19] The *Surveillance Devices Act 2000* (NT) covers listening devices, optical surveillance devices, tracking devices and data surveillance devices.[20]

2.7 In NSW, although the title of the LDA suggests that the legislation regulates only listening devices, its operation is slightly broader. "Listening device" is defined in the LDA to mean:

> *any instrument, apparatus, equipment or device capable of being used to record or listen to a private conversation simultaneously with its taking place.*[21]

The LDA was amended in 2000 to clarify that a listening device may also have a visual or tracking capacity.[22] The definition does not cover visual or tracking devices without an audio component, or computer or enhancement equipment.

---

14. State offences with a federal aspect are defined in *Surveillance Devices Act 2004* (Cth) s 7.
15. Except for Tasmania and the Australian Capital Territory, which still only regulate listening devices: see *Listening Devices Act 1991* (Tas) and *Listening Devices Act 1992* (ACT).
16. *Police Powers and Responsibilities Act 2002* (Qld) Part 2 and Schedule 4. This law does not cover the use of those devices by private individuals
17. *Surveillance Devices Act 1998* (WA) s 5-7.
18. Replacing the *Surveillance Devices Act 1999* (Vic).
19. *Surveillance Devices Act 1999* (Vic) s 3 and s 9. The 1999 Act was recently amended by the *Surveillance Devices (Amendment) Act 2004* (Vic) to implement the Model Laws on Cross Border Investigations: see discussion at para 2.35-2.38 below.
20. *Surveillance Devices Act 2000* (NT) s 3 and s 5.
21. LDA s 3(1).
22. LDA s 3(1A). This amendment was introduced as a result of the decision in *R v Peter Kay and Roula Kay* (District Court of NSW, Viney J, 22 October 1999, unreported) which questioned whether a multi-function device fell within the definition of "listening device": cf *R v McNamara* (1995) 1 VR 263.

2.8 NSW also has legislation specifically regulating the use of covert video surveillance in the workplace. The *Workplace Video Surveillance Act 1998* (NSW) enables employers to conduct video surveillance in the workplace if the employee has been given prior written notice of the surveillance, the surveillance cameras are clearly visible and there are visible signs notifying people that they may be under surveillance.[23] Surveillance that does not satisfy these criteria is considered covert video surveillance under the Act and is unlawful, unless an authorisation has been issued by a Magistrate.[24] A draft Bill amending this legislation has recently been released by the Government for public comment. The *Workplace Surveillance Bill 2004* (NSW) aims at extending the scope of the 1998 legislation to include the regulation of covert camera, computer and tracking surveillance of employees by employers.[25] The provisions of this draft Bill are discussed in more detail in Chapter 5.

Privacy laws

2.9 There are Commonwealth and NSW statutes that regulate the use of personal data that relates to individuals. The Commonwealth *Privacy Act 1988* (Cth) lays down strict Information Privacy Principles which Commonwealth government agencies must observe when collecting, storing, accessing and using personal information. In December 2001, the *Privacy Act 1988* (Cth) was extended to apply National Privacy Principles[26] to certain private sector organisations.[27] This legislation and others[28] would, for example, cover data-matching which involves bringing together data from different sources and comparing it to identify people for further action or investigation.[29] The *Privacy Act 1988* (Cth) contains various exemptions for certain agencies from the requirement to comply with the privacy principles, including an exemption for media organisations.[30]

---

23. *Workplace Video Surveillance Act 1998* (NSW) s 4.
24. *Workplace Video Surveillance Act 1998* (NSW) Part 2 and 3.
25. *Workplace Surveillance Bill 2004* (NSW) cl 3. The Bill specifically excludes the use of listening devices from its ambit.
26. *Privacy Amendment (Private Sector) Act 2000* (Cth). The National Privacy Principles cover the same broad areas as the Information Privacy Principles, but differ slightly to accommodate the environment in which commercial organisations operate.
27. Private sector organisations that are not required to comply with the Privacy Act include those with an annual turnover of less than $3 million (Privacy Act s 7B(2)(b) and s 6B(1)) and media organisations engaged in "the course of journalism": Privacy Act s 7B(4).
28. For example, the *Data-Matching Program (Assistance and Tax) Act 1990* (Cth) regulates the use of the tax file number in comparing personal information held by the Australian Taxation Office and by assistance agencies (Centrelink and the Department of Veterans Affairs).
29. For example, records from different government departments are often compared to identify people who are being paid benefits to which they are not entitled or people who are not paying the right amount of tax.
30. Under the *Privacy Act 1988* (Cth), a media organisation is exempt for the purposes acts done, or practices engaged in:
    (a) by the organisation in the course of journalism; and
    (b) at a time when the organisation is publicly committed to observe standards that:
        (i) deal with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters); and

2.10 In NSW, the *Privacy and Personal Information Act 1998* (NSW) contains a set of principles that regulate the way certain public sector agencies should deal with personal information. The principles do not apply to the private sector, and apply only to personal information, that is, any information that relates to an identifiable person. This definition covers not only traditional ideas of data storage such as paper files, but also such things as electronic records, video recordings, photographs, genetic material and biometric information, like fingerprints.[31]

Regulation of email and other electronic communications

2.11 As noted above, the regulation of telephone intercepts whilst the communication is in transit across a telecommunications system is the sole legislative responsibility of the Commonwealth. The situation is less clear regarding other communications carried by means of a telecommunications system. Although the Interception Act defines "communication" to include text or image-based material,[32] it defines "interception" only in terms of "listening to or recording" communications, which seemingly has no application to text or other non-voice communications.[33] A number of questions have surrounded the issue of determining what communications are covered by the Interception Act, and at what point a communication can be deemed to have passed across a telecommunications system, and thus not be within the scope of the Interception Act. For example, has an email finished its passage along a telecommunications line if it has been received by an employer's server, but has not yet reached the intended employee recipient? Similarly, what is the status of an email that is stored on the server of an Internet Service Provider ("ISP"), particularly where that email has not been accessed by the intended recipient?

2.12 The answers to these questions are significant for a number of reasons. First, determining the scope of the Interception Act provides clear guidance on when an interception warrant is necessary in order to access electronic communications. Secondly, and more significantly for the purpose of this Report, the clear operation of the Interception Act is necessary in identifying the limits of the legislative power of the States to regulate the surveillance of email and other electronic communications.

(ii) have been published in writing by the organisation or a person or body representing a class of media organisations: s 7B(4).

31. *Privacy and Personal Information Act 1998* (NSW) s 4(2).
32. Interception Act s 5.
33. Interception Act s 6(1). An attempt to extend the definition of "interception" to include "reading or viewing" a communication in its passage across a telecommunications system was recently rejected by the Senate Legal and Constitutional Legislation Committee: Australia, Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2004* (March 2004) at para 3.66. Other provisions of this Bill and the recommendation of the Senate Committee are discussed at para 2.14-2.19.

Stored electronic communications

2.13 The Commonwealth Government has made three attempts since Report 98 to amend the Interception Act to clarify the application of the Act to email and other electronic communications. Achieving such clarification has proved difficult, particularly in relation to delayed access message services, such as voicemail or email, where the communication may be stored for some time before being accessed by the recipient. As noted earlier, the Interception Act currently applies only to "real time" or "live" communications intercepted whilst in transit: the Act has no application to the interception or surveillance of communications after they have passed across a telecommunications system and reached the recipient, or when stored on the equipment of the sender or recipient.[34]

2.14 The first two attempts to amend the Interception Act to deal with stored communications were rejected by the Senate Legal and Constitutional Legislation Committee ("the Senate Committee") in 2002[35] and early 2004.[36] The 2002 Bill provided that a warrant was not necessary under the Interception Act to intercept stored communications where a telecommunications line was not being used (except for the purpose of turning on the equipment on which the communication was stored). The Senate Committee disagreed with this approach and asked the Government to reconsider the law with a view to requiring an interception warrant in such circumstances.[37]

2.15 The first 2004 Bill contained a similar provision, but also stated that an interception warrant was required where access was sought to a stored communication that had not been read by the intended recipient, unless such access could be gained by using equipment which the intended recipient could have used, but did not.[38] Submissions to the Senate Committee Inquiry into the first 2004 Bill raised a number of difficulties associated with the scope and effect of the proposed amendments. In particular, the Senate Committee heard that the Bill failed to offer sufficient clarification in relation to:

- the legality of accessing read emails at an ISP server with a search warrant (as opposed to an interception warrant);[39]

- the possible conflict between the Bill and the current powers of the Australian Federal Police to access remotely both read and unread emails from a computer under section 3L of the *Crimes Act 1914* (Cth);

---

34. See para 2.11.
35. *Telecommunications Interception Legislation Amendment Bill 2002* (Cth).
36. *Telecommunications (Interception) Amendment Bill 2004* (Cth).
37. Australia, Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications Interception Legislation Amendment Bill 2002* (May 2002) at para 4.17, Recommendation 5.
38. Provided that this did not require the use of a telecommunications line, except to the extent necessary for turning on the equipment: see *Telecommunications (Interception) Amendment Bill 2004* (Cth) proposed s 6(7).
39. This is currently legal. However, in practical terms it can be difficult to determine whether an email has been read or not. Accordingly, the effect of the proposed amendments would mean that an interception warrant, rather than a search warrant, would be necessary whenever a law enforcement officer was in doubt.

- the legality of reading emails after they have passed through an organisation's firewall (eg, for the purposes of internal security) but before they have reached the recipient.[40]

2.16 As a result of the persisting confusion and practical difficulties raised, the Senate Committee recommended that the amendments relating to reading, viewing or otherwise accessing delayed access or stored communications be deferred pending further clarification of the above issues.[41]

2.17 The Bill returned in revised form in May 2004 as the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* (Cth) ("the Stored Communications Bill"). That Bill provides that the Interception Act should have no application at all to stored communications, that is, the Act would only apply to "live" communications, and surveillance of any stored communications would not require an interception warrant to be obtained under the Interception Act.[42] However, a communication that is stored on a highly transitory basis as part of the integral function of the technology used in its transmission, is not considered to be a stored communications for the purpose of the Bill.[43] In his Second Reading Speech on the Bill, the Commonwealth Attorney-General, the Hon Philip Ruddock, MP, noted that the amendments address the "practical implications of modern technology on access to communications".[44] It is proposed that the amendments will have effect for 12 months only,[45] during which time the Attorney-General has requested his Department to undertake a comprehensive review of the Interception Act to ensure its "contemporary relevance" to modern electronic communications.[46]

2.18 Like the previous two amendments, the Stored Communications Bill was sent to the Senate Legal and Constitutional Legislation Committee for inquiry. Many submissions to the inquiry endorsed the need to bring clarity to this complex area, and also noted the inadequacy of the Interception Act (introduced 25 years ago to regulate the interception of land based telephone systems) in dealing with modern, convergent electronic communications.[47] Others raised concerns regarding the privacy implications of not requiring an interception warrant to

40. See Senate Committee Report at para 3.55-3.66.
41. See Senate Committee Report at para 3.66 and Recommendation 1 at para 4.33. See also Australia, *Parliamentary Debates (Hansard)* House of Representatives, 1 April 2004 at 28073. The Government agreed to this recommendation and omitted those provisions from the Bill which passed into law on 27 April 2004.
42. Proposed s 7(2)(ad). A general search warrant would still be required to access stored communications.
43. Stored Communications Bill, proposed s 7(3). The Bill provides the example of momentary buffering (including momentary storage in a router in order to resolve a path for further transmission) as an illustration of storage on a highly transitory basis.
44. Australia, *Parliamentary Debates (Hansard)* House of Representatives, 27 May 2004 at 29309.
45. Proposed s 7(3A).
46. Australia, *Parliamentary Debates (Hansard)* House of Representatives, 27 May 2004 at 29309.
47. Australia, Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* (July 2004) at para 3.3-3.7.

access stored emails, particularly where they had not been read by the intended recipient.[48] The view was also expressed that, although ordinary search warrants would be required to access stored communications in most cases, they did not provide the same level of scrutiny and accountability as interception warrants.[49]

2.19 The Committee was of the view that there is a genuine need to ensure clarity in the application of the Interception Act in terms of enabling access to stored communications, and was satisfied that the provisions of the Stored Communications Bill were satisfactory in achieving such clarity.[50] The Committee recommended that the Stored Communications Bill should proceed, subject to being amended to refer specifically to the review of the Interception Act ordered by the Commonwealth Attorney General. The Committee also further recommended that the review should be conducted publicly, and should consider the issue of whether stored communications should continue to be exempt from the Interception Act.[51] The Stored Communications Act was passed by Commonwealth Parliament in December 2004.[52]

The role of State email surveillance laws

2.20 The history of these attempts to amend the Interception Act illustrate the complexity of the legal, policy and practical issues associated with the regulation of surveillance activity, many of which the Commission has been grappling with during the course of this reference. It also highlights the inadequacy of making incremental amendments to outdated legislation in an attempt to deal with modern technology. This is one of the key reasons why the Commission recommended that new surveillance legislation should be introduced to respond to ongoing technological developments and the consequent policy implications, rather than simply expand the LDA.

2.21 The law as it stood prior to the passage of the Stored Communications Act was unclear in its application to the interception and surveillance of electronic communications, particularly when those communications have been stored by the sender or recipient for a period of time. The passage of the Stored Communications Act at least brings a degree of clarity to this area. The potential downgrading in privacy protection that could occur as a result is indeed a matter of concern, and one that makes the need for comprehensive State surveillance legislation to regulate the surveillance of communications not covered by the Stored Communications Act more crucial than ever.

---

48. Australia, Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* (July 2004) at para 3.23-3.41.
49. Australia, Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* (July 2004) at para 3.36 and 3.42-3.46.
50. Australia, Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* (July 2004) at para 3.20 and 3.53-3.54.
51. Australia, Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* (July 2004) at para 3.47-3.48 and 3.54-3.55.
52. Taking effect on 15 December 2004.

2.22 In Report 98, the Commission concluded that, although the Interception Act is uncertain in scope, the safe assumption (and most practical solution) would be that the interception of any communication which is being carried by or travelling along a telecommunications system is the sole legislative responsibility of the Commonwealth, provided that the interception occurs whilst the communication is in transit.[53] Following from this, the Commission then argued that it would be open to the States and Territories to regulate surveillance of these communications at points either before or after they have passed across a telecommunications system.[54] This approach would, for example, support legislation to enable employers to scan emails stored on the hard drives of employees' computers for inappropriate content.[55]

2.23 The legal developments since Report 98 was released have not contradicted this approach. Indeed, the discussion in the Senate Report and Second Reading debates over the proposed Interception amendments only serves to reinforce the Commission's view. Further, the fact that existing and proposed Commonwealth and State surveillance laws deal concurrently with computer and data surveillance devices would seem to indicate that this is an area where the Commonwealth does not purport to "cover the field".[56] Consequently, the Commission sees no reason to deviate from the position taken in relation to the surveillance of electronic communications outlined in Report 98.

OTHER LEGAL DEVELOPMENTS SINCE REPORT 98

2.24 A number of other legal developments have occurred since the Commission delivered Report 98 in 2001, which are consistent with or directly or indirectly affect the recommendations in that Report. While some have been discussed in the paragraphs above, others are outlined in the following paragraphs.

Criminal law

2.25 On 16 March 2004, the *Crimes Legislation Amendment Bill 2004* (NSW) was passed. Schedule 8 to that legislation amends the *Summary Offences Act 1988* (NSW) to include the

53. Report 98 at para 2.47.
54. Report 98 at para 2.48. The Commission acknowledged that this two-tier system of regulation between the Commonwealth and the States was not ideal, but, in the absence of comprehensive Commonwealth regulation of email and other delayed access communications, it was preferable to leaving the unauthorised interception of those communications insufficiently regulated: Report 98 at para 2.49-2.50.
55. See discussion in Senate Committee Report at para 3.12-3.16. The Commission notes that this practice would be permitted under the Recommendations made in Report 98 regarding surveillance in the context of employment, provided that it was conducted overtly and that certain privacy safeguards were complied with. If such email surveillance were to be conducted covertly, a prior authorisation would be necessary. This also accords with the regime set out in the draft *Workplace Surveillance Bill 2004* (NSW).
56. For example, the *Surveillance Devices Act 2004* (Cth) specifically preserves the ability of the States to legislate on surveillance: s 4(1).

offences of filming for indecent purposes (inserting s 21G) and installing a device to facilitate filming for indecent purposes (inserting s 21H). Section 21G provides that any person who films,[57] or attempts to film, another person to provide sexual arousal or sexual gratification, whether for himself or herself or for a third person, where the other person:

(a) is in a state of undress, or is engaged in a private act,[58] in circumstances in which a reasonable person would reasonably expect to be afforded privacy, and

(b) does not consent to being filmed,

is guilty of an offence carrying a maximum penalty of 100 penalty units, 2 years imprisonment, or both.

2.26 Section 21H provides that a person who installs a device, or constructs or adapts the fabric of any building, vehicle, vessel, tent or temporary structure for the purpose of facilitating the installation or operation of any device, with the intention of enabling that or any other person to commit an offence under s 21G is guilty of an offence.[59]

2.27 The law covers filming in private homes and public areas. The Attorney General has expressed the view that the legislation is designed to address the inappropriate use of phone cameras, which he says have developed a breed of "21st-century peeping toms".[60]

Police investigations

2.28 In December 2004, the *Law Enforcement (Powers and Responsibilities) Amendment (In-car Video System) Act 2004* (NSW) ("the In-car Video System Act") was passed.[61] That Act requires police vehicles fitted with an in-car video system (comprising digital video and audio components), to use that equipment to record dealings between police officers and members of the public in circumstances where police:

- are following a vehicle with the intention of stopping it; or
- have stopped a vehicle for the purpose of conducting an investigation.

---

57. For the purposes of the section, a person films another person if he or she causes one or more images (whether still or moving) of another person to be recorded or transmitted for the purpose of enabling himself or herself, or a third person, to observe those images (whether while the other person is being filmed or later): s 21G(2)(a).
58. For the purposes of the section, a person is engaged in a private act if the person is using the toilet, showering or bathing, carrying on a sexual act of a kind not ordinarily done in public or any other like activity: s 21G(2)(b).
59. The maximum penalty of 100 penalty units, 2 years imprisonment, or both: s 21H
60. L Silmalis "Phone camera abusers face jail" *Sunday Telegraph* (Sunday 14 March 2004 at 9).
61. This Act amends the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW). Neither piece of legislation has been proclaimed.

2.29 Police officers are required to inform members of the public that their conversations will be recorded using the in-car video system, either immediately before the recording of the conversation commences, or as soon as practicable after the recording has commenced, and may occur irrespective of whether that person consents to the recording.[62] Since the audio recording of a conversation conducted without the consent of at least one of the participants to that conversation is currently regulated by the LDA, the provisions of the In-car Video System Act create an exemption from the terms of the LDA.[63] In his Second Reading Speech on the Bill, the Minister for Police, the Hon John Watkins, MP, emphasised that the fact that the recording may be done without the consent of the participants does not mean that it will be done in secret, since members of the public must be informed of the recording and are under no compulsion to answer questions.[64]

2.30 While this Act does not directly implement Report 98, it does give effect to significant fundamental elements of that Report. In particular, the In-car Video Act represents the first legislative regulation of overt surveillance in New South Wales. This recognises the Commission's view that even where surveillance is conducted with the knowledge of the participants, it still has a sufficient impact on personal privacy and other interests to warrant some form of legislative regulation. The In-car Video Act also departs from the LDA in rejecting the concept of consent in relation to surveillance. In Report 98, the Commission considered that consent should not be a factor in proving whether or not surveillance was overt. The Commission was of the view that attempts to infer consent to surveillance based on behaviour such as entering premises with CCTV systems operating, or using Automatic Teller Machines, are futile, since people generally have no option to choose a surveillance-free alternative. Similar issues arise in dealings between police and members of the public, where the power imbalance may render consent meaningless. Accordingly, the In-car Video System Act echoes the Commission's view that knowledge, rather than consent, should be the key determinant in overt surveillance.

Workplace surveillance

2.31 In his speech to the NSW ALP State Conference in October 2003, the Premier, the Hon Bob Carr, MP, announced that new legislation would be introduced to govern the installation and use of any surveillance devices that record, monitor or listen to employees.[65] The *Workplace Surveillance Bill 2004* (NSW) ("the Workplace Surveillance Bill") was released for public comment in June 2004. That Bill is consistent with the recommendations made by the Commission in Report 98, and largely follows the existing model set out in the *Workplace Video Surveillance Act 1998* (NSW) ("WVSA") of requiring an authorisation to be obtained prior to covert surveillance being conducted during the course of employment. The Workplace

62. *Law Enforcement (Powers and Responsibilities) Amendment (In-car Video System) Act 2004* (NSW) s 108D(1) and (3).
63. *Law Enforcement (Powers and Responsibilities) Amendment (In-car Video System) Act 2004* (NSW) s 108F.
64. New South Wales, *Parliamentary Debates (Hansard)*, Legislative Assembly, 7 December 2004 at 13420.
65. Premier of NSW, the Hon Bob Carr, MP, *Speech to the NSW ALP State Conference*, Sunday 5 October 2003.

Surveillance Bill extends the coverage of the WVSA to include additional forms of surveillance such as email and internet monitoring and the use of tracking devices. The Commission discusses the terms of the Workplace Surveillance Bill in more detail in Chapter 5.

Anti-spamming legislation

2.32 Spamming refers to the practice of sending bulk unsolicited electronic messages (usually by email but also by other electronic means), generally in an automated and indiscriminate manner. Spam may contain illegal or offensive material, may be sent for the purpose of fraudulent commercial gain, and generally does not enable the recipient to identify the sender or request to be removed from the mailing lists.[66] Electronic addresses of spam recipients may also be harvested in a way that contravenes or circumvents privacy legislation.

2.33 In April 2004, the *Spam Act 2003* (Cth) came into effect, designed to prohibit the sending of unsolicited electronic commercial messages and to establish a scheme of regulation for other general commercial electronic messages, regardless of whether or not they are unsolicited.[67] The Australian Communications Authority is the body nominated under the Act to investigate complaints and breaches and to assist in the development of industry codes and education campaigns.

2.34 In Report 98, the Commission discussed the interplay between data protection and surveillance, noting the practice of electronic data warehousing and information cross-matching. The Commission concluded that, although these practices represented significant privacy threats, the random collection, retrieval and matching of information on computer databases should be regulated by data protection or other more appropriate legislation rather than the surveillance legislation proposed by the Commission.[68] The Commission notes the introduction of the *Spam Act 2003* (Cth) as one such measure.

Mutual recognition of surveillance laws

2.35 There is currently little uniformity between the surveillance laws of the Commonwealth and each State and Territory. Differences exist in areas such as who may apply for a warrant, the types of devices a warrant may cover, the duration of warrants, what a warrant may authorise, and record keeping and accountability requirements. This lack of consistency is not a problem where surveillance is being conducted within one State only, and in relation to State offences or issues. However, law enforcement officers have expressed concern over the difficulties involved in conducting surveillance operations that cross State borders, for example, where a tracking device is installed in a vehicle in NSW, which travels through Victoria and South

66. See *Spam Bill 2003* (Cth) Explanatory Memorandum at 3.
67. See *Spam Bill 2003* (Cth) Explanatory Memorandum at 1.
68. See Report 98 at para 2.69-2.72 and Recommendation 6.

Australia. Currently, warrants must be obtained separately in each jurisdiction, which can result in operational delays, loss of evidence and wasted resources.[69]

2.36 Issues concerning multi-jurisdictional investigations were discussed in a Report by the Standing Committee of Attorneys General and Australasian Police Ministers' Council Joint Working Group released in November 2003 ("the Joint Working Group Report"). That Report recommended a series of model laws, including surveillance legislation, to "facilitate seamless law enforcement across jurisdictions".[70] The model laws are intended to apply only to covert surveillance conducted by law enforcement officers in the course of investigating offences across more than one jurisdiction,[71] and provide for a system of authorisation and accountability measures based on existing Commonwealth and State surveillance laws.

2.37 Under the model surveillance laws, police in one State could apply for a warrant to conduct covert surveillance, which would be valid not only in that jurisdiction, but also recognised in any other State that had adopted the model provisions.[72] The Joint Working Group Report states that this would alleviate the need to apply for a warrant separately in each participating jurisdiction, as well as the need to call on the resources of interstate police.[73] The model Bill sets out minimum standards, which participating States may choose to improve upon in relation to their own law enforcement agencies.[74] While the model laws are focussed only on cross-border investigations, States may choose to apply the provisions to intra-state surveillance operations as well.[75] The model laws have recently been adopted, with some amendment, by Victoria,[76] and the Commonwealth Parliament.[77]

2.38 The provisions of the model laws are discussed in more detail in relation to covert law enforcement recommendations in Chapter 5.

---

69. See Standing Committee of Attorneys General and Australasian Police Ministers' Council Joint Working Group on National Investigative Powers, *Cross-Border Investigative Powers for Law Enforcement* (November 2003) ("Joint Working Group Report") at 345.
70. Joint Working Group Report at i.
71. Existing State laws would continue to operate in relation to intra-State surveillance operations: see Joint Working Group Report at v.
72. Joint Working Group Report at vi.
73. Joint Working Group Report at vi.
74. For example, a State could choose to require its law enforcement officers to observe higher standards of accountability during cross-border surveillance operations. However, a jurisdiction "that adopts higher standards must nevertheless accept that participation in the national scheme means that the law enforcement agencies of other external jurisdictions could be operating in its local jurisdiction to the minimum, nationally agreed standards": Joint Working Group Report at iv.
75. Victoria (the only State so far to have legislated to adopt the model laws) has chosen to implement the model in relation to local as well as cross-border investigations: *Surveillance Devices (Amendment) Act 2004* (Vic).
76. *Surveillance Devices (Amendment) Act 2004* (Vic).
77. *Surveillance Devices Act 2004* (Cth).

Decision in Lenah Game Meats

Facts and background

2.39 In November 2001, the High Court decision in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*,[78] examined the issue of whether or not an injunction was available to prevent the broadcasting of material obtained through covert surveillance.

2.40 In that case, the Lenah Game Meats operated a possum meat processing plant in Tasmania. The ABC obtained video material from a third party, filmed illegally as a result of trespass, of brush tail possums being slaughtered and processed. Lenah Game Meats applied to the Tasmanian Supreme Court for an interlocutory injunction to prevent the ABC from broadcasting the material on the 7.30 Report for fear of negative repercussions on its business.

2.41 Since the ABC was not implicated in the initial trespass, the issue before the court was whether interlocutory relief was available to restrain the ABC from broadcasting the material even though there was no enforceable cause of action against the ABC. This distinguished *Lenah Game Meats* from previous similar cases which held that injunctions could be awarded to restrain the broadcast of covert surveillance material in circumstances where the media organisation was the trespasser.[79] Initially, the Tasmanian Supreme Court refused the injunction, finding that, even if the allegations were true, there was no serious question to be tried.[80] However, on appeal, the Full Court determined that an injunction could be awarded on the basis that it would be unconscionable for the ABC to profit from illegal activity.[81]

2.42 The ABC sought, and was granted, special leave to appeal to the High Court. In considering the grounds on which an interlocutory injunction may be available, the High Court examined issues of unconscionability, breach of confidence, and, most significantly for the current purpose, the contention made by Lenah Game Meats that Australian law recognises a tort of privacy which is available to a corporation to protect its commercial interests.

The decision

2.43 The majority of the High Court was of the view that an interlocutory injunction was not available in the circumstances of the case. In reaching this view, Gleeson CJ, Gummow, Hayne, and Gaudron JJ determined that the application for an injunction failed because Lenah was unable to identify the legal rights sought to be protected or to establish an equitable basis for intervention. On the other hand, Kirby J considered that the court had the discretionary power to grant an injunction without an identifiable legal cause of action or basis for equitable intervention. However, on the facts at hand, Kirby J considered that the material was not relevantly private, and that "[w]hen the constitutional consideration favouring free discussion of governmental and political issues of animal welfare in this context is given due weight, a proper exercise of the discretion obliges that the interlocutory injunction be refused".[82] Callinan J dissented, considering

78. (2001) 208 CLR 199.
79. See, eg, *Lincoln Hunt Australia Pty Ltd v Willesee* (1986) 4 NSWLR 457.
80. *Lenah Game Meats Pty Ltd v ABC,* Supreme Court of Tasmania, Underwood J, 3 May 1999, unreported.
81. *Lenah Game Meats Pty Ltd v ABC* [1999] TASSC 114.
82. (2001) 208 CLR 199 at para 221.

that the injunction could and should be awarded, on the basis that Lenah had a property interest in the film obtained as a result of covert surveillance, held on the basis of a constructive trust.

High Court's views on breach of confidence

2.44 The various judgments also commented on the application, and possible extension, of the common law doctrine of breach of confidence. However, as this ground was not argued by counsel for Lenah, the comments are obiter only. The broadest view was expressed by Kirby J, who considered that a relationship of confidence could exist between the subject of surveillance and the broadcaster or publisher of that information, sufficient to restrain its publication or broadcast, where that information was obtained "illegally, tortiously, surreptitiously or improperly, even where the possessor [of the information] is itself innocent of wrongdoing".[83]

2.45 The majority of the Court, however, was not prepared to accept such a broad argument. Gleeson CJ considered that, in some circumstances, equity may impose an obligation of confidence upon those who obtained surveillance material *of private activities*, and upon those into whose possession that material subsequently fell, if they knew, or ought to have known, the manner in which the material was obtained.[84] Gleeson CJ discussed the difficulty involved in determining what amounted to a "private" activity for the purpose of grounding an action for breach of confidence, proposing that information or conduct should be regarded as private if disclosure would be regarded as "highly offensive to a reasonable person of ordinary sensibilities".[85] If the covert filming had been of activity deemed to be private, Gleeson CJ was of the view that the law of breach of confidence would be adequate to cover the case.[86] In the circumstances of the *Lenah Game Meats* case, Gleeson CJ considered the material to be neither confidential nor private, providing no grounds for injunctive relief.[87]

2.46 Gummow and Hayne JJ (with Gaudron J concurring) also rejected the notion that material obtained as a result of trespass should always be equated with confidential information. Instead, their Honours expressed the view that publication of such information could possibly be restrained by imputing an equitable proprietary interest, on the part of the surveillance subject, in the copyright of the videotape, if the material was obtained in circumstances involving "the invasion of the legal or equitable rights" of the surveillance subject.[88] On this interpretation, the property right in the videotape would be the key factor, with the privacy or confidentiality of the information being irrelevant.[89]

2.47 In his dissent, Callinan J acknowledged that the copyright argument may have some validity, but did not consider it pertinent to the circumstances before the Court. Instead, he considered that publication of material obtained as a result of trespass could be restrained because of a fiduciary relationship of confidence that existed between Lenah, who was entitled to

83. (2001) 208 CLR 199 at para 170 and para 183.
84. (2001) 208 CLR 199 at para 34-36.
85. (2001) 208 CLR 199 at para 42. See discussion below at para 2.49 and 2.56-2.57.
86. (2001) 208 CLR 199 at para 39.
87. Note that Lenah conceded that the material was not private.
88. (2001) 208 CLR 199 at para 102-103.
89. As with breach of confidence, Lenah did not argue a breach of copyright, and therefore these comments are obiter only.

exclusive occupation of its premises, and the ABC, who knew that the video was obtained illegally. Callinan J was of the view that, in these circumstances, the ABC was acting unconscionably, and that it held the videotape on constructive trust for Lenah.

High Court's views on a tort of privacy

2.48 The majority of the High Court held that, in the circumstances of the case, involving the commercial interests of a corporation whose legal rights had not been directly impugned by the appellant, there was no invasion of privacy. However, the broad question of whether a general tort of invasion of privacy exists in Australian law, and if so, what the elements of such a tort be, was left open.[90] In fact, in expressing the view that a tort of privacy would not be available to protect the commercial interests of a corporation, Gummow and Hayne JJ took pains to note that nothing "said in these reasons should be understood as foreclosing any such debate or as indicating any particular outcome".[91] In considering that an interlocutory injunction should have been granted on the basis of the illegality involved in obtaining the tape, Kirby J deemed it unnecessary to examine the existence of a privacy tort.[92]

2.49 Gleeson CJ noted the "lack of precision in the concept of privacy", and the "tension that exists between interests in privacy and interests in free speech" as reasons for "caution in declaring a new kind of tort", suggesting that this weighted the argument in favour of the extension of the doctrine of breach of confidence.[93] It is interesting to note that Gleeson CJ considered that the commercial interests of a corporation could be covered by an extension of that doctrine, but not in the present case given that the surveillance material was not sufficiently private.

2.50 On the other hand, Callinan J appeared to view the recognition of a privacy tort favourably:

> *It seems to me that, having regard to the current conditions in this country, and the developments of the law in other common law jurisdictions, the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country, or whether the legislatures should be left to determine whether provisions for a remedy for it should be made.*[94]

2.51 Callinan J was mindful of the increasingly fragile nature of individual privacy, particularly in a climate where there are powerful media organisations owned by a concentrated few. He considered that a tort of privacy would be capable of extending to protect corporations or

90. See view expressed in D Lindsay, "Protection of privacy under the general law following ABC v Lenah Game Meats Pty Ltd: Where to now?" (2002) 9(6) *Privacy Law and Policy Reporter* 101 at 104.
91. (2001) 208 CLR 199 at para 132.
92. (2001) 208 CLR 199 at para 189 and 191.
93. (2001) 208 CLR 199 at para 41.
94. (2001) 208 CLR 199 at para 335.

governments.[95] He was also of the view that, if such a tort existed, it would have been committed in *Lenah Game Meats* by the unlawful intrusion into the processing plant and the covert filming.

Implications of Lenah Game Meats for privacy and surveillance laws

2.52 Many commentators have noted the significance of *Lenah Game Meats*. Just as the High Court Judges held wide-ranging views in the case, commentators have drawn different conclusions as to its impact on the development of privacy rights in Australia.[96] Some submissions received by the Commission from media organisations in response to Interim Report 98 have argued that the case represents the rejection by the High Court of the opportunity to develop a common law right to privacy.[97] Those submissions view the judgment in *Lenah Game Meats* as being at odds with the Commission's recommendations, which they view as effectively amounting to a statutory tort of invasion of privacy. [98]

---

95. (2001) 208 CLR 199 at para 328.
96. See eg G Taylor and D Wright, "Australian Broadcasting Corporation v Lenah Game Meats, Privacy, Injunctions and Possums: An Analysis of the High Court's Decision" (2002) 26 *Melbourne University Law Review* 707; D Lindsay, "Protection of privacy under the general law following ABC v Lenah Game Meats Pty Ltd: Where to now?" (2002) 9(6) *Privacy Law and Policy Reporter* 101; M Richardson, "Whither Breach of Confidence: A Right of Privacy for Australia?" (2002) 26 *Melbourne University Law Review* 381; D Stewart, "Protecting Privacy, Property, and Possums: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd" (2002) 30(1) *Federal Law Review* 177; B Harris, "Privacy and 'possum' let the debate begin" (2002) 10 *elawpractice.com.au* at 13; F Trindade, "Possums, privacy and the implied freedom of communication" (2002) 10 *Torts Law Journal* 119; H Heuzenroeder, "Brushtail Carnage: Privacy Interests and the Common Law" (2002) 24(1) *Law Society Bulletin* (SA) 22; G Greenleaf, "Privacy at common law – not quite a dead possum" (2001) 8(7) *Privacy Law and Policy Reporter* 129; T Wilson, "Does the decision in ABC v Lenah Game Meats Pty Ltd open the door to privacy rights?" (2002) 16(5) *Australian Property Law Bulletin* 45; J Horton, "Common law right to privacy moves closer in Australia" (2001) 8(7) *Privacy Law and Policy Reporter* 144; J Horton, "Towards a Real Right of Privacy" (2003) 29(2) *Monash University Law Review* 401; R Martin and J Macdonnell, "Privacy after Lenah Game Meats" (2001) 5(7) *Telemedia* 106; D Lindsay, "Playing possum? Privacy, freedom of speech and the media following ABC v Lenah Game Meats Pty Ltd: Part 11- The future of Australian privacy and free speech law, and implications for the media" (2002) (September) *Media and Arts Law Review* 161; WM Heath, "Possum Processing, Picture Pilfering, Publication and Privacy: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2002) 28(1) *Monash University Law Review* 162; S Gibson, "Emerging law of privacy in Australia" (2003) 16(5) *Australian Intellectual Property Law Bulletin* 65; C Doyle and M Bagaric, ""The right to privacy and corporations" (2003) 31 *Australian Business Law Review* 237; GHL Fridman, "A Scandal in Tasmania: The Tort That Never Was" (2003) 22(1) *University of Tasmania Law Review* 84.
97. However, the Australian Press Council News cites *Lenah Game Meats* as one of a number of cases in which the courts are giving "limited recognition" to the "embryonic common law tort of breach of privacy": see *Australian Press Council News* vol 16(2) May 2004 at 7.
98. Australian Broadcasting Corporation *Submission* at 4; Australian Press Council *Supplementary Submission* at 3; Special Broadcasting Service Corporation *Submission* at

2.53 Others see the decision as more narrowly constrained and less definitive in terms of general privacy jurisprudence:

> *The facts before the High Court in Lenah were not conducive to the development of principles relating to the protection of privacy under Australian general law. On any view of the facts, Lenah was concerned to protect commercial interests in business goodwill or reputation, and not privacy interests.*[99]

> *On a formal level, the decision in Lenah leaves the concept of a tort of privacy in Australian law in much the same position as it was before the case was decided: it remains a matter of great uncertainty, and arguments in favour of the existence of such a tort will only be resorted to by those who have no case under more familiar headings.*[100]

2.54 Some see the decision not to award an injunction to prevent publication of the material not to be indicative of the absence of any public interest in privacy, but as understandable given the failure of Lenah to establish an enforceable cause of action capable of supporting an injunction against the ABC. Others are of the view that the decision is "unsatisfactory" and "wrong".[101] However, *Lenah Game Meats* is generally acknowledged by these commentators to be an "important turning point" in Australian privacy law, albeit one presenting an "extraordinary collection of views" ultimately resulting in a "legal limbo" in an important area of law.[102]

> *The main significance of the decision for the future of privacy law lies in the extent to which each of the judgments appeared to recognise, at least implicitly, that protection of privacy under Australian general law is, at present, inadequate.*[103]

2; Commercial Television Australia Limited *Submission* at 6 and 12; John Fairfax Holdings *Submission* at 5.

99. D Lindsay, "Protection of privacy under the general law following ABC v Lenah Game Meats Pty Ltd: Where to now?" (2002) 9(6) *Privacy Law and Policy Reporter* 101 at 105.
100. G Taylor and D Wright, "Australian Broadcasting Corporation v Lenah Game Meats, Privacy, Injunctions and Possums: An Analysis of the High Court's Decision" (2002) 26 *Melbourne University Law Review* 707 at 709.
101. G Taylor and D Wright, "Australian Broadcasting Corporation v Lenah Game Meats, Privacy, Injunctions and Possums: An Analysis of the High Court's Decision" (2002) 26 *Melbourne University Law Review* 707 at 735.
102. D Lindsay, "Protection of privacy under the general law following ABC v Lenah Game Meats Pty Ltd: Where to now?" (2002) 9(6) *Privacy Law and Policy Reporter* 101 at 105-106. See also D Stewart, "Protecting Privacy, Property, and Possums: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd" (2002) 30(1) *Federal Law Review* 177 at 201; T Wilson, "Does the decision in ABC v Lenah Game Meats Pty Ltd open the door to privacy rights?" (2002) 16(5) *Australian Property Law Bulletin* 45 at 47; J Horton, "Common law right to privacy moves closer in Australia" (2001) 8(7) *Privacy Law and Policy Reporter* 144 at 144.
103. D Lindsay, "Protection of privacy under the general law following *ABC v Lenah Game Meats Pty Ltd*: Where to now?" (2002) 9(6) *Privacy Law and Policy Reporter* 101 at 105.

2.55 Much of the judgment is concerned with the question of whether it is better to address this inadequacy by means of extending the common law action for breach of confidence or to develop and recognise a tort of privacy.[104] Some have welcomed the fact that the High Court appears willing at least to consider reform, with all of the justices in *Lenah Game Meats* who canvassed the concept of a privacy tort (with the exception of Gleeson C), expressing some degree of support.[105]

2.56 As noted above, Gleeson CJ pointed out the difficulties inherent in defining concepts of privacy, suggesting that this weighted the argument against the development of a specialised tort. Gleeson CJ also noted the difficulty associated with balancing privacy and freedom of expression.[106] However, others have argued that, while defining privacy and balancing it against other public interests is undoubtedly difficult, this is a difficulty confronted by any liberal democracy, and that the way to overcome it is to develop a flexible framework in which those interests may be weighted against each other in particular circumstances.[107]

2.57 There has been much discussion and debate following *Lenah Game Meats* on the nature of privacy and what activities would, or should, be considered to be private. Gleeson CJ, in a much quoted statement, asserted that there is "no bright line that can be drawn between what is private and what is not".[108] He also states that an act does not "become private simply because the owner [of private property] would prefer that it were unobserved". Others challenge this assertion, noting "if that is not private, what is? What more does the owner of private property have to do?"[109]

2.58 So far as the particular impact of surveillance material on the nature of private or confidential activity, it has been observed that a "video is much more media-effective than any possible description of the abattoir in a government document or even an eyewitness description".[110] It is argued that the videos were, therefore, not existing information, but "entirely

104. Although these issues were immaterial to the case at hand since Lenah conceded that the material on the tape was not "confidential".
105. See, eg, H Heuzenroeder, "Brushtail Carnage: Privacy Interests and the Common Law" (2002) 24(1) *Law Society Bulletin* (SA) 22 at 24. See also J Horton, "Common law right to privacy moves closer in Australia" (2001) 8(7) *Privacy Law and Policy Reporter* 144 at 145.
106. See para 2.29 and 2.56.
107. D Lindsay, "Protection of privacy under the general law following ABC v Lenah Game Meats Pty Ltd: Where to now?" (2002) 9(6) *Privacy Law and Policy Reporter* 101 at 107.
108. (2001) 208 CLR 199 at para 42.
109. G Taylor and D Wright, "*Australian Broadcasting Corporation v Lenah Game Meats*, Privacy, Injunctions and Possums: An Analysis of the High Court's Decision" (2002) 26 *Melbourne University Law Review* 707 at 717.
110. G Taylor and D Wright, "Australian Broadcasting Corporation v Lenah Game Meats, Privacy, Injunctions and Possums: An Analysis of the High Court's Decision" (2002) 26 *Melbourne University Law Review* 707 at 717.

new information in pictorial form to which *no-one* had previously had access and which accordingly should have been recognised as having the necessary quality of confidence".[111]

Analysis

2.59 *Lenah Game Meats* is relevant to the Commission's work on this reference insofar as it involves issues of media, surveillance and privacy. However, contrary to the claims of media organisations, nothing in *Lenah Game Meats* precludes a legislative statement on privacy or surveillance in the manner proposed by the Commission. Nor is *Lenah Game Meats* authority for the proposition that a common law tort of privacy should not be developed. The High Court either felt that there was no need to decide the question in light of the facts at hand, or were unsure of which approach to take. What the case does reveal is the current uncertainty of the common law in its application to emerging technology and the challenges that this represents.

2.60 The case also muddies several distinct concepts, such as privacy, confidentiality and proprietary interests, and is further complicated by the fact that the subject of the surveillance was a corporation, and that the surveillance material was not considered, or even argued to be, private or confidential. In the Commission's view, the case highlights the complexity of the issues surrounding privacy, confidentiality and surveillance, and the inadequacy of the common law to provide clear and effective guidance on when surveillance can occur and privacy interests may be displaced. As stated in Report 98, there are undoubtedly circumstances in which the public interest in conducting surveillance outweighs an individual's interest in protecting his or her personal privacy. However, where intrusions into privacy interests by means of surveillance are unwarranted and unjustified, the protection of privacy should be respected in its own right, and not be viewed in the context of other proprietary interests, or whether or not a relationship of confidentiality exists. In effect, the Commission considers that the decision in *Lenah Game Meats* can be viewed as highlighting the need for considered surveillance legislation setting out the interests designed to be upheld or protected.

111. G Taylor and D Wright, "Australian Broadcasting Corporation v Lenah Game Meats, Privacy, Injunctions and Possums: An Analysis of the High Court's Decision" (2002) 26 *Melbourne University Law Review* 707 at 717.

3. General issues

- Introduction
- Surveillance
- Privacy and other interests
- Privacy invasion
- The current self-regulatory regime

INTRODUCTION

3.1 In this chapter we address particular issues discussed in the Interim Report. However, their treatment here is angled towards objections raised in submissions to some of the Commission's recommendations. In large measure these objections emanated from media organisations, both public and private. While the media did figure in the Interim Report, they were not seen as central to an inquiry into surveillance devices. Many of the comments in this chapter, however, relate specifically to media concerns.

3.2 One topic we do not propose to revisit - except to respond briefly to comments regarding the media's self-regulatory regime[1] - is current surveillance regulation and remedies for breach, as the Commission's views have been canvassed at some length in the Interim Report.[2] Similarly, the Commission's reasons for recommending a broad-based regulatory system that, among other things, eschews a device-specific approach, have been set out previously,[3] and it serves little purpose to repeat them here. In response, however, to the comment[4] that it is inappropriate to undertake legislating now "for *possible* future technological developments, including convergence" or for the *potential* "for certain outcomes (for example, convergence of technologies resulting in intrusive information gathering activity)" (emphasis added), the Commission would make the preliminary observation that convergence is not of the future, but the present. This is why the Commission also has concerns about the proposition that "it is … entirely appropriate to have a different way of regulating different kinds of privacy,"[5] that is "information privacy, …privacy of personal space and privacy of communications". This treats privacy as a divisible concept. However, the convergence of technologies, breaking down barriers between what were largely separate areas, renders increasingly irrelevant the demarcation that may have existed between the technology of surveillance (eg, monitoring the activities of the living, breathing person) and that of information (eg, the data held about a person in a databank). Flexibility is required to avoid enacting legislation with built-in obsolescence. When the Commission makes reference to "potential" and "future developments", it intends not only technologies and inventions yet undreamt of, but also the use of *existing* technologies in new, privacy-intrusive ways.

3.3 For example, in the short time that mobile phone cameras have been available, their use has already caused consternation. Photographs of an inmate on weekend detention at a Sydney prison appeared on the front page of a Sunday newspaper in mid-2003. They were taken by another inmate, who had smuggled a mobile phone camera into the prison and was subsequently charged with introducing contraband to a correctional facility.[6] Around the same time, the YMCA and the Royal Life Saving Society of Australia took the decision to ban the new phones from public changing rooms, such as those at swimming pools, health clubs and

1. See below para 3.31-3.35.
2. Report 98 at para 1.36-1.56.
3. Report 98 at para 2.8-2.32.
4. SBS, *Submission* at 8.
5. SBS, *Submission* at 7.
6. L Kennedy, "Inmate on Phone Camera Charge" *Sydney Morning Herald* (19 June 2003) at 3.

recreational sports stadiums.[7] In December 2004 a man was convicted on a charge of offensive behaviour in a public place, after he had used his mobile phone camera to take photographs of women sunbathing topless on a Sydney beach.[8] The President of the Australian Computer Society, representing more than 16,000 information technology professionals, stated:[9]

> *Mobile phones are rapidly moving towards integrated video and sound capabilities and enhanced computing functionality, which means you're not just talking about a camera, but an advanced surveillance device.*

SURVEILLANCE

3.4 Whether an activity constitutes surveillance for the purposes of the proposed Act is a threshold issue. If an activity does not fit within the suggested definition[10] then the proposed Act will not apply. For an activity to constitute surveillance it must comprise the following elements: (1) the use of a surveillance device (2) where there is a deliberate intention to monitor a person, place, etc (3) for the purpose of obtaining information about the surveillance subject. For example, with regard to overt surveillance specifically, the Interim Report stated:[11]

> *The Commission's concern is with those surveillance devices that are used for surveillance. This may seem a tautology. However, recreational photography or the taping by a student of a lecture are examples of surveillance devices in use* for non-surveillance activities*, according to the definition of surveillance at paragraphs 2.37-2.39. This is because their purpose is not to obtain information about the subjects of the surveillance … but merely to record an occasion for later enjoyment or as an aid to memory. … Surveillance devices also bring many of the sounds and images to news reports on television, radio and in the press. While some of the activity involved in obtaining this material could be characterised as surveillance,* much of it is merely a straightforward recording of events to illustrate a story, without any intention of monitoring for the purpose of obtaining further information. In the latter respect it is similar to recreational photography and lecture-taping. *(emphasis added)*

This point was re-stated later:[12]

7. D Hoare, "Don't Look Now, Privacy Laws are Changing" *Australian* (12 June 2003) at 3; see also D Gregory, "Ban on Phone Cameras in Change Rooms" *Sun-Herald* (17 October 2004) at 38, regarding similar bans imposed by a council in south-western NSW.
8. L Lamont, "Unhappy Adventures End as Beach Pest Loses Camera" *Sydney Morning Herald* (2 December 2004) at 5.
9. E Mandla, "Naked Truth of Phonecams" *Australian* (9 June 2004) at 35; J Lee, "Call for Tighter Controls to Stop Camera Phone Perverts" *Sydney Morning Herald* (21 June 2004) at 3.
10. Report 98 at Rec 2.
11. Report 98 at para 3.4.
12. Report 98 at para 4.20.

> *[R]ecreational photography, the taping of lectures, and so on, would not be regarded as overt surveillance for the purposes of the proposed Act as these would not meet the legislative definition of surveillance.*

3.5 In other words, for the proposed legislation to apply, something more is required than "capturing the scene". The Commission made this distinction in the specific context of media usage at para 3.19 of the Interim Report, where everyday news gathering activity is *contrasted* with surveillance:

> *Surveillance devices capture much of the matter comprising our mass entertainment and current affairs information, delivered through aural, visual and print media. Most of this material is gathered overtly and unexceptionably for the purpose of recording an event, and transmitting it to a wide audience. Sometimes, however, the activity is more akin to surveillance, because the purpose of the monitoring has been to uncover information, most commonly for public interest, or prurience, or, possibly, both. (emphasis added)*

3.6 As stated above and in our earlier Report,[13] recreational photography is not included within the ambit of the suggested legislation. It is not proposed, for example, to prevent beachgoers filming "electronic keepsakes"[14] of family, friends or the general scene. The activity cited at para 3.3 above, of the person convicted after filming topless bathers, while offensive, would not be deemed "surveillance" according to the definition we have proposed. While our suggested definition of "monitoring" includes the recording of images, and while there was "a deliberate intention to monitor a person", it cannot be said that this was "with the purpose of obtaining information" about the person, as the same information was freely and lawfully available to the accused without the need for a surveillance device. The situation might be different, however, where a telescopic lens had been used to effect the same purpose. The latter case would also call into question whether the filming was genuinely "recreational" or carried out for some other purpose.

3.7 For reasons of public policy, the Commission does not wish to introduce a situation where members of the public feel constrained in taking photographs in public, or cannot carry cameras and the like without raising suspicions that they are about to commit an unlawful act. To use the proposed Surveillance Act as a way of catching voyeurs filming in public places is too heavy-handed and fraught with the difficulty of needing to distinguish innocent activities. At the same time, incidents such as those mentioned in para 3.3 are likely to heighten public unease at the sinister potential of seemingly innocuous devices. The offensive behaviour charge brought successfully against one perpetrator is one possible direction for authorities to pursue. In certain contexts a more grassroots approach may be effective. Surf Life Saving Sydney, concerned that photographs of junior members (or Nippers) were turning up on internet child pornography websites, introduced a media accreditation requirement for all "strangers" photographing club activities. Additionally, they called for vigilance amongst parents and others associated with clubs, in keeping watch for individuals filming who were not known to them or lacked

13. Report 98 at para 2.66-2.67.
14. Report 98 at para 2.53.

accreditation, and reporting them to club officials and police.[15] Bans imposed by other organisations on taking cameras into privacy sensitive areas such as changing rooms is similarly proactive.

3.8 To reiterate, only those surveillance devices *being used to conduct surveillance* fall within the ambit of the proposed legislation. There must also be a deliberate intention to monitor a subject for the purpose of obtaining information about that subject.

3.9 In the light of the foregoing, it is difficult to understand criticisms levelled by some media organisations that have claimed the proposed Act would be unduly onerous. This assertion has been made in relation to the regulatory regimes proposed for both overt and covert surveillance. For example, the Special Broadcasting Service Corporation ("SBS") states "the proposed Act will regulate *all* filming and recording, even in public places" (emphasis added).[16] The submission from John Fairfax Publications ("Fairfax"), the nation's largest newspaper publishing group, expresses the view that the Commission's recommendations, if implemented, would "place powerful curbs on the media's daily activities and the public's right to be informed and entertained."[17] An article[18] by a Nine Television Network employee, appearing in Fairfax's *Sydney Morning Herald*, claimed that:

> *The proposed Surveillance Act will regulate the use of* all *cameras – even in public places. … The legislation will impose restrictions on everyday news gathering in public places…(emphasis added)*

These assertions are baseless. The proposed legislation is not intended to apply to most everyday news gathering activity, as the latter does not accord with the suggested definition of surveillance.

3.10 The Roads and Traffic Authority ("RTA") sought clarification as to whether the activities of the Transport Management Centre ("TMC") would fall within the definition of surveillance.[19] The RTA operates the TMC, as its name suggests, for the management of traffic. In its submission, the RTA stated that there is no deliberate intention in the use of cameras to monitor a person etc.[20]

> *There is, however, a deliberate intention to monitor objects, ie motor vehicles and places such as roads and intersections but not for the purpose* of obtaining information about a person who is the subject of the surveillance. *Clearly, the cameras observe some people incidentally.*

15. Surf Life Saving Sydney, News Centre "Renew Your Media Accreditation for 2004-05" (as at 14 December 2004) «www.surflifesavingsydney.com.au/main/newsitem.asp?NewsID=206».
16. SBS, *Submission* at 1.
17. Fairfax, *Submission* at 8.
18. S Rice, "They'll Soon Be Safe From Candid Cameras" *Sydney Morning Herald* (13 June 2002) at 13.
19. RTA, *Submission* at 2.
20. RTA, *Submission* at 1-2.

As the RTA submission suggests, the activities of the TMC are *not* intended to fall within the scope of the proposed Act because there is no deliberate intention to obtain information about persons who are surveillance subjects. During O J Simpson's slow-speed car chase along a Los Angeles Highway in 1994 a great deal of filming took place from helicopters, mostly by the media in the course of news gathering. As discussed above, this would not be regarded as surveillance within the terms of the proposed legislation. However, even in circumstances where the watching or filming of such an event *were* to constitute overt surveillance, it is highly unlikely that the subject of the surveillance could claim to have had a reasonable expectation of privacy.[21]

The public/private distinction

3.11 Current regulation of surveillance devices, both here and in other jurisdictions, operates according to whether the activity being monitored is considered private or not conducted in a public place.[22] However, neither geographical location nor the status of the property's ownership is a reliable determinant of this. In the Interim Report[23] we explained in greater detail our rejection of the public/private distinction, with its lack of clarity or meaningfulness, as a basis for our proposed legislative framework. Since the publication of that paper, the High Court has handed down judgment in *ABC v Lenah Game Meats*, in which Chief Justice Gleeson observed:[24]

> *There is no bright line which can be drawn between what is private and what is not. Use of the term "public" is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private.*

Overt and covert surveillance

3.12 The Interim Report laid out a framework for regulating all surveillance devices according to one of two regimes, depending on the type of surveillance being conducted, whether overt or covert. The demarcation between the two regimes is based on whether the persons being subjected to surveillance have been notified of this fact by the surveillance user. Presence or absence of knowledge as the distinguishing criterion was criticised by Free TV Australia[25] ("Free TV") as "an arbitrary and inappropriate distinction", and the Australian Broadcasting Corporation ("ABC")[26] commented:

> *It is difficult to understand what privacy end is sought to be achieved by this distinction, particularly in respect of surveillance of activities in a public place.*

---

21. Report 98 at para 4.41-4.43.
22. Report 98 at para 2.21.
23. Report 98 at para 2.20-2.27.
24. (2001) 208 CLR 199 at 226.
25. Free TV Australia, *Submission* at 13. Free TV Australia was formerly known as Commercial Television Australia. The peak industry body representing the free-to-air commercial broadcasters announced its name change on 10 June 2004: «www.203.147.163.200/documents/Industry_Briefing_Media_Release_100604.pdf».
26. ABC, *Submission* at 6.

> *Knowledge per se does not confer the right to prevent surveillance nor to complain about it to the person or organisation conducting the surveillance.*

3.13 Knowledge confers information that is used by the subject to choose his or her response within a surveillance environment. If notices announced that the interior of a changing room or lift were being watched, would this not affect the conduct of at least some of the people entering? Indeed, the potential to change conduct is precisely what the deterrence goal of overt surveillance relies on.

3.14 As Chief Justice Gleeson states, the public/private dichotomy is a "convenient method of contrast". However, it also serves as recognition of the fact that when it comes to preserving their privacy and selfhood, most people will modify their behaviour if they know they can be seen or heard by strangers. By using the terms "overt" and "covert", we have rejected the public/private distinction, but retained what lies at its core, namely the recognition that the subject's knowledge of whether he or she is under surveillance is very much linked to the issue of whether the individual's personal privacy has been breached. The presence or absence of such knowledge should, therefore, help determine the degree of regulation and the weight of sanction applying.

3.15 Under the proposed legislation, overt surveillance activity is permissible - by anyone - so long as complying with principles designed to safeguard a reasonable level of privacy. Covert surveillance attracts a more stringent scheme of regulation under the recommendations contained in the Interim Report, but can be carried out in limited cases subject to strict conditions. This fundamental point appears to have been overlooked or misunderstood by those complaining that certain acts would be deemed "surveillance" for the purposes of the proposed Act, as if this in itself proscribed or restricted the activity. For example, the Australian Press Council ("APC")[27] states:

> *Among the activities that [would be defined as 'surveillance'] would be any use of binoculars at sporting events or opera glasses in the theatre; the use of long-lens cameras to capture images of sporting events; the use of wide-angled shots of localities which might inadvertently include individuals or identifiable groups; the use of cameras (whether with long lenses or not) in public places; shooting wedding or Bar Mitzvah videos; any and all webcams; and a vast range of other activities, many of which would not be seen as remotely threatening to the privacy of individuals. In fact, on a 'black letter' reading of the definitions, the use of contact lenses, hearing aids and, even, cochlear implants could be seen as covert surveillance, even in public places.*

None of the examples cited in this list would necessarily constitute surveillance, as they are recreational or do not in some other respect satisfy the proposed definition.[28] In addition, the Commission suggested a schedule to the proposed Act to list any devices that might technically fit the definition of a surveillance device but which ought not to be subject to regulation, such as

27. APC, *Submission* at 2.
28. See para 3.4.

medical imaging equipment.[29] However, even if it could be established that the activity did amount to surveillance, that does not of itself render the activity a breach of the proposed Act.

3.16 Fairfax[30] lists a number of examples it claims could have been published lawfully in the past, but which could not be published under the proposed regime, such as:

(a) Royal Commission covert footage showing police taking bribes;

(b) footage from street or security cameras, circulated by police to help locate persons of interest, be they suspects, witnesses or missing persons eg, a person filmed in a service station and wanted for questioning in the Peter Falconio case, the last known sighting of Mrs Kerrie Whelan;

(c) amateur videos of the type showing the bashing of Rodney King; and

(d) footage showing drug dealing or illegal immigrants being escorted to work in brothels.

3.17 Publication of this type should continue to be permitted, and the Commission's proposals would not prevent this from happening. With regard to footage obtained overtly, the Commission expressed concern that access to surveillance material be restricted so that it is not used inappropriately.[31] The example given in the Interim Report was that "videotape recordings or images obtained from surveillance should not be sold, given to unauthorised persons, used for entertainment purposes, or displayed as 'wanted' posters." This would not include publication by the media of footage authorised and supplied by police or other officials, where the purpose of the publication is to elicit public assistance in a criminal investigation. In discussing the principle that material obtained through overt surveillance be used only for the purpose obtained, the Commission stated:[32]

> *Where material obtained for one purpose is sought to be used for another, acceptable, purpose, the proposed legislation should allow for an order to be made to this effect. This might take the form of a law enforcement exception to the principle. For example, police may wish to circulate the photograph fairly obtained by the media of an individual being sought by them.*

Fairfax's examples are, in the main, the reverse of this scenario, and could be similarly provided for.[33]

3.18 The comment was also made in some media submissions[34] that the demarcation between overt and covert surveillance is unclear, especially given the media's exemption from

29. Report 98 at para 4.16, and see also para 3.5-3.6.
30. Fairfax, *Submission* at 4-5.
31. Report 98 at para 4.59.
32. Report 98 at para 4.61.
33. See para 4.34.
34. SBS, *Submission* at 9; ABC, *Submission* at 7.

the notice requirement.[35] The absence of notice, in the case of non-media surveillance users, would normally deem an activity covert in the Commission's proposed scheme.

3.19 Unless the media are engaged in a lot of hidden camera activity, in the overwhelming majority of cases it should not be difficult to distinguish the two. In the Interim Report we stated that, where the media were concerned, "so long as recording is carried out openly, and no attempt is made to actually conceal surveillance devices" the notice requirement could be dispensed with, and any actual surveillance regarded as overt.[36]

3.20 The threshold issue, however, as already discussed, is whether the activity constitutes surveillance at all. To try to illustrate the distinction we look at three related scenarios:

(a) A couple are sitting on a bench in the Botanical Gardens, and are engaged in an apparently emotional conversation. Other people are about, close enough to see and be seen by the couple. A bystander takes a photograph of the couple. On these facts this would not constitute surveillance. The activity was not one that could be characterised as monitoring people for the purpose of obtaining information about them. Any information gleaned about these people was not obtained through another's monitoring but by their own willingness to reveal it, or, to quote in part from SBS's submission, "the camera reproduces what could have been seen by anyone" in those circumstances.[37]

(b) A couple are having an emotional conversation in their backyard. In the circumstances it is reasonable to assume that they do not expect anyone else to be watching or listening. They are not aware that a newspaper photographer is shooting them from the other side of their fence. Because of the proposed media exemption from a requirement to give notice, the actions of the photographer would most likely be construed as overt surveillance. Note that if the surveillance user were a non-media photographer, this scenario would be regarded as an example of covert surveillance.

(c) A journalist is admitted to the home of a couple for the purpose of conducting an interview. With a camera concealed in a briefcase, the journalist takes photographs of the family and home. This is covert surveillance.

Note that in (a), were a device to be employed capable of enhancing the ability, for example, to listen to the couple's conversation, this *would* constitute monitoring and, therefore, surveillance. Moreover, this form of surveillance would be covert due to the device's concealment.

3.21 SBS queried[38] the status of "filming a significant public event from inside a media van", in which case the equipment might not be visible. The Commission had suggested previously[39] that, even though it was proposing that media organisations be exempt from giving notice, its

35. Report 98 at para 4.26.
36. Report 98 at para 4.26.
37. P Chadwick and J Mullaly, *Privacy and the Media* (Communications Law Centre, Sydney, 1997) at 28, quoted in SBS, *Submission* at 11.
38. SBS, *Submission* at 9.
39. Report 98 at para 4.49.

personnel should nevertheless be readily identifiable through station logos. Presumably, station vans carry such identification. Filming from an unmarked van would most likely constitute covert surveillance.

PRIVACY AND OTHER INTERESTS

3.22 It is important to re-state that this inquiry is about the use and regulation of surveillance devices, by which we mean, primarily, street cameras, bugging devices, hidden cameras, tracking devices and the like. This inquiry is not concerned with each and every activity that might be thought of as surveillance. Activities such as prying and eavesdropping, if using only the unaided senses, are outside the terms of reference.

3.23 Nor is this an inquiry into privacy rights. The Commission is required by its terms of reference to have regard to "the protection of the privacy of the individual" but within the context of reviewing the *Listening Devices Act 1984* (NSW) ("LDA") and related matters. The rationale underpinning any regulation of surveillance devices is the safeguarding of personal privacy.

3.24 Australian law does not confer a general right to privacy. However, privacy interests are recognised within specific statutory contexts.[40] In a similar way, within the specific context of the statutory regulation of surveillance devices, the Commission stated[41] as its approach:

> *that personal privacy is paramount, but that intrusions into it by way of surveillance are sometimes necessary for the greater public benefit. Those intrusions, particularly when conducted without the knowledge of the subject, should occur only when reasonably able to be justified, and when supported by clear rules.*

3.25 Some submissions received by the Commission in response to the Interim Report have characterised the Commission's approach as asserting *as a general proposition* the paramountcy of privacy over other public interests, in particular the right to free speech. All of these submissions have come from media organisations. For example, the Special Broadcasting Service ("SBS") commented:[42]

> *The Commission's starting point then appears to be that privacy is a fundamental right that overrides other public interest objectives.*

The Australian Broadcasting Corporation stated:[43]

> *Underlying the Commission's recommendations is the view that "privacy should be the paramount concern". This approach, however, is contrary to international law, Australian common law and the* Privacy Act 1988 *(Cth) all of which recognise that*

40. Eg *Health Records and Information Privacy Act 2002* (NSW); *Privacy and Personal Information Protection Act 1998* (NSW).
41. Report 98 at para 2.7.
42. SBS, *Submission* at 2.
43. ABC, *Submission* at 1, 4.

> *individual privacy is only one important right to be balanced against competing rights, in particular the right to free speech and the free flow of information.*

All submissions received from media organisations mentioned the importance of freedom of expression, as did the Interim Report.[44] However, the latter, while referring frequently to the media,[45] did not deal at length with these issues, as they are not central to the inquiry. The Commission does not share the view contained in these submissions as to the impact the proposed *Surveillance Act* would have on media organisations.

3.26 We have not stated or implied that, in general, the human right to privacy (as embodied for example in Article 12 of the Universal Declaration of Human Rights)[46] is more or less important than other human rights, such as freedom of expression (Article 19). Human rights are not absolutes; they must be balanced against each other. However, the weight accorded a particular principle will depend on the context. In the context of the unregulated use of surveillance devices, the important human right at threat is privacy. The greatly increased capability, array and usage of surveillance devices led the Commission to conclude that their control is necessary in order to maintain individual privacy. At the same time, there is clearly a need to allow surveillance to take place where this is in the public interest, so long as surveillance users are accountable for their activities. The Interim Report stated that not all surveillance devices pose a threat to personal privacy, and accordingly suggested exemptions or balancing mechanisms for various scenarios. As well, privacy protection will grate against some other public interests, such as freedom of expression. The Interim Report did not ignore the other interests, but recommended mechanisms for adjudicating between them as they arise in different circumstances.

Media as business

3.27 While many journalists are motivated by a genuine desire to pursue truth in the public interest, there is also no denying that their employers are public or private corporations, driven of necessity by commercial and ratings imperatives. They seek, therefore, to give the public what interests it. The public's interest in a subject is not, however, the measure of whether the subject is "in the public interest". In their submissions, the media organisations have stressed the public interest aspect of their activities. They do not mention their self-interest in boosting sales and ratings. They have sought to portray the issue as a simple tug-of-war between two competing human rights. This would be misleading even if this were an inquiry into the regulation of the media. It is not. It is an inquiry into the regulation of surveillance devices. The Senate Select Committee on Information Technologies, which *did* conduct an inquiry into media regulation,[47] commented:

---

44. Report 98 at para 1.34, 2.58, 6.16.
45. Report 98 at para 3.4, 3.19, 3.88, 4.15, 4.26, 4.46. 4.61, 6.12-6.20.
46. See «www.un.org/Overview/rights.html».
47. Australia, Senate Select Committee on Information Technologies, *In the Public Interest: Monitoring Australia's Media* (Senate Printing Unit, Canberra, 2000) (hereinafter "*In the Public Interest*"). The terms of reference were "to evaluate the appropriateness, effectiveness and privacy implications of the existing self-regulatory framework in relation

> *The small number of major commercial interests in Australia's media industries, and the potential threat posed to the public interest by the push for higher circulation and ever higher ratings, suggest a need for an effective system of their regulation. Without it, private corporate interests may well be promoted over and above the public interest.*

Professor Mark Pearson, the Head of Communication and Media Studies at Bond University, is quoted[48] in the Senate Select Committee Report, as follows:

> *We have a whole shift in media outlets – a shift in attitude towards the bottom line, circulations and ratings while still flying the flag of public interest and press freedom. You wonder who is the real master sometimes of these organisations – whether it is the MBA that is ruling the newsroom, as one American article suggested, or whether it is a legitimate concern for public interest rather than just what is interesting to the public.*

Not mutually exclusive

3.28 Privacy and freedom of expression should not be regarded as mutually exclusive. Freedom of speech or expression is a universal human right, not the exclusive preserve of the media, and it can be enhanced through confidence in the *privacy* of one's communications and activities. The feeling that one is being watched or monitored can easily have a chilling effect on freedom of speech. Journalists know this well when it comes to protecting their sources:

> *The media have been pressing for legislative action to protect journalists from the law of contempt in cases where they invoke an ethical obligation to keep secret the identity of a confidential source. It bases its claim on the argument that the ability to keep a source confidential is essential to the maintenance of the free flow of information in a democratic society and that sources of information will dry up if journalists are forced to disclose them. Unless they can guarantee anonymity they will not be trusted with information which needs to be disclosed in the public interest.*[49]

PRIVACY INVASION

3.29 In *ABC v Lenah Game Meats* Chief Justice Gleeson observed[50] that there were certain kinds of information about a person that may be easy to identify as private, such as information relating to health, personal relationships or finances. One might add that where private information is easily identifiable, its breach is more readily discernible. However, sometimes

---

to the information and communications industries and, in particular, the adequacy of the complaints regime."

48. *In the Public Interest* at para 1.9.
49. Australia, Senate Standing Committee on Legal and Constitutional Afairs, *Off the Record: Shield Laws for Journalists' Confidential Sources* (Senate Printing Unit, Canberra, 1994) at para 2.4.
50. (2001) 208 CLR 199 at 226.

disagreement may arise as to what constitutes an invasion of privacy. For example, SBS states:[51]

> *The Commission's emphasis in its Report is on the collection of material, with no distinction made between a private individual and a journalist. The key issue for media organisations, however, is not the* collection *of material but its* dissemination*. Any harm suffered by an individual results from the broadcast or publication of the material and breaches of privacy in the media tend to occur in a context of disclosure. The emphasis on collection rather than publication, which is the critical issue for the media, is therefore inappropriate.*

It is self-evident that an individual's privacy is invaded as much by the collection of personal information about that individual as by its dissemination. The Commission stated earlier that "the threshold problem with surveillance remains the act itself: being watched or otherwise monitored."[52] The Commission reaffirms its position. Whether privacy is breached is not a question of *who* is breaching it. It makes little sense to assert that the unauthorised collection of personal information, by means of surveillance, is somehow less intrusive on personal privacy if carried out by a journalist than by a "private individual".

3.30 Were material collected through covert surveillance and not broadcast or published, no opportunity would arise to test whether the surveillance was carried out in the public interest. On the test proposed by SBS, putting the emphasis on broadcast not collection, the media would have licence to carry out surveillance without accountability so long as the material did not come to light. Yet it is the public interest in publishing the material that is the media's major justification for engaging in surveillance.

THE CURRENT SELF-REGULATORY REGIME

3.31 In the Interim Report we addressed arguments for and against self-regulation,[53] concluding that the public interest in this regard would be better served by making users accountable for their use of surveillance. The Commission has not conducted any detailed research into the media effort at policing themselves. In response to matters raised in submissions, however, the Commission makes the following observations.

3.32 Both SBS and Free TV make the point that the level of complaints about privacy is low compared to those of, for example, accuracy and bias.[54] The Commission accepts this. In the seven years ending 2001-2002, Free TV reports that privacy complaints never constituted more than 1.7% of the total number of complaints. The most recent report of 2002-2003, however, has the figure at 2.4%, double that of the previous year.[55] The Commission wonders at the relevance

51. SBS, *Submission* at 7.
52. Report 98 at para 3.29.
53. Report 98 at para 3.84-3.99, 4.17-4.20.
54. SBS, *Submission* at 6; Free TV, *Submission* at 9.
55. Free TV Australia, "Commercial Television Industry Annual Code Complaints Report 2002-2003" (as at 1 October 2004)

of presenting privacy complaints as a percentage of the total received, especially when privacy complaints will only be relevant to a small percentage of the programs broadcast. The table lists 15 categories of program.[56] Every one of these categories logged complaints relating to program classification, particularly concerning sex, nudity or sexual references. This ground of complaint, at 24.7% of the total, constituted the greatest proportion of the total number of complaints received. The next highest ground of complaint, constituting 22.5% of the total, related to sex and nudity, and complaints were logged in 11 of the 15 categories. Privacy complaints, by contrast, applied to only two categories of program, news and current affairs. If one considers news programs in isolation, one finds that of the total number of 73 complaints lodged against these, 12 (or 16%) related to privacy.

3.33 Stations reported receiving a total of 741 written complaints during 2002-2003, of which they upheld 20 (2.7%). One of these related to privacy. Viewers then chose to refer to the Australian Broadcasting Authority ("ABA") 33 (4.5%) of the complaints that had been assessed but not upheld by the stations. Of these, 12 were upheld by the ABA. We are not told the nature of the complaint in these cases. Free TV's Report concludes "the small number of complaints referred to the ABA indicates that in more than 95% of cases viewers are satisfied with the station's investigation and response."[57] Possibly this analysis is correct, but it is impossible to know for certain. The Commission does not take issue with the proposition that privacy complaints are not high. The reports available to the public, however, do not provide much detail from which to draw any clear assessment as to the level of public satisfaction.

3.34 On the matter of enforcement mechanisms the Commission would cite one example, raised by Free TV. The Interim Report made mention of the Senator Bob Woods case.[58] This prompted Free TV to comment:[59]

> *[W]hat the Commission ignores is that in this case, the Australian Press Council's decision clearly illustrates that there are already appropriate forums in place that govern the media. These forums are able to adjudicate appropriately on the sometimes competing interests of privacy and freedom of speech.*

3.35 How effective are these forums? The Senate Select Committee that considered media regulation[60] reported the aftermath of the Press Council's finding in the Woods case, namely that the publication was "a blatant example of the unjustified breach of privacy":

> *The newspaper printed the adjudication but took issue with it in an editorial on the same day. The editorial stated that Senator Woods' wife became a public figure when her husband introduced her through his statement regarding allegations that*

«www.ctva.com.au/documents/Annual_Code_Complaints_Report_2002-2003.pdf» at Appendix 2 part (i).

56. Children, comedy, current affairs, documentary, drama, information, movie, music video, news, program promos, quiz, religion, sport, unspecified and variety.
57. Commercial Television Industry Annual Code Complaints Report 2002-2003 at 6.
58. Report 98 at para 2.25, 4.42.
59. Free TV, *Submission* at 14.
60. Australia, Senate Select Committee on Information Technologies, *In the Public Interest: Monitoring Australia's Media* (Senate Printing Unit, Canberra, 2000) at para 2.24.

he had misused his parliamentary entitlements, and when her activities were investigated by the Australian Federal Police.

Some nine months later and after Senator Woods had left the Senate the newspaper republished one of the photographs when the photographer won a merit award in the Nikon-Kodak press photographer awards for a portfolio which included the offending photo. When the Committee questioned [the APC's] Mr Herman about the re-publication, he replied that:

… the Press Council is not aware of that, if I can say so, because we have not received a complaint about it. The Press Council does not operate as judge, jury and prosecutor. The Press Council operates … on complaints received from the public, from organisations and individuals. Until we receive such a complaint, we do not act.

The photograph in the Daily Telegraph *that was the subject of the successful complaint also appeared on the same day in the* Herald Sun*, the* Courier-Mail*, the* Advertiser *and possibly other newspapers. Yet the APC's adjudication did not deal with these publications, presumably because the complaint related only to the* Daily Telegraph*. Once again the other publications thereby escaped censure as a result of the narrow, reactive approach taken by the APC.*

4. Overt surveillance

- Introduction
- Notice
- Scheme of regulation

INTRODUCTION

4.1 If an activity constitutes overt surveillance under the proposed legislation, the media or any other surveillance user may engage in it, so long as it is carried out in accordance with the regulatory scheme. Comments on the proposed framework for overt surveillance came mostly from media organisations, despite the fact that operators of CCTV and other security systems are the surveillance users most affected. The impact on the media would be limited, because the preponderance of newsgathering activity would be outside the scope of the proposed Surveillance Act. Media organisations generally opposed suggestions that tended to limit their discretion to gather material by means of overt surveillance. In general they also opposed measures that would impose on the media a greater degree of accountability than the current self-regulatory regime.

NOTICE

4.2 Notice, as we said earlier,[1] is the element distinguishing overt from covert in the Commission's proposed scheme for the regulation of surveillance devices.[2] However, the Interim Report contained suggested exceptions to the requirement for giving notice.[3] One such exception applied to the media in their everyday news gathering capacity, in recognition of the impracticality such an obligation would impose.[4] It is not clear if all media organisations fully appreciated the Commission's position. For example, Fairfax submits that the Interim Report proposes "what we believe to be an unworkable system of notification and authorisation, in the absence of which almost any act of news gathering risks being deemed covert surveillance."[5] This is incorrect. A lack of notification by the media has been stated explicitly *not* to result in this consequence,[6] while authorisation plays no part in the regulation of overt surveillance. The ABC states:[7]

> *The existence of a remote camera situated on top of a building, for example, to film an event on Sydney Harbour, would not be apparent to anyone participating in that event. Similarly, it would not be readily apparent that an ABC helicopter flying overhead was filming. Providing more direct notification is impractical. … [T]he possibility that day-to-day news gathering could constitute overt surveillance makes it possible for a person to complain that they were not aware they were being watched and that the media's recording constitutes covert surveillance.*

SBS comments[8] that in a case where:

1. Para 1.9.
2. Report 98, Rec 9, 13.
3. Report 98 at para 4.26-4.28.
4. Report 98 at para 4.26.
5. Fairfax, *Submission* at 6.
6. Report 98 at para 4.26.
7. ABC, *Submission* at 6.
8. SBS, Submission at 9.

> *a cameraperson is openly filming a political rally … it may not be clear whether the individuals who are a certain distance away are aware they are being filmed, creating immense practical problems in the distinction [between overt and covert surveillance] as drafted.*

4.3 Given the proposed media exemption from being required to provide notification, it is difficult to understand either the nature of the "immense practical problems" foreshadowed in, or even the relevance of, the foregoing comments from the ABC and SBS. In any event, for the reasons already stated above,[9] the types of scenario described here are ones to which the proposed legislation is unlikely to apply.

4.4 SBS[10] further referred to:

> *the Commission's mistaken assumption that a subject invariably knows they are being photographed. This is simply not the case when filming streetscapes, crowds, or public events such as rallies.*

The Interim Report[11] stated:

> *[M]edia coverage of newsworthy events could easily include footage of* members of the public unaware they are being recorded*. Much of the everyday activity of media organisations would be impossible or unduly cumbersome if notice to surveillance subjects were compulsory. So long as recording is carried out openly, and no attempt is made to actually conceal surveillance devices, it appears reasonable in such cases to dispense with notice requirements. (emphasis added)*

SCHEME OF REGULATION

4.5 The mechanism proposed in the Interim Report for the regulation of overt surveillance comprises two main elements, namely codes of practice and overt surveillance principles.

Codes of practice

4.6 It was proposed that some surveillance users be required to adopt a code of practice, consistent with the overt surveillance principles, in relation to their use of surveillance. Although the code would be mandatory, in practice it would operate as an internal working document. Advantages of requiring surveillance users to adopt codes of practice were discussed in the Interim Report at para 4.32 and following.

4.7 Privacy NSW, the Office of the New South Wales Privacy Commissioner, suggested[12] that the development of a written code not be mandatory, due to confusion and the unnecessary expenditure of time and resources in determining such issues as to which surveillance users

9. Eg para 3.4-3.5.
10. SBS, *Submission* at 9-10.
11. Report 98 at para 4.26.
12. Privacy NSW, *Submission* at 4.

would be required to have a code. It suggested that the "default position" for all surveillance users should be, simply, compliance with the overt surveillance principles. The Commission agrees that this eliminates a potentially confusing and cumbersome administrative layer. As the Commission has maintained throughout that it wishes to avoid imposing unnecessary burdens on lawful surveillance users, the adoption of codes of practice will not be mandatory.

4.8 Many organisations already have codes of practice in place and will choose to continue doing so. Privacy NSW also suggests that a public sector agency, already required to implement a privacy management plan,[13] could include within that plan overt surveillance principle compliance measures, "[reinforcing] the message that surveillance is inherently an interference with individuals' privacy".[14]

Overt surveillance principles

4.9 Eight mandatory principles, designed to facilitate the responsible and accountable use of overt surveillance, were discussed in the Interim Report at para 4.38 and following.[15] If engaging in overt surveillance, the surveillance user must comply with all the principles applicable to that user. The principles do not apply to non-surveillance activities such as recreational photography and would also have minimal application to the media. In light of comments contained in submissions, further discussion of specific principles follows.

Principle 1 Overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy

4.10 In the Interim Report we described the "reasonable expectation of privacy" as an intuitive measure of the acceptability of surveillance conduct.[16] The concept of a reasonable expectation of privacy is an acknowledgement of the flexibility required to accommodate different circumstances, including the nature of the surveillance device, the surveillance subject, the location, the occasion and so on. The activity in which the surveillance subject is engaged is also relevant, so that wrongdoing is not shielded by a claim for privacy.

4.11 According to some media submissions, the concept gives rise to "definitional problems"[17] and is "an ambiguous concept".[18] In particular, these organisations expressed concern at how the concept would apply to those actively courting publicity. For example, whereas the Commission stated[19] that people who court publicity may be entitled to a lower expectation of privacy *in some contexts*, SBS proposed[20] that "a lesser entitlement to privacy for people actively seeking publicity is justifiable in *all* contexts".[21] Either view fits easily within the notion of

13. *Privacy and Personal Information Protection Act 1998* (NSW) s 33.
14. Privacy NSW, *Submission* at 4.
15. See also Rec 17.
16. Report 98 at para 4.41-4.43.
17. SBS, *Submission* at 10.
18. Free TV, *Submission* at 14.
19. Report 98 at para 4.42.
20. SBS, *Submission* at 11.
21. Cf Australian Press Council Privacy Standards November 2001 "Public figures necessarily sacrifice their right to privacy, where public scrutiny is in the public interest. However, public

a "reasonable expectation of privacy", the rationale of which lies in recognising that different circumstances generate different responses in terms of privacy protection from overt surveillance.

4.12 Celebrities, politicians and others who figure often in the public eye, and often have a mutually beneficial relationship with the media, would generally have a lesser expectation of privacy than others. Judicial discussion of this subject appeared recently in *Campbell v MGN Limited*.[22] The House of Lords found in favour of the appellant, the celebrated model Naomi Campbell. Having previously declared publicly that she neither took drugs nor had a drug problem, she sued the publisher of an English newspaper after it published information relating to her treatment for drug addiction, as well as photographs of her taken covertly in the street as she attended meetings of Narcotics Anonymous ("NA"). There was general agreement that the appellant could not complain about the revelation of her drug usage and the fact that she was receiving treatment, given that she had publicly lied about it previously in order to present a false image. However, the majority held that publishing details of the treatment, as well as photographs taken covertly in the street of the appellant emerging from an NA meeting, amounted to an unjustifiable infringement of her right to privacy. On the subject of celebrity, Lord Hoffmann, dissenting, commented:[23]

> *She and they have for many years both fed upon each other. She has given them stories to sell their papers and they have given her publicity to promote her career. This does not deprive Ms Campbell of the right to privacy in respect of areas of her life which she has not chosen to make public. But I think it means that when a newspaper publishes what is in substance a legitimate story, she cannot insist upon too great a nicety of judgment in the circumstantial detail with which the story is presented.*

His Lordship was also of the opinion[24] that:

> *the fact that she is a public figure who has had a long and symbiotic relationship with the media …[does] not in itself justify publication. A person may attract or even seek publicity about some aspects of his or her life without creating any public interest in the publication of personal information about other matters.*

4.13 Lord Hope, similarly, observed "it is not enough to deprive Miss Campbell of her right to privacy that she is a celebrity and that her private life is newsworthy."[25] Princess Caroline of Monaco brought a complaint under Article 8 of the European Convention on Human Rights, that decisions of German courts had infringed her right to respect for private life by failing to prevent the publication by German newspapers of photographs taken without her knowledge. In June 2004 the European Court of Human Rights found there had been a violation of her rights. The

---

figures do not forfeit their right to privacy altogether. Intrusion into their right to privacy must be related to their public duties or activities."

22. [2004] 2 All ER 995.
23. [2004] 2 All ER 995 at 1012.
24. [2004] 2 All ER 995 at 1011.
25. [2004] 2 All ER 995 at 1026.

Court stated that "anyone, even if they are known to the general public, must be able to enjoy a 'legitimate expectation' of protection of and respect for their private life."[26]

4.14 By contrast, ordinary members of the public may, through circumstances not of their own choosing, find themselves in the media spotlight. In mid-2004 the public witnessed the media circus surrounding the attendance at a Darwin court of Joanne Lees, key witness in the Peter Falconio murder case. The authorities assisted her in her desire to shy away from the media. It was reported, however, that due to concern at someone being injured in the melee, Ms Lees offered media organisations the opportunity to film her at a location of her choosing, and for a fee payable to charity. Following the failure to reach an agreement, several media organisations said they would continue to pursue her.[27]

4.15 Free TV, the peak industry body representing the free-to-air commercial broadcasters, asks "what if the person is the subject of unsolicited but warranted public scrutiny?"[28] In response one might ask who decides whether the scrutiny is "warranted", and to what extent? The answer implicit in Free TV's query is the media. The Commission questions why such a determination should be left entirely to them, especially when there is so little recourse by the surveillance target to a remedy in cases where the surveillance by the media has overstepped the mark. The media should not be hamstrung in pursuing their legitimate activities; they should also be meaningfully accountable when they get it wrong.

4.16 The Commission believes the flexibility of the "reasonable expectation" concept is of greater relevance and utility in the range of circumstances discussed above, than the existing assortment of privacy-related self-regulatory provisions. The following are examples of the latter:

> Respect private grief and personal privacy. Journalists have the right to resist compulsion to intrude.[29] (AJA)
>
> The rights of individuals to privacy should be respected in all SBS programs. However, in order to provide information to the public relating to a person's performance of public duties or about other matters of public interest, intrusions upon privacy may, in some circumstances, be justified.[30] (SBS)
>
> The rights of individuals to privacy should be respected in all ABC programs. However, in order to provide information which relates to a person's performance

26. *Von Hannover v Germany* (application no 59320/00) at para 69.
27. "Lees Media Deal Reaches Stalemate" *ABC Online* (21 May 2004) «www.abc.net.au/news/newsitems/s1113058.htm».
28. Free TV, *Submission* at 14.
29. Media Entertainment and Arts Alliance, "Australian Journalists' Association Code of Ethics" (as at 7 September 2004) «www.alliance.org.au/hot/ethicscode.htm» , Principle 11.
30. Special Broadcasting Service, "Codes of Practice" (as at 25 October 2004) «sbs.com.au/media/1706Codes.pdf», cl 2.7.

> of public duties or about other matters of public interest, intrusions upon privacy may, in some circumstances, be justified.[31] (ABC)
>
> In broadcasting news and current affairs programs, licensees … must not use material relating to a person's personal or private affairs, or which invades an individual's privacy, other than where there is an identifiable public interest reason for the material to be broadcast.[32] (Free TV)
>
> Readers of publications are entitled to have news and comment presented to them honestly and fairly, and with respect for the privacy and sensibilities of individuals. However, the right to privacy should not prevent publication of matters of public record or obvious or significant public interest. Rumour and unconfirmed reports, if published at all, should be identified as such.[33] (APC)

4.17 Most of the provisions are fairly broad, not drafted with specific regard to the gathering of material by means of surveillance devices, and leave the issue of privacy intrusion to the discretion of the journalist or broadcaster/publisher. It is not clear, for example, whether the SBS code supports SBS's proposition above (see para 4.11) regarding those seeking publicity. Free TV's provision refers specifically to the "broadcasting" and "use", rather than "collection", of material. Contrast these with the privacy provisions contained in the code of practice of the United Kingdom's Press Complaints Commission ("PCC"),[34] also a self-regulatory system:

> i. Everyone is entitled to respect for his or her private and family life, home, health and correspondence, including digital communications. Editors will be expected to justify intrusions into any individual's private life without consent.
>
> ii It is unacceptable to photograph individuals in private places without their consent.
>
> Note – Private places are public or private property where there is a reasonable expectation of privacy.

The public interest exception applicable to the above clause is explained in the code as follows:

> 1. The public interest includes, but is not confined to:
>
> i) Detecting or exposing crime or serious impropriety.

31. Australian Broadcasting Corporation, Code of Practice 2004 (as at 12 October 2004) «www.abc.net.au/corp/codeprac04.htm» cl 2.5. See also ABC Editorial Policies cl 10.9 «abc.net.au/corp/edpol02.pdf».
32. Free TV Australia, "Commercial Television Industry Code of Practice July 2004" (as at 6 September 2004) «203.147.163.200/documents/Code_of_Practice_July_2004.pdf», cl 4.3.5.
33. Australian Press Council, "Statement of Principles" (as at 12 October 2004) «www.presscouncil.org.au/pcsite/complaints/sop.html» principle 3.
34. United Kingdom Press Complaints Commission, "Code of Practice" (as at 26 October 2004) «www.pcc.org.uk/cop/cop.asp» cl 3.

ii) Protecting public health and safety.

iii) Preventing the public from being misled by an action or statement of an individual or organisation.

2. There is a public interest in freedom of expression itself.

3. Whenever the public interest is invoked, the PCC will require editors to demonstrate fully how the public interest was served.

4. The PCC will consider the extent to which material is already in the public domain, or will become so.

5. In cases involving children under 16, editors must demonstrate an exceptional public interest to over-ride the normally paramount interest of the child.

4.18 In contrast with the views contained in media submissions, the concern expressed by Privacy NSW[35] is that by using the "reasonable expectation" formulation, the onus will fall on the individuals who are targeted by overt surveillance to prove that their expectation of privacy was reasonable, a task made more difficult in an environment in which an expectation of privacy is diminishing through the proliferation of CCTV, strengthened airport and other security measures and so on. Privacy NSW recommends that the principle should therefore be amended, such that overt surveillance "not intrude unnecessarily or unreasonably into a person's private affairs or personal space," and that the obligation should rest on the surveillance user to justify why an interference with privacy is warranted. By analogy, Privacy NSW cites Information Protection Principle 4 ("IPP 4") of the *Privacy and Personal Information Protection Act 1998* (NSW),[36] which requires an agency collecting personal information to ensure that, amongst other things, collection of the information "does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates".[37]

4.19 Privacy NSW's observation, that "reasonable expectation of privacy" is a reflective rather than proscriptive standard,[38] may well be accurate. Nevertheless, the Commission does not regard it as a workable scheme of regulation to require every overt surveillance user to justify surveillance in the individual circumstances pertaining to each surveillance target. It is difficult to see how this could be feasible in regard to the use of, for example, street cameras. In contrast with IPP 4, which deals specifically with "personal information", not all the information gleaned by street cameras is personal; nor can every individual within range of a CCTV camera be said to be under surveillance within the terms of the proposed Act, as there may be no deliberate intention to monitor each person so "captured" in order to obtain information about that person. Because CCTV and other such devices are installed with the intention, or at least the potential, to carry out surveillance on some individuals, they need to be operated in accordance with the proposed Act. However, to require CCTV operators to justify the filming of each individual within range would be unduly onerous.

35. Privacy NSW, *Submission* at 6.
36. Section 11.
37. Section 11(b).
38. Privacy NSW, *Submission* at 7.

4.20 The Commission does acknowledge that as the public becomes increasingly accustomed to being watched, the bar may be raised for anyone attempting to establish he or she had a reasonable expectation of privacy in given cases. However, legislation such as that being here proposed is designed to maintain an expectation of privacy by restraining unwarranted intrusions by surveillance devices into personal privacy, and thus helping to prevent daily life becoming a surveillance free-for-all.

Principle 2 Overt surveillance must only be undertaken for an acceptable purpose

4.21 This was discussed in the Interim Report at paragraphs 4.44 to 4.46. The Commission stated[39] that overt surveillance should be permissible only for one or more of the following purposes:

1. protection of the person
2. protection of property
3. protection of the public interest
4. protection of a legitimate interest

4.22 Submissions contained no suggestions for other purposes to be added to this list. Fairfax[40] comments:

> *We note that the investigation of, or activities connected with, the reporting of news and current affairs, comment, opinion or discussion of matters of public concern does not rate a mention as an "acceptable purpose"…*

This is not correct. First, the commentary on Principle 2 in the Interim Report begins with a reference to an earlier discussion of "legitimate uses of overt surveillance", that contained a paragraph[41] headed "collection of material for news and entertainment". Secondly, and more significantly, the third stated purpose, namely "protection of the public interest", is a broad category that explicitly includes the media in the discussion at para 4.46 of the Interim Report. Thirdly, it is unclear what activities such as "comment, opinion or discussion of matters of public concern" have to do with surveillance.

4.23 The Interim Report stated that, to avoid breaching the proposed Act, surveillance users must ensure their operations can be justified according to one or more of the criteria enumerated above.[42] Fairfax interprets this statement as requiring "an affirmative case to be made out first, that the use is for protection of the public interest or protection of a "legitimate" interest, and thereafter that any infringement of a private right to privacy is outweighed by those factors."[43] To what "case" does this refer, and to whom is it presented? Under the regulatory regime being

39. Report 98 at para 4.44.
40. Fairfax, *Submission* at 7.
41. Report 98 at para 3.19. See also para 1.34 regarding the important social contribution of the media.
42. Report 98 at para 4.45.
43. Fairfax, *Submission* at 7.

proposed, overt surveillance users require no prior approval in conducting their activities. Subsequently, they may be called to account if a complaint is made. Even under existing self-regulatory codes[44] the invasion of personal privacy is not sanctioned unless in the public interest. It must be assumed, therefore, that the media already engages in the exercise of considering whether any surveillance it undertakes is in the protection of the public interest. The concept referred to by Fairfax, of "a private right to privacy", is not alluded to in the Interim Report, nor is it applicable to the proposed legislation.

4.24 The Interim Report stated[45] that "in cases of doubt, recourse may be had to the Privacy Commissioner for a ruling as to whether the purpose is acceptable." SBS responded[46] that it:

> *does not believe it is appropriate for an external body to be given responsibility for ruling on definitions of public interest for the purposes of news gathering and media reporting. There would also be practical problems in obtaining consent in the case of breaking news.*

Fairfax[47] rejected:

> *any suggestion that it should be in a position to have its publications "vetted" in this or any other way by a non-elected non-judicial appointee of the executive government, according to subjective and as yet undefined notions of taste or propriety.*

4.25 In complying with Principle 2 – as with Principle 1 – media organisations and other overt surveillance users are expected to make their own decisions and use their own judgment. With regard to overt surveillance, no suggestion of "vetting" or need to obtain consent from any kind of official was mentioned. As was clear from the words used, no compulsion is involved in the suggestion that "recourse may be had"[48] to the Privacy Commissioner for guidance. This suggestion was put on a purely discretionary basis and entirely at the instigation of the surveillance user.

4.26 Privacy NSW expressed the view that the four categories of acceptable purpose should be restricted. For example, with respect to private individuals or organisations, protection of the public interest should only be claimable by the news/current affairs media.[49] Furthermore, Privacy NSW suggested that overt surveillance by "domestic" users to protect the person or property should only be permissible on the user's own property, including entrances and exits, while surveillance of neighbouring properties should not be permitted at all. In the context of commercial users of overt surveillance Privacy NSW commented:[50]

---

44. See para 4.16.
45. Report 98 at para 4.46.
46. SBS, *Submission* at 11.
47. Fairfax, *Submission* at 8.
48. Report 98 at para 4.46.
49. Privacy NSW, *Submission* at 10.
50. Privacy NSW, *Submission* at 10-11.

> *The Act should allow regulations to be prescribed to define the limits of what may be considered "reasonably necessary" for [the protection of their property, commercial interests, or the personal safety of their staff or clients], allowing for some differences across industry sectors, taking account for instances of the type and frequency of surveillance and the relative risks to the organisation.*

Given the countless instances of legitimate surveillance usage in society, and the varying circumstances in which they occur, the adoption of these suggestions would lead to a scheme of regulation that is overly prescriptive, lacking flexibility, and difficult to administer. Other Overt Surveillance Principles, such as those that protect a reasonable expectation of privacy, and require that surveillance be conducted in a manner appropriate for purpose,[51] are designed to allow for adjustments to the facts of a particular case.

4.27 Privacy NSW suggests[52] that, as Principle 2 "reflects the sense of the fundamental threshold nature of the 'purpose' test", it should be Principle 1. The Commission agrees that any proposed legislation should reverse the orders of Principles 1 and 2 as they appear here and in the Interim Report.

Principle 4 Notice provisions shall identify the surveillance user

4.28 It was proposed in the Interim Report[53] that notices advising the public that surveillance is being conducted in an area should also be required to display the identity of the surveillance user and provide contact details to which enquiries and complaints can be directed. Privacy NSW suggests[54] this be taken further, and public sector surveillance users required:

> *at a minimum … [to] be obliged to erect signs which show the agency's name, the purpose of collection, and the circumstances in which footage will be used and disclosed to other authorities. A phone contact number should be included to identify who should be contacted to obtain additional information.*

The Commission does not regard this measure as contributing a practical benefit, and may rather contribute to visual clutter through excessive signage. The salient feature of Principle 4 is that a member of the public wishing to gain more information pertaining to the surveillance should be able to do so without undue difficulty.

Principle 5 Surveillance users are accountable for their surveillance devices and the consequences of their use

4.29 Paragraphs 4.50 and 4.51 of the Interim Report, together with Recommendation 20, suggest measures for keeping account of surveillance devices, in particular a requirement that a register be kept of such details as the number and location of surveillance devices. SBS queried[55] whether this was intended to apply to the media. It was not intended to apply to the media's news gathering equipment (as opposed to station security cameras and the like), and an exemption to this effect should be included in the proposed legislation. Recommendation 20

51. Principle 3: see Report 98 at para 4.47.
52. Privacy NSW, *Submission* at 8.
53. Report 98 at para 4.48-4.49.
54. Privacy NSW, *Submission* at 12.
55. SBS, *Submission* at 12.

required both public sector surveillance users and "relevant surveillance users" to maintain a register. [56] With the abandoning of the proposal that codes of practice be mandatory, reference to a "relevant surveillance user" is redundant. The Principle should therefore apply to public sector users, as well as private non-domestic users. Regulations could stipulate which surveillance users falling into the latter category need to keep a register. Proprietors of a corner store, for example, who operate a single security camera, could be exempted from this requirement.

Principle 6 Surveillance users must ensure all aspects of their surveillance system are secure

4.30 This principle is concerned with establishing a secure system of CCTV and similar surveillance devices, so as to ensure that the integrity of the system and the confidentiality of material collected, are maintained. The surveillance material referred to in para 4.59 of the Interim Report was the type obtained from security devices. SBS addressed this Principle[57] in terms of the restrictions it places on copying or transcription of material. This issue will be referred to in the discussion below of Principle 7. It is proposed to exempt the media from compliance with Principle 6 in the context of news gathering.

4.31 In furtherance of this principle, the Interim Report recommended[58] that staff operating equipment in control rooms with which to conduct overt surveillance should be licensed in accordance with the *Security Industry Act 1997* (NSW). Under that Act a person must hold a licence in order to carry out a security activity.[59] A person carries on a "security activity" if, in the course of conducting a business or in the course of employment, the person patrols, protects, watches or guards any property,[60] or installs, maintains, repairs or services security equipment.[61] The Interim Report stated the Commission's understanding that staff hired to monitor security cameras are required to hold a licence under the *Security Industry Act 1997*. Recommendation 21 went further, recommending that the definition of "security activity" be widened to include the monitoring or operating of surveillance (as opposed to security) equipment. The Commission has received confirmation[62] that the watching of security camera monitors is considered to fall within the definition of a security activity. Section 4(b) is intended to apply to those persons employed specifically for this function, but not to those who may, in the course of other duties, undertake such activity eg, a receptionist providing access to visitors or staff members after first ascertaining their identities from a monitor.

4.32 In relation to other types of surveillance devices, such as tracking devices, which are not necessarily used for security but rather as "an asset and/or employee management tool", the *Security Industry Act 1997* has been interpreted to exclude their monitoring from a licensing requirement.[63] The Commission received a submission from Minorplanet Asia Pacific Pty Limited

56. Report 98 at para 4.57.
57. SBS, *Submission* at 12.
58. Report 98, Rec 21.
59. *Security Industry Act 1997* (NSW) s 7.
60. *Security Industry Act 1997* (NSW) s 4(b).
61. *Security Industry Act 1997* (NSW) s 4(c).
62. Information supplied by P Houlton, Registrar, Security Industry Registry, NSW Police (by letter dated 15 December 2004).
63. Letter, Security Industry Registry.

("Minorplanet"), a company that installs and maintains Vehicle Management Information ("VMI") systems. These rely on tracking devices for clients to manage risks and costs arising from operating a fleet of vehicles.[64] According to Minorplanet, the VMI systems are used by their clients to provide information relating to the location of vehicles in their fleet, distances and speeds travelled by their vehicles, and the lengths of time for which vehicles are driven and stationary. The information is used for developing more efficient route plans, minimising unauthorised use of vehicles, proof of site visits and times, and other benefits to Minorplanet's clients.[65] Minorplanet maintains that the primary purpose for which its clients use its product is to track vehicles.[66] It submits that on the present definition its clients are not engaged in security activities;[67] however, were our recommendation to be adopted, their clients would require licences to carry out what are essentially fleet management, and not security, activities.

4.33 If the VMI systems are being used to track vehicles, then they are not surveillance devices within the meaning of the proposed Act. For a device to be regarded as conducting surveillance, it must be obtaining information about a *person*.[68] One of the Commission's concerns is that equipment such as tracking devices installed in vehicles can be used to keep the drivers of the vehicles under surveillance. In that circumstance, and where drivers have been notified of their use, the Commission is of the view that such devices should be operated only in accordance with the Overt Surveillance Principles. However, monitoring employees by means of such devices is the subject of a draft bill released in June 2004. The Workplace Surveillance Bill 2004, which has yet to be introduced into Parliament, would extend the regulatory scheme in the *Workplace Video Surveillance Act 1998* (NSW) to tracking surveillance and computer surveillance.[69] To avoid potential duplication of regulatory measures, the Commission does not plan to proceed with Recommendation 21 at this time.

Principle 7 Material obtained through surveillance to be used in a fair manner and only for the purpose obtained

4.34 The Interim Report stated[70] that, where it is sought to use material obtained for one acceptable purpose for another acceptable purpose, an order could be made to this effect. The Commission has decided to dispense with the requirement for an order, as this may prove an unduly cumbersome process for making surveillance material available for what is an acceptable purpose. This should meet the objections of SBS[71] and ABC[72], that limitations would be imposed on the provision of material to members of the public (for example, through copying and transcription) and on the sharing of information with other broadcasters and publishers.

64. Minorplanet, *Submission* at 1.
65. Minorplanet, *Submission* at 2.
66. Minorplanet, *Submission* at 3.
67. Minorplanet, *Submission* at 5.
68. Report 98, Rec 1, 2.
69. L Roth, *Workplace Surveillance* (Briefing Paper 13/04, NSW Parliamentary Library Research Service, 2004) at 1.
70. Report 98 at para 4.61.
71. SBS, *Submission* at 12-13.
72. ABC, *Submission* at 6.

Principle 8 Material to be obtained through surveillance to be destroyed within specified period

4.35 In paragraphs 4.64 to 4.66 of the Interim Report we discussed the optimum period for which surveillance material should be retained, setting the limit at 21 days, with extensions of time available in certain circumstances. The Report also made clear that this did not apply to the media where the material was obtained overtly and genuinely for media purposes, so that it could be retained for file footage. This is a wide exemption. SBS stated[73] that this Principle was in contravention of its obligations to retain records under the *Archives Act 1983* (Cth). To clarify the situation, the Commission proposes exempting from this Principle material obtained overtly and genuinely for media purposes.

Recommendation 1

The use of overt surveillance should be in accordance with the proposed Surveillance Act. For the purposes of the proposed Act the following are the Overt Surveillance Principles:

Overt Surveillance Principle 1:
Overt surveillance must only be undertaken for an acceptable purpose.

Overt Surveillance Principle 2:
Overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy.

Overt Surveillance Principle 3:
Overt surveillance must be conducted in a manner that is appropriate for purpose.

Overt Surveillance Principle 4:
Notice provisions shall identify the surveillance user.

Overt Surveillance Principle 5:
Surveillance users are accountable for their surveillance devices and the consequences of their use.

- Public sector surveillance users and private non-domestic surveillance users, as part of their compliance with this Principle, must maintain a register containing such details as the number, types and locations of all their overt surveillance devices. Regulations should specify the details required, together with criteria identifying private surveillance users to whom this requirement applies.
- News gathering equipment operated by media organisations is exempt from any requirement to be listed in a register of surveillance devices.

Overt Surveillance Principle 6:
Surveillance users must ensure all aspects of their surveillance system are secure.

- This does not apply to media organisations in the context of their news gathering activities.

Overt Surveillance Principle 7:

73. SBS, *Submission* at 13.

Material obtained through surveillance to be used in a fair manner and only for the purpose obtained.

Overt Surveillance Principle 8:
Material to be obtained through surveillance to be destroyed within specified period.

- Material obtained overtly and genuinely for media purposes is exempt from this Principle.

Role of the Privacy Commissioner

4.36 The Interim Report suggested various responsibilities and tasks that could be undertaken by the Office of the Privacy Commissioner.[74] However, Privacy NSW rejected[75] some of these, due to potential conflicts arising in cases which the Office might be called on to investigate and in which it had previously furnished advice. It also cited a lack of resources. It agreed with proposals regarding general powers[76] and inspection powers.[77] With regard to the latter, Privacy NSW suggested[78] that the proposed Act clarify that inspection might occur either as part of dealing with a complaint lodged with the Office or on a routine or random basis. The Commission agrees with this suggestion.

4.37 The Interim Report also suggested that a role in educating the public would be beneficial.[79] An example is publishing information relating to the use of CCTV and other surveillance devices, emphasising the need to protect personal privacy, and outlining the acceptable use of such devices. As well, Privacy NSW, acting in an advisory capacity only, could assist surveillance users to draft codes of conduct.

Recommendation 2

With respect to the regulation of overt surveillance, the Privacy Commissioner should have the following powers and functions:

- promoting, and providing assistance (eg, educational) for, compliance with the Overt Surveillance Principles;
- assisting surveillance users in drafting codes of practice;
- appointing inspectors to investigate complaints, and to conduct both routine and random inspections of surveillance systems or devices to ascertain compliance with the proposed Act;
- right of entry to non-residential premises to inspect surveillance systems or devices to ascertain compliance with the proposed Act;
- educating the public on the acceptable use of surveillance devices.

74. Report 98 at para 4.68-4.70.
75. Privacy NSW, *Submission* at 5.
76. Report 98 at para 4.68.
77. Report 98 at para 4.70.
78. Privacy NSW, *Submission* at 6.
79. Report 98 at para 4.69.

5. Covert surveillance recommendations

- Covert surveillance by law enforcement officers
- Covert surveillance in the public interest
- Covert surveillance in employment

5.1 This chapter examines specific recommendations concerning the conduct of, and accountability for, covert surveillance. The three-pronged structure follows that of Report 98, which provides for separate but complementary authorisation procedures for covert surveillance depending on whether it is conducted in the course of law enforcement, the public interest or employment. Some discussion in this Chapter is motivated by developments that have occurred following the release of the Interim Report, but in most cases the issues discussed are those raised in submissions and consultations.

5.2 Having taken all things into account, the Commission sees no need to recommend changes to the authorisation or accountability procedures set out in Report 98 for covert surveillance in law enforcement or employment. So far as covert surveillance in the public interest is concerned, while the Commission considers that the overall authorisation and accountability mechanisms remain valid, some changes are recommended, largely in response to the submissions received from media organisations and representatives of the insurance and private investigation industries.

COVERT SURVEILLANCE BY LAW ENFORCEMENT OFFICERS

Recommendations in Report 98

5.3 Chapter 5 of Report 98 outlines in detail the Commission's 47 recommendations concerning the regulation of covert surveillance conducted by law enforcement agencies.[1] Those recommendations are based for the most part on the existing warrant regime set out in the *Listening Devices Act 1984* (NSW) ("the LDA"). In summary, the Commission recommends that all covert surveillance conducted by law enforcement officers[2] must be authorised under a warrant issued by an "eligible judge" as declared by the Attorney General.[3] Warrants may be issued to authorise the use of any surveillance device[4] and in respect of any offence.[5] The Commission also made a series of recommendations concerning the grounds for determining whether the granting of a warrant can be justified,[6] the powers that may be authorised under a warrant,[7] as well as the specific information that must be provided to an eligible judge in a

1. Comprising Recommendations 22-48.
2. The Commission recommends that "law enforcement officer" should be defined broadly to include agencies such as the Australian Federal Police, State and Territory Police, the Australian Security Intelligence Organisation, the Independent Commission Against Corruption, the National Crime Authority, the NSW Crime Commission, Royal Commissions, the Police Integrity Commission, and any office holder specifically empowered to enforce a particular law: see Recommendation 23 at para 5.21.
3. See Recommendation 25 at para 5.35.
4. The Commission also recommends that one warrant may be issued to authorise the use of more than one device, or a device with more than one function: see Recommendation 44 at para 5.83.
5. See Recommendation 24 at para 5.27.
6. See Recommendation 26 at para 5.36-5.38.
7. See Recommendations 27-34 at para 5.39-5.57.

warrant application and contained in the warrant itself.[8] The Commission also recommended that a warrant should be in force for a maximum of 30 days.[9] The need to obtain a warrant in emergency situations was also acknowledged by the Commission, with provision being made for warrant applications to be transmitted by telephone, facsimile, email or other electronic means, and sought retrospectively in certain circumstances.[10]

Views in submissions

5.4 The Commission received only one submission on the issue of covert surveillance by law enforcement officers, that being from Privacy NSW. Although agreeing with the majority of the Commission's recommendations, Privacy NSW disagreed specifically with two of the Commission's recommendations concerning covert law enforcement. First, Privacy NSW considered that Recommendation 24, which provides that an application for a warrant should be able to be made with respect to any offence, should instead provide that a covert surveillance authority should only be available regarding serious indictable offences carrying a maximum penalty of at least seven years imprisonment.[11] Secondly, Privacy NSW was of the view that Recommendation 25 should be amended to provide that only Supreme Court judges should be allowed to issue warrants.[12]

The Commission's view

5.5 The Commission considered both of these issues in developing the recommendations for the Interim Report. In relation to Recommendation 24, the Commission noted that it is often not possible, when applying for a warrant, to know in advance whether the criminal activity under investigation would result in a prosecution for a summary or an indictable offence,[13] or whether it would fall within the category of offences carrying a maximum penalty of seven years imprisonment or longer.[14] Further, some offences, although not indictable, may be very serious in nature and warrant the use of covert surveillance in particular circumstances. The Commission continues to hold the view that not limiting the category of offences for which warrants may be sought is in the best interests of effective law enforcement, and considers that the fact that a warrant application must pass judicial scrutiny before any covert surveillance can occur is a sufficient safeguard against abuse. Given that the Commission also recommends that covert surveillance should be able to be authorised when justified in the public interest and in employment situations, it would seem anomalous to restrict law enforcement agencies access to covert surveillance in respect of particular offences.

5.6 So far as Recommendation 25 is concerned, the Commission noted in Report 98 that, while it was envisaged that "eligible judges" should wherever possible be drawn from the Supreme Court, there are two main reasons for not recommending that the legislation should

8. See Recommendations 35-37 at para 5.58-5.64, and Recommendations 39-43 at para 5.72-5.78.
9. Recommendation 38 at para 5.71.
10. Recommendations 47-48 at para 5.89-5.94.
11. This would accord with the *Telecommunications (Interception) Act 1979* (Cth).
12. Privacy NSW *Submission* at 19.
13. Report 98 at para 5.27.
14. The LDA currently provides that a warrant may be obtained in relation to a "prescribed offence", being an indictable offence or one prescribed by regulation for the purposes of Part 4, whether indictable or not: s 15.

restrict the category solely to Supreme Court judges. First, as the use of surveillance devices to combat criminal activity increases due to developing technological sophistication, the number of Supreme Court judges who have consented to become "eligible judges" may be insufficient to meet demand. Secondly, it may be impractical in rural areas to bring an application before a Supreme Court judge, which could jeopardise a covert operation.[15] While in this situation it may be possible to send an electronic emergency application,[16] or apply for retrospective authorisation,[17] the Commission is of the view that these provisions should be limited only to situations of genuine emergency and not resorted to because of administrative deficiencies in the warrant regime. Consequently, the Commission does not see any reason to deviate from Recommendation 25, which preserves the current position in the LDA.[18]

5.7 With regard to the remaining recommendations in Chapter 5 concerning the authorisation process for covert surveillance in law enforcement, the Commission has not been presented with any reason to recommend changes. The same applies for the accountability requirements in Chapters 8 and 9 insofar as covert law enforcement is concerned. The Commission is of the view that these recommendations provide the appropriate balance between efficient and effective law enforcement and the need to safeguard the privacy interests of those subject to intrusive surveillance. The recommendations were framed to be broad and flexible enough to avoid the need for constant change.

Mutual recognition

5.8 As noted in Chapter 2, in late 2003, the Standing Committee of Attorneys-General and the Australasian Police Ministers' Council Joint Working Group on National Investigation Powers produced a report ("the Joint Working Group Report") recommending model legislation dealing with cross-border investigative powers for law enforcement agencies.[19] The model laws relating to covert surveillance recommend procedures for authorising warrants, exceptions to the warrant provisions, and accountability measures, including reporting requirements and restrictions on the use of "protected information". The model laws are based on what the Joint Working Group considered to be the best practice provisions in existing Commonwealth, State and Territory surveillance legislation.[20]

5.9 The intention in developing the model laws was that the Commonwealth and the States and Territories would legislate to adopt the model laws to facilitate a more streamlined warrant application process in circumstances where investigations extend beyond the border of a single

15. See Report 98 at para 5.35.
16. Under Recommendation 47.
17. Under Recommendation 48.
18. See s 3B and s 16(7) of the LDA which allow the Attorney General to nominate District Court judges and Local Court magistrates to exercise the functions of an "eligible judge".
19. The model laws cover four areas of law enforcement: controlled operations, assumed identities, electronic surveillance and witness identity protection.
20. The Joint Working Group notes at several points throughout the Report that there is merit in other ways of approaching the regulation of surveillance, including the Commission's recommendations, but also notes that its brief was to examine existing laws and to facilitate the mutual recognition of warrants, rather than overhaul surveillance legislation in each jurisdiction: see, eg, Joint Working Group Report at 346-347 and 351.

State. In order to qualify for a warrant under the model laws, a law enforcement agency must satisfy the issuing authority in State A that the investigation will, or is likely to, cross the border into State B.[21] Should the warrant be issued, it would be recognised not only in State A, but also in State B (providing State B has adopted the model laws) without needing to obtain a separate warrant under the laws of State B, or involve the law enforcement agencies of State B. The Joint Working Group made it clear that the model laws are not intended to replace existing intra-state laws, but create an additional regime for cross-border investigations, thereby creating a dual system of surveillance regulation for law enforcement agencies.[22] The Joint Working Group Report notes that this reflects, to some extent, the "reality that each State and Territory has very different privacy and surveillance devices laws, making consistency in areas other than cross-border investigations difficult to achieve".[23]

The model laws

5.10 The model laws differ from the Commission's recommendations concerning covert surveillance in the following material respects. First, they are device-specific, covering only listening devices, optical surveillance devices, data surveillance and tracking devices. In addition, the laws distinguish between tracking and other devices, enabling tracking devices to be authorised by a magistrate (rather than a Supreme Court judge as per the other devices), as they were considered by the Joint Working Group to be less privacy invasive. In Report 98, the Commission discusses at length the drawbacks of device-specific legislation, and how increasingly convergent technology makes a distinct authorisation procedure for specific types of devices somewhat near-sighted and quickly outdated.[24] Secondly, warrants to conduct covert surveillance under the model laws may only be sought in relation to offences carrying a maximum penalty of three years imprisonment or more. The Commission notes at paragraph 5.5 above its reasons for not adopting this approach.

5.11 Other procedural differences include the recommendation in the model laws that a law enforcement officer of the rank of Inspector or above be empowered to issue emergency authorisations, which must be brought before a Supreme Court judge for approval within two business days.[25] The Commission is of the view that, given the serious privacy incursions involved in covert surveillance, judicial scrutiny of all warrant applications is desirable, and that remote applications by electronic means and the availability of retrospective authorisation should be sufficient to deal with emergency situations.[26] The model laws also recommend that the maximum duration of a warrant should be 90 days,[27] whereas the Commission recommends a 30 day maximum (in the interests of greater privacy protection and accountability), with the opportunity for further applications to be made should the time prove insufficient.[28]

21. See Model Laws cl 7(1)(b) and cl 9(1)(a).
22. Joint Working Group Report at 357 and 359.
23. Joint Working Group Report at 359.
24. See Report 98 para 2.15-2.19.
25. See model laws cl 21.
26. See Report 98 para 5.34 and Recommendations 47 and 48.
27. See model laws cl 10.
28. See Report 98 para 5.65-5.71 and Recommendation 38.

The Commission's view

5.12 The Commission notes that the adoption of both the model laws and the Commission's recommendations would result in two distinct covert surveillance regimes for intra-state and cross-border investigations. This could result in NSW police being required to observe one standard of accountability when undertaking investigations within NSW, and different standards when an investigation becomes cross-border. Similarly, interstate police would be able to conduct covert surveillance in NSW in relation to cross-border investigations subject to different accountability measures from those applicable to NSW police investigating NSW offences.

5.13 The Commission does not make any recommendation concerning whether or not NSW should participate in the model laws scheme, since its operation would extend beyond the borders of NSW. However, the Commission is of the view that its recommendations in Report 98 concerning surveillance by law enforcement officers remain the most effective way of upholding the dual public interests of efficient crime prevention and detection as well as the protection of individual privacy.

COVERT SURVEILLANCE IN THE PUBLIC INTEREST

Recommendations in Report 98

5.14 In Chapter 6 of Report 98, the Commission made a series of recommendations concerning covert surveillance in the public interest, recognising that there may be situations where a particular public interest may be so significant as to justify the displacement of individual privacy in certain circumstances. Due to the serious and intrusive nature of covert surveillance, the Commission recommended an authorisation process, as well as reporting and accountability measures,[29] roughly equivalent to those recommended for law enforcement officers.

5.15 The Commission examined the meaning of the term "public interest", and looked at comparable legislation in Western Australia, noting that the term could include media reportage, as well as surveillance conducted by private investigators and individuals, and could encompass the protection of private rights and interests in appropriate circumstances. The Commission concluded that the nebulous nature of the "public interest" defied precise definition, and recommended instead that the term should be interpreted broadly on a case by case basis by the authority issuing the authorisation to conduct covert surveillance in the public interest, and supplemented by guidelines supplied by the Privacy Commissioner.[30]

5.16 The Commission discussed the issue of whether a court or a specialist tribunal would be the most appropriate authority to issue public interest authorisations, deciding to leave the question open on the basis that the answer would be likely to be determined by practical matters such as the availability of resources.[31] The Commission also made recommendations concerning the information that should be provided to the issuing authority, the factors to be

29. Report 98, Chapters 8 and 9.
30. See Report 98 at para 6.1-6.23, Recommendations 49-51.
31. However, the Commission specified that whichever forum was considered to be the most appropriate, the authorisation process should be accessible, affordable, expeditious and impartial: see Report 98 at para 6.34-6.36, Recommendation 52.

considered in determining whether or not a public interest authorisation should be issued,[32] and the type of information that should be contained in such an authorisation.[33] The Commission also recommended that retrospective authorisation should be available in circumstances where prior authorisation is not possible or practicable.[34]

Views in submissions

Definition of public interest

5.17 The Australian Broadcasting Corporation ("the ABC") was of the view that there should be some broad inclusive legislative guidelines on what constitutes "public interest" which, to ensure consistency with the Australian Constitution, should refer to the discussion of government and political matter.[35] The Special Broadcasting Service Corporation ("SBS") also considered that there should be a legislative definition of public interest to make it clear what conduct is covered, and to prevent the authorising body from developing its own "objectionable criteria unfettered by any legislative restraints".[36] However, SBS was also of the view that the categories of public interest should not be foreclosed. SBS further considered that the examples of public interest given by the Commission do not adequately cover all aspects of the public interest and that it, as a media organisation, is "already positioned to determine that which serves a legitimate public need to enable the media to perform the public interest role".[37]

5.18 Privacy NSW was also concerned that the term "public interest" is commonly misunderstood, manipulated or inconsistently applied, and should therefore be specifically defined in the new Act in a way that "weighs appropriately the public interest in the protection of privacy as a human right against other interests". Privacy NSW agreed with the examples provided by the Commission at paragraph 6.11 of Report 98,[38] but considered that the emphasis should be on "ethical" rather than "immoral" behaviour. They also suggested that the definition could be supplemented by guidelines in regulations made by the Attorney General on the advice of the Privacy Commissioner.[39]

The Commission's view

5.19 In Report 98, the Commission did not consider it necessary to define the term "public interest", since its amorphous nature would mean that only a very broad, abstract (and virtually meaningless) definition would be appropriate. It is not possible to determine in advance every

32. Those factors include the nature of the interest or interests at stake, the extent to which individual privacy would be affected, the intended use of the information obtained as a result of the surveillance, whether or not other measures of obtaining the information had been used or may be more effective, and whether the public interest in each particular case justifies the displacement of individual privacy: see Report 98 para 6.37-6.38, and Recommendation 54.
33. Report 98, Recommendation 55.
34. Report 98 at para 6.43-6.44, Recommendation 56.
35. ABC *Submission* at 7.
36. SBS *Submission* at 14.
37. SBS *Submission* at 14.
38. See para 5.21.
39. Privacy NSW *Submission* at 21.

instance in which surveillance in the public interest would be justified.[40] Indeed, the difficulties inherent in the concept of public interest are evident in the SBS submission, which advocates a clear definition, but not one which proscribes the categories of public interest.

5.20 The Commission noted that the *Surveillance Devices Act 1998* (WA) defines public interest as including:

> *the interests of national security, public safety, the economic well-being of Australia, the protection of public health and morals and the protection of the rights and freedoms of citizens.*[41]

However, the Commission also noted that a definition is more relevant and helpful in the Western Australian context since their Surveillance Devices Act does not require authorisation prior to *conducting* covert surveillance in the public interest.[42] Under the Commission's recommended model, covert surveillance in the public interest would not be able to be conducted without prior authorisation by the issuing authority, which would weigh that particular interest or interests against considerations of privacy and other public interests, and so a broad definition would be of little value.

5.21 Nevertheless, while considering it unnecessary, the Commission is not completely opposed to an open-ended, inclusive definition of public interest, should that be considered desirable. That definition could be based on the Western Australian model, and should provide examples of the type of circumstances that may justify covert surveillance in the public interest, along the lines of those listed at paragraph 6.11 of Report 98. Those circumstances include, but are not limited to, allegations of:

- bribery or corruption scandals;
- paedophilia or child abuse;
- breaches of hygiene standards;
  medical negligence;
- insurance fraud;
- practices by retailers or manufacturers which may contravene consumer protection laws;
- threats to an individual's personal safety or legal or human rights;
- extortion or blackmail;
- the threat of misrepresentation or wrongful prosecution; or
- other illegal or unethical practices.

40. Report 98 at para 6.10-6.11.
41. *Surveillance Devices Act 1998* (WA) s 24.
42. Report 98 at para 6.10. Judicial authorisation must be obtained under the *Surveillance Devices Act 1998* (WA) before the information gathered as a result of conducting covert surveillance in the public interest can be published or communicated: s 31.

5.22 Whether or not the new surveillance legislation specifically defines public interest, the Commission continues to endorse Recommendations 50 and 51, namely, that the term should be interpreted as broadly as possible by the issuing authority, and that the Privacy Commissioner should be empowered to develop guidelines as to what may constitute the public interest from time to time.

5.23 The Commission also acknowledges the views of media organisations and Privacy NSW, to the effect that the specific role of the media in promoting the public interest, and the importance of privacy interests, should be specifically mentioned in any definition of public interest. However, the Commission considers that these issues should more appropriately be dealt with under the factors to be considered when deciding whether or not to grant a public interest authorisation, rather than in any definition of public interest.[43]

Impact on the media

Current media surveillance practices

5.24 The ABC noted that it does not engage in covert surveillance "as a matter of course", but where "all other appropriate avenues have been explored, appropriate editorial decision making has occurred and it believes that there is a legitimate public interest in doing so", and distanced itself from the "unsavoury practices" that characterise "some tabloid sections of the media".[44] Before using hidden cameras, the ABC's Editorial Policies require ABC Legal Services to be consulted, and the material obtained may not be broadcast without the approval of the Managing Director "having regard to the editorial principles and on the advice of the relevant divisional Director".[45]

5.25 SBS also stated that it uses covert surveillance "rarely and only in exceptional circumstances", following a "rigorous editorial process".[46] Despite this lack of frequency, SBS maintained that the impact of the Commission's recommendations would be severely restrictive, would "outlaw some of the most important journalistic investigation, and significantly inhibit investigative journalism justified in the public interest by requiring media organisations to convince judges that the investigation is genuine".[47]

Media's view of the Western Australian experience

5.26 At the consultation meeting held with media organisations, the Commission asked the media to detail their experience in dealing with the public interest provisions of the *Surveillance Devices Act 1998* (WA), which have been in operation for a number of years now.[48] The ABC considered the Western Australian Act to be unworkable, contending that retrospective authorisations from a judge to publish surveillance material under Part 5 of the Act have

43. See para 5.47 and Recommendation 3 of this report.
44. ABC *Submission* at 4.
45. ABC *Submission* at 4.
46. SBS *Submission* at 15.
47. SBS *Submission* at 15.
48. The Commission discusses the provisions of the Western Australian legislation in Report 98 at para 6.28-6.33.

generally cost "up to $5,000". "The time involved and the uncertainties of obtaining authorisation for such surveillance is often no longer a practical option for the media".[49]

5.27 Free TV Australia ("Free TV")[50] considered that the WA Act has "severely curtailed the ability of the media to communicate freely with members of the public on matters that are in the public interest".[51] Free TV stated that the WA provisions are rarely used in practice due to the cost involved in preparing affidavits and attending hearings (estimated at $3000-$5000), the risk of the application being refused and the money being wasted, and the delays involved.[52] Therefore, the WA media "work around" the legislation by filming only in public places, not investigating stories where footage is thought to be unobtainable, or leaving out critical aspects of a story.[53]

5.28 The Australian Press Council noted the differences between the WA Act and the Commission's recommended scheme, with the WA applying only to "private" conversations and activity. The Council reported that local WA newspapers have considered the effect of the WA law on newspapers and journalists to be "intangible", in that it has not prevented publication of material. "The West Australian has made only one application for publication under the provisions of the Act … The court granted an order enabling publication of the transcript but also ordered that the transcripts and tapes be sent to the police".[54] Nevertheless, the Press Council is concerned about the capacity of the authorisation process to cause cost and time problems.[55]

Application and authorisation process

5.29 All the media organisations with whom the Commission consulted were opposed to the application and authorisation process recommended by the Commission in Chapter 6 of Report 98. The ABC maintained that the Commission's recommendations concerning covert authorisations are likely to be unworkable, and would "rarely, if ever, result in the media obtaining an authorisation".[56] The ABC was concerned that this would "severely curtail the media's capacity" to report on matters in a way that serves the public interest,[57] and would operate as a prior restraint on free speech and media freedom.[58] The ABC was of the view that the courts generally "have been reluctant to recognise the bona fide role of media in society in informing the public about matters of public interest".[59] The ABC suggested that the legislation should expressly provide that, when considering an application to conduct covert surveillance, a judge must take into account "the legitimate and important role played by the media in society in informing the public about matters of public interest".[60]

---

49. ABC *Submission* at 7.
50. Formerly known as Commercial Television Australia.
51. Free TV Australia *Submission* at 17.
52. Free TV Australia *Submission* at 17.
53. Free TV Australia *Submission* at 17-18.
54. Australian Press Council *Supplementary Submission* at 3.
55. Australian Press Council *Supplementary Submission* at 3.
56. ABC *Submission* at 2; SBS *Submission* at 18.
57. ABC *Submission* at 4.
58. ABC *Submission* at 6. Free TV Australia agrees: see *Submission* at 15.
59. ABC *Submission* at 6.
60. ABC *Submission* at 7.

5.30 The ABC also considered that, in making an application to conduct covert surveillance, it may prejudice aspects of its investigation, force the revelation of confidential sources, or encroach upon its editorial independence and prevent or delay the publication of material which the ABC considers to be important and in the public interest.[61] The ABC was also concerned about the time and cost of making applications to conduct surveillance.[62] SBS also considered that the authorisation process would be too time consuming, and would impinge on its ability to report in a timely manner, and in some instances prior authorisation would not be feasible. SBS contends that the media would be unlikely to risk applying for authorisation retrospectively, due to the possibility of incurring criminal sanctions.[63] Free TV was also concerned about the administrative burden that the authorisation process would have on the media, and that it would prejudice getting a "scoop" on stories.[64] Free TV stated that it is not always possible to get prior authorisation as it may not be initially clear what the surveillance footage will show up, and agreed with SBS that the risk of criminal prosecution would deter many media organisations from applying for retrospective authorisation.[65]

5.31 SBS raised some practical questions concerning the operation of the recommendations. For example, it was suggested that, in an exceptional circumstance, a story may be filmed in South Australia, the recording of which would be illegal in NSW, and SBS would need to seek the means to broadcast the story in all states except NSW.[66] SBS also queried how the "purpose" of a covert surveillance authorisation would be defined (for example, if an authorisation is sought in relation to an investigation for one particular program, could the material be used for another SBS program, or given to a member of the public).[67]

5.32 Fairfax agreed with the ABC that the recommendations concerning public interest authorisations were couched in terms "so narrow that the media will never be capable, as a matter of practical reality, of satisfying it".[68] Fairfax also expressed the view that the issuing authority should not be in a position to "take the part of publisher" in deciding the uses to which surveillance material should be put.[69] Fairfax also agreed with Privacy NSW in considering that only judicial officers should be able to make decisions concerning authorisations.[70]

---

61. ABC *Submission* at 6. SBS expresses similar views: SBS *Submission* at 18-19. See also John Fairfax Holdings *Submission* at 13.
62. The ABC states that because, in its opinion, the distinction between overt and covert surveillance is unclear, it would need to seek authorisation whenever it was in doubt, which would not be the case in reality: ABC *Submission* at 7. The Commission discusses such misunderstandings and clarifies the difference between overt and covert surveillance so far as the media are concerned in Chapter 3.
63. SBS *Submission* at 18.
64. Free TV Australia *Submission* at 15.
65. Free TV Australia *Submission* at 16.
66. SBS *Submission* at 13. The Commission notes that this would not be the case under its recommendations, since the scope of the proposed legislation would only extend to surveillance conducted in NSW.
67. See discussion at para 5.43-5.44 and 5.48.
68. John Fairfax Holdings *Submission* at 12.
69. John Fairfax Holdings *Submission* at 12.
70. John Fairfax Holdings *Submission* at 12; Privacy NSW *Submission* at 21.

5.33 Privacy NSW agreed with the Commission about the need for prior public interest authorisations, and did not consider that this would prevent legitimate public interest stories from being published.[71] Privacy NSW further considered that authorisations should only be able to be sought by news or current affairs media, licensed security operators and private investigators. Privacy NSW did not believe that the media themselves are in a position to define the balance between the "public interest" in a story, and the public interest in the protection of privacy, as evidenced by examples of covert surveillance conducted inappropriately by the media in the past.[72]

Accountability measures

5.34 Fairfax considered that the administrative requirements contained in Recommendations 67-80 are too onerous for the media, and objected strenuously to those recommendations on the basis of the inherent threat to free speech, and the increased financial burden the authorisation and reporting mechanisms would place on the public purse.[73] Fairfax also considered Recommendations 81-87 (re publication of surveillance material) to be "unacceptable" and flawed with regard to the media, and would prevent them from using material obtained in ways which could "in no way be said to amount to surveillance in any normal sense of that term".[74] Fairfax was particularly concerned that material must be reported to the AG.[75]

5.35 The ABC also held the view that the requirement of maintaining records on the use of surveillance equipment, and the restriction on use of material for purposes other than authorised ones, was unduly onerous and unworkable. Further, the ABC asserts that the requirement to destroy material is inconsistent with its statutory obligations under the *Archives Act 1983* (Cth).[76] The Australian Press Council and News Limited agreed.[77]

Complaints process and sanctions

5.36 Fairfax opposed any application of criminal sanctions to the media, as well as the recommended civil action for damages,[78] saying it "can confidently be predicted to give rise to a wave of litigation, which does not focus on anything like surveillance, properly so called, but in truth will amount to speculative actions for breach of privacy".[79] Also, Fairfax indicated that it would "vigorously oppose" the introduction of orders for apology or retraction, claiming that such a thing is "unprecedented".[80] The Australian Press Council also objected to the role of the Privacy Commissioner in hearing and determining complaints, as recommended by the Commission.[81]

---

71. The submission notes that 10% of complaints received by Privacy NSW in 2000-2001 related to media organisations: Privacy NSW *Submission* at 20.
72. Privacy NSW *Submission* at 21.
73. John Fairfax Holdings *Submission* at 13-14.
74. John Fairfax Holdings *Submission* at 14.
75. John Fairfax Holdings *Submission* at 13.
76. ABC *Submission* at 2 and 7.
77. Australian Press Council *Preliminary Submission* at 4, News Limited *Submission* at 2.
78. Report 98, Recommendation 112.
79. John Fairfax Holdings *Submission* at 16-17.
80. John Fairfax Holdings *Submission* at 17.
81. Australian Press Council *Preliminary Submission* at 4-5.

The Commission's view

5.37 In the Commission's view, the media organisations consulted object to the recommendations on the basis of the following broad categories:

1. The belief that free speech will be impeded.

2. The concern that the cost and administrative burden may be too onerous.

3. Strenuous opposition to any system of regulation that is not self-regulatory.

Arguments concerning free speech

5.38 The Commission discussed the issues concerning privacy, free speech and surveillance in Chapter 3, noting that the privacy-focused approach favoured in Report 98 is not all-encompassing, but must be seen in its proper context.[82] Regarding surveillance conducted by the media, the Commission continues to endorse the following comments made in Report 98:

> *Freedom of speech is a matter of fundamental importance, and the media have a significant role in upholding that freedom and presenting the public with information. This Report makes recommendations which, if implemented, will regulate the use of surveillance devices and the information obtained as a result. Restrictions placed on information gathering by covert means do not automatically amount to limitations on the freedom of the press or of free speech. The proposed legislation recommended by the Commission is not aimed at restricting freedom of speech in terms of what the media prints or broadcasts. It will merely ensure that, in upholding that freedom, the media respect other equally important public interests. In this way, the proposed legislation would be no more restrictive of freedom of speech than the current LDA, the criminal law, or the laws of trespass, defamation and contempt. Even if freedom of speech were an issue in this context, it is not an absolute freedom, and must sit with other fundamental interests.*[83]

5.39 The Commission rejects the media's claim that the recommendations would "rarely, if ever" result in an authorisation being granted to a media organisation. Where a legitimate public interest is at stake, it is difficult to see why an authorisation would not be granted. What also needs to be recognised is that the concept of public interest goes beyond freedom of speech, as does the media's responsibilities. In addition to presenting the public with information, the media also play an important role in helping to ensure the public interest in the protection of personal privacy is upheld by not making unwarranted intrusions into privacy in the name of freedom of speech. It should also be kept in mind that, while covert surveillance may *sometimes* be justified to further the public interest, it will undoubtedly *always* represent a significant invasion of privacy.

Cost and administrative burdens

5.40 As noted in Chapter 3, not all activity conducted by the media will amount to surveillance. Only that activity that falls within the definition of surveillance recommended by the Commission

82. See para 3.22-3.30.
83. Report 98 at para 2.58.

would be caught by the provisions of the proposed legislation. As also noted in Chapter 3, for surveillance by the media to be classified as covert, there must be a deliberate intention to hide the fact from the person under surveillance that he or she is being filmed. Media organisations themselves have acknowledged that covert surveillance is conducted rarely and as a matter of last resort, so the cost and administrative burden on the media should not be that acute.

5.41 The reporting and accountability requirements set out in Report 98, applicable to all those, including the media, conducting covert surveillance, consist of:

- providing information based on affidavit to the issuing authority, specifying things such as the circumstances in which the device is to be used, the name of any person who is to be the subject of surveillance and who is to conduct the surveillance, the public interest(s) at stake, and the intended uses of the material obtained as a result;[84]
- reporting back the particulars of the surveillance to the issuing authority and to the Attorney General after the surveillance has been conducted;[85]
- keeping records concerning the covert surveillance conducted and allowing a designated inspecting authority (either the Privacy Commissioner or the Ombudsman) to inspect those records if required;[86] and
- restrictions on the publication or communication of the material obtained as a result of the covert surveillance, subject to the purposes allowed under the terms of the public interest authorisation.[87]

5.42 While these requirements may seem onerous at first, in reality they amount only to organising and keeping information (and providing copies to two agencies) concerning the type of surveillance conducted, who is conducting it and who is the subject of it, the public interests at stake, and the duration of the filming and the ultimate use of the material. This information should not be difficult to gather or collate, and it would indeed be surprising if media organisations did not already keep such information in relation to the footage they film. Further, these requirements apply only to covert surveillance, to reflect the need for higher standards of accountability, and so would only need to be followed rarely by media organisations.

5.43 The Commission rejects the contention by media organisations that the Commission's recommendations would result in preventing legally filmed material from being broadcast. Recommendation 82 provides that a public interest or employment authorisation must specify the purposes for which the information obtained as a result of covert surveillance may be used and the circumstances in which it may be published or communicated. So far as the media are concerned, the Commission envisages that the authorisation would simply state that any material legally obtained as a result of the covert surveillance being authorised may be published or broadcast at the discretion of the media organisation. The intention of Recommendation 82 was not to empower the issuing authority to specify the particular programs on which the material may be broadcast.

84. Recommendation 53.
85. Recommendations 68-71.
86. Recommendations 72-78.
87. Recommendations 81-82.

5.44 However, the Commission does consider that Recommendation 81 needs to be amended to clarify that the general prohibition on publication or communication of covert surveillance material may be overridden by the terms of a public interest authorisation. The Commission also agrees with the views expressed in submissions that the recommendation concerning destruction of material should be brought into line with the *Archives Act 1983* (Cth).[88]

An independent arbiter of public interest

5.45 The Commission is of the view that much of the criticism of its recommendations from media organisations is based on the fact that the proposed regulatory scheme involves an independent arbiter of the public interest: that is, unlike the current system under which the media operate, it is not self-regulatory. In submissions, the media argued that they are in the best position to determine what constitutes the public interest, and consider it inappropriate for any other body to exercise this authority. As the Commission discussed in Report 98 and in Chapter 3 of this Report,[89] the concept of public interest is multifarious and extends beyond the realm of the media. Further, while the media are uniquely charged with the responsibility of upholding and furthering the public interest through the material they publish and broadcast, there are many significant reasons why the media are not best placed to determine where the public interest lies in all cases, particularly where individual privacy concerns are at odds with ratings and circulation figures.

Conclusion

5.46 On the whole, the Commission is of the view that the system of prior and retrospective authorisation for covert surveillance in the public interest should remain, and should continue to apply to the media. As the discussion in Chapter 3 shows, covert surveillance by media organisations will only occur where there is a deliberate attempt to hide the fact of the filming from the subject. The comments from media organisations themselves indicate that this type of surveillance is not done regularly.

5.47 However, in light of the views raised in submissions, the Commission agrees that some amendments to the recommendations concerning covert surveillance in the public interest do need to be made. First, in recognition of the fact that all relevant factors need to be considered when determining whether or not to grant an authorisation, Recommendation 54 should be amended to require the issuing authority to have due regard to the role of the media in upholding the public interest. Clearly this dot point would only be relevant where a media organisation is seeking an authorisation.

5.48 Secondly, Recommendation 82 (public interest or employment authorisations to specify the purpose for which information may be used or published) should be amended to clarify that, where the applicant for such an authorisation is a media organisation, the authorisation should specify that the material may be broadcast or published at the discretion of the media organisation provided that it has been lawfully obtained within the terms of that authorisation. Following from this, Recommendation 81, which deals with the circumstances in which covert surveillance material may be published or communicated, should also be amended to clarify that material obtained as a result of a public interest authorisation may be released in accordance with the terms of that authorisation.

---

88. See para 5.49.
89. See, eg, Report 98 para 2.56-2.61, and para 6.12-6.15, and para 3.22-3.26 of this Report.

5.49 Finally, the Commission accepts that the media should be specifically exempted from the requirement to destroy surveillance material in Recommendation 87, so as to accord with the provisions of the *Archives Act 1983* (Cth).

Recommendation 3

Recommendation 54 should be amended to require the issuing authority to have due regard to the role of the media in upholding the public interest. The revised recommendation would read as follows:

In determining whether to grant an authorisation to conduct covert surveillance in the public interest, the issuing authority should have regard to:

- the nature of the issue in respect of which the authorisation is sought;
- the public interest (or interests) arising from the circumstances;
- the extent to which the privacy of any person is likely to be affected;
- whether measures other than covert surveillance have been used or may be more effective;
- the intended use of any information obtained as a result;
- the role played by the media in upholding the public interest; and
- whether the public interest (or interests) involved justifies the displacement of individual privacy in the circumstances.

Recommendation 4

The Commission recommends that an additional dot point should be added to Recommendation 81, clarifying that material obtained lawfully in accordance with the terms of a covert surveillance authorisation may be communicated, published or broadcast in accordance with that authorisation (See Recommendation 5 below).

Recommendation 5

The Commission recommends that Recommendation 82 should be amended to clarify that, where the applicant for a public interest authorisation is a media organisation, the authorisation should specify that the material may be broadcast or published at the discretion of the media organisation provided that it has been lawfully obtained within the terms of that authorisation.

Recommendation 6

The Commission recommends that the media should be exempted from the requirements to destroy material obtained as a result of covert surveillance set out in Recommendation 87.

Impact on the insurance and private investigation industry

Industry representative bodies

5.50 The detection of insurance fraud arguably represents the most significant use of covert surveillance by private investigators. Submissions were received from two organisations representing the insurance industry: the Insurance Council of Australia ("ICA") and the Investment and Financial Services Association Limited ("IFSA").

5.51 Overall, both the ICA and IFSA recognised the need for surveillance to be regulated, and acknowledged the validity of privacy concerns while conducting surveillance in the public interest.[90] However, both organisations were concerned that the recommended system of

90. Insurance Council of Australia *Submission* at 2; Investment and Financial Services Association Limited *Submission* at 1-2.

authorisation for covert surveillance may impact adversely on insurers, consumers and the government.[91] In particular, IFSA was of the view that some of the Commission's recommendations, if implemented, could "severely impact on the ability of life insurance companies to properly assess and manage insurance claims".[92] IFSA considered the proposed system of prior authorisation before covert surveillance could be carried out to investigate insurance fraud unduly onerous and inefficient, and that it could lead to delays in collecting vital evidence.[93] The ICA argued that the recommendations could result in increased premiums and delays, even to the point of causing insurers to forgo investigations, resulting in a reduction in the detection of exaggerated or fraudulent claims.[94] Accordingly, ICA sought an exemption for the general insurance industry.[95]

5.52 In terms of specific recommendations, the ICA noted that the recommended 30 day period for which an authorisation may be in force may be insufficient, given that investigations of personal injury claims may involve several separate surveillance exercises over a period of time.[96] Also, the ICA queried whether the investigator, lawyer or insurer should apply for the authorisation, and that "public interest" should be more clearly explained.[97]

5.53 So far as the authorisation process is concerned, the ICA envisaged a number of problems associated with feasibility, accessibility and practicality. It suggested that agencies other than a court or a tribunal could be empowered to issue authorisations, such as Justices of the Peace, the Motor Accidents Authority or WorkCover, or perhaps a compliance officer within an insurance company, so that authorisations could be done quickly, particularly in country areas.[98] The ICA also considered there to be a distinction between surveillance conducted by law enforcement officers who should get a warrant to enter premises and surveillance conducted by investigators in "public" places.[99] IFSA agreed that surveillance in "public" areas should not be regulated.[100]

5.54 The ICA considered the requirement contained in Recommendation 55 (naming all those using surveillance devices on the authorisation) to be impractical as insurers generally brief firms of investigators not individual agents.[101] The ICA also queried whether there is a right to appeal if

91. Insurance Council of Australia *Submission* at 3; Investment and Financial Services Association Limited *Submission* at 3.
92. Investment and Financial Services Association Limited *Submission* at 1-2.
93. Investment and Financial Services Association Limited *Submission* at 3.
94. Insurance Council of Australia *Submission* at 3. The ICA had the expense of obtaining a warrant costed by two major insurers at $3865 and $7490: Insurance Council of Australia *Submission* at Appendix 1.
95. Insurance Council of Australia *Submission* at 16.
96. Insurance Council of Australia *Submission* at 6.
97. Insurance Council of Australia *Submission* at 6-7. See para 5.17-5.23 for a discussion of the definition of public interest.
98. Insurance Council of Australia *Submission* at 7.
99. Insurance Council of Australia *Submission* at 7.
100. Investment and Financial Services Association Limited *Submission* at 4. See Report 98 at para 2.20-2.27, and para 3.11 of this Report, for a discussion of the Commission's views on the public/private distinction.
101. Insurance Council of Australia *Submission* at 9.

an authorisation is refused,[102] and in relation to the liability of employers acting in good faith if their employees breach an authorisation.[103]

5.55 While the ICA agreed with the general concept of having accountability mechanisms, it expressed concern about the administrative and reporting requirements being too onerous on insurers.[104] Regarding Recommendation 87 and the destruction of information, the ICA noted that an insurance company may want to retain information in certain situations, for example, in relation to a re-occurring injury, prior claims or the aggravation of a pre existing injury.[105] The ICA and IFSA also sought clarification regarding the possible conflict between the Commission's recommendations and the obligations on insurers deriving from the *Privacy Amendment (Private Sector) Act 2000* (Cth), since conducting surveillance also necessarily involves collecting personal information.[106] Further information was also sought by the ICA on the type of penalties that would apply to the various offences recommended by the Commission.[107]

Submissions from investigation agents

5.56 The Commission received a number of submissions from individuals and agencies involved in the investigations industry.[108] They were eager to reinforce the importance of surveillance in the investigative process as a useful community tool, particularly in relation to the detection of fraud.[109] It was estimated that two or three out of every one hundred insurance claims may come under suspicion.[110] Most questioned the need for legislative regulation, being of the view that surveillance activity was already sufficiently regulated by insurers' Codes of Conduct.[111] It was also suggested that existing legislation such as the Commonwealth Privacy Act has focused the attention of insurers and investigators on the need to be mindful of the privacy rights of claimants.[112]

5.57 Nearly all of the private investigators who made submissions to the Commission were of the view that there should be no legislation to govern the taking of video footage in a public place.[113] In disagreeing with the recommendation to obtain an authorisation, one firm of investigators claimed that there was a difference between police operations and the investigation

102. Insurance Council of Australia *Submission* at 9.
103. Insurance Council of Australia *Submission* at 10.
104. Insurance Council of Australia *Submission* at 11-13.
105. Insurance Council of Australia *Submission* at 15.
106. Insurance Council of Australia *Submission* at 10; Investment and Financial Services Association Limited *Submission* at 3.
107. Insurance Council of Australia *Submission* at 14-15.
108. Gary Cox Investigations Pty Ltd *Submission*; Rumore and Associates *Submission*;
109. Rumore and Associates *Submission*. That submission also referred to the efficacy of surveillance in intellectual property, family law, employee misconduct and criminal law: see 3-4. See also Chris Jones *Submission*; and Peter A Cox and Associates *Submission*; Gary Cox Investigations Pty Ltd *Submission* at 3.
110. Peter A Cox and Associates Pty Limited *Submission* at 4.
111. See, eg, Gary Cox Investigations Pty Ltd *Submission*; and Chris Jones *Submission*; Rumore and Associates *Submission* at 5.
112. Peter A Cox and Associates Pty Limited *Submission* at 14.
113. Peter A Cox and Associates Pty Limited *Submission* at 4.

of an insurance claim.[114] It was acknowledged that, while there are unscrupulous and unlicensed operatives, the way to deal with this problem should be to tighten the *Commercial Agents and Private Inquiry Agents Act 1963* (NSW), and not introduce surveillance legislation.[115]

5.58 Reference was made in submissions to some practical difficulties with the Commission's recommendations. For example, since covert surveillance is an everyday activity for private investigators, they would be required to make a large number of warrant applications under the proposed recommendations.[116] It was also pointed out that difficulties with the authorisation process may arise regarding investigations that last for a number of years since instructions may be given to conduct surveillance on the same claimant on a number of occasions.[117] There was also concern that the requirement to report back to the issuing authority is unworkable and unnecessarily bureaucratic.[118] Some were also of the view that the current investigative arrangements were only successful because of open communication between insurers and investigators, which could be jeopardised under the Commission's recommendations.[119]

5.59 It was also suggested that an appropriate "issuing authority" would be a senior claims officer or manager within an insurer, assisted by guidelines from the Privacy Commissioner, since judges or tribunal members may not "fully appreciate the intricacies of an insurance policy".[120] Also, the requirement to destroy surveillance material after a certain period of time was considered to be unworkable in relation to insurance, since a claimant may make further claims in relation to the same alleged injury.[121] However, there was some agreement that records should be kept by insurers, and be able to be accessed by either the Privacy Commissioner or the Ombudsman.[122] One investigator strongly disagreed with the requirement to inform the subject that surveillance has occurred.[123] The role of the Attorney General in the reporting mechanism was also questioned.[124]

5.60 Concern was expressed that the Commission's recommendations would have the effect of increasing the difficulty and cost of investigating fraudulent claims, which could prompt many insurers not to pursue allegations of fraud, resulting in increased premiums.[125] Accordingly, a number of investigators sought an exemption from the covert surveillance requirements when

---

114. Peter A Cox and Associates Pty Limited *Submission* at 13.
115. Peter A Cox and Associates Pty Limited *Submission* at 7. The Commission notes the passage of the *Commercial Agents and Private Inquiry Agents Act 2004* (NSW): see para 5.64 below.
116. Rumore and Associates *Submission* at 2.
117. Rumore and Associates *Submission* at 2. See also Peter A Cox and Associates Pty Limited *Submission* at 11.
118. Rumore and Associates *Submission* at 2; Peter A Cox and Associates Pty Limited *Submission* at 17.
119. Rumore and Associates *Submission* at 2.
120. Peter A Cox and Associates Pty Limited *Submission* at 12.
121. Peter A Cox and Associates Pty Limited *Submission* at 18.
122. Peter A Cox and Associates Pty Limited *Submission* at 19.
123. Peter A Cox and Associates Pty Limited *Submission* at 19.
124. Peter A Cox and Associates Pty Limited *Submission* at 20.
125. Gary Cox Investigations Pty Ltd *Submission* at 4; Peter A Cox and Associates Pty Limited *Submission* at 3.

acting for the insurance industry.[126] It is claimed that fully licensed private investigators should be able to run their business, including conducting covert surveillance,[127] "unimpeded by over-regulation".[128]

5.61 It was suggested to the Commission that the ICA and the Insurance Enquiries and Complaints body (a watchdog body to whom members of the public may report any complaint concerning insurance claims or procedures), could arrange a regulatory framework to ensure appropriate accountability within the insurance industry, and to allow independent access to records by the Privacy Commissioner and the Ombudsman.[129]

The Commission's views

5.62 The Commission acknowledges the arguments put forward by investigators and insurers concerning the potential impact of its recommendations, especially in relation to the insurance industry. Covert surveillance, particularly video surveillance, is a crucial element of the everyday work of a private investigator. This differentiates them from the media, because, while media organisations do conduct video surveillance, they do not conduct activity that would be classified as covert surveillance on a regular basis. While law enforcement agencies would also be affected by the Commission's recommendations, it is fair to say that the majority of surveillance work undertaken by police and other like agencies involves the use of covert listening devices, either alone or in conjunction with video and/or tracking devices. As a result, those agencies are already bound by the accountability requirements prescribed under the LDA.[130] Although the LDA applies generally and not just in relation to law enforcement agencies, there has never been a record of its use by a private investigator, presumably because they operate outside the realm of the Act by using video surveillance without activating the listening device component.

5.63 Consequently, while the policy issues regarding covert surveillance in the public interest are basically the same for all applicants, the impact on private investigators in practical terms will be more significant than on other groups or individuals. The impact on the insurance industry, and the consequent effect on policy-holders, is a matter of concern. At the same time, however, the need remains to ensure that covert surveillance is conducted responsibly and accountably. Material obtained through covert surveillance by private investigators has the potential to affect people adversely and severely, and could result not only in loss of financial benefits, but termination of employment or the laying of criminal charges.

5.64 The Commission has considered a number of options designed to overcome the difficulties raised in submissions, yet still promote accountability for covert surveillance. It was suggested in submissions that it would be preferable to tie accountability for covert surveillance conducted by private investigators together with their licensing arrangements. This idea was

126. Gary Cox Investigations Pty Ltd *Submission* at 6; Peter A Cox and Associates Pty Limited *Submission* at 8.
127. Chris Jones *Submission*.
128. Rumore and Associates *Submission* at 5.
129. Peter A Cox and Associates Pty Limited *Submission* at 26.
130. Consequently, the authorisation and accountability procedures recommended by the Commission would only create an additional impact on law enforcement agencies where surveillance was being conducted without a listening device component, eg, email surveillance or the use of video or tracking devices in isolation.

considered by the Commission in the Interim Report, but rejected due to the inadequacy of the licensing arrangements at that time. However, new arrangements are about to come into operation. At the end of September 2004, a new *Commercial Agents and Private Inquiry Agents Act 2004* (NSW) was passed, replacing the old 1963 Act.[131] One of the objects of that Act is to protect the public in relation to commercial agent and private inquiry agent activities (that is, process serving, debt collection, repossession of goods, surveillance of persons and investigation of persons).[132]

5.65 One possibility considered by the Commission is that, as licensed private investigators would be required to satisfy surveillance competency criteria annually under the new arrangements when applying for the granting or renewal of a licence, the requirement to obtain an authorisation every time a private investigator needs to conduct covert surveillance could be waived. This would be subject to the licensing system being appropriately supervised and accountable, and provision for an investigator's licence to be suspended or revoked in the event of evidence of the misuse of covert surveillance powers. Under this option, private investigators would still be required to meet the general accountability provisions recommended by the Commission, such as the keeping of records and submitting annual documents to the Attorney General, as well as the authority responsible for issuing authorisations to conduct covert surveillance in the public interest.

5.66 However, there a number of problems associated with this option. First, it is unclear how the details of the new system will operate, and the Commission is concerned that the training and accreditation procedures regarding covert surveillance may not be satisfactory to assure the appropriate level of privacy protection. Further, the area of insurance fraud investigation was overwhelmingly referred to by private investigators as the only practice area in which the Commission's recommendations would be likely to have a major impact, due to the cost of obtaining a large number of applications and the subsequent effect on insurance premiums. However, it would be administratively cumbersome to waive the requirement for a private investigator to obtain an authorisation only in relation to insurance-related covert surveillance, and require an authorisation for all other types of covert surveillance conducted by investigators. Accordingly, such a scheme would need to operate broadly in relation to every private investigator conducting any covert surveillance in the public interest. The Commission is of the view that exempting private investigators from obtaining an authorisation in relation to all of their covert surveillance work would run counter to the public interest in ascertaining adequate protection of individual privacy, and would also be inconsistent with the tenor of the Commission's recommendations as a whole.

5.67 It would also sit uneasily with the existing and proposed requirements in relation to workplace surveillance. The *Workplace Video Surveillance Act 1998* (NSW) requires employers to obtain a prior authorisation before every instance of covert surveillance in the workplace may be conducted. The Commission made similar recommendations in Report 98 concerning prior authorisations for workplace surveillance. Even if the Commission were persuaded that

131. Note that this Act had not yet commenced operation at the time this Report was finalised.
132. Under the Act, licenses for the 3,000 agents and sub-agents in NSW are to be issued by the Commissioner for Police, and are to be subject to the provisions of the *Licensing and Registration (Uniform Procedures) Act 2002* (NSW): New South Wales, *Parliamentary Debates (Hansard)* Legislative Assembly (3 June 2004) at 9636.

satisfactorily licensed private investigators should be exempted from the requirement to obtain prior authorisation before every instance of covert surveillance, the Commission would continue to endorse its recommendations in Report 98 concerning the need to obtain authorisations for covert surveillance in the workplace, due to the particular rights and responsibilities of employers and employees. Since many private investigators carry out workplace surveillance, they would, therefore, be subject to two separate regimes depending on whether the covert surveillance was conducted in an employment context or in the public interest.

5.68 The Commission is of the view that the preferable option is to grant insurers, rather than the investigators themselves, a 12 month authorisation to conduct covert surveillance. Insurers could then contract surveillance work out to private investigators, in the same way as they do currently. This would be dependent on the insurers having a demonstrated policy or Code of Practice concerning the conduct of covert surveillance, including provisions relating to privacy protection and a restriction on contracting work out only to reputable, suitably licensed investigators. The Commission recommends that both insurers and private investigators should be required to conform with the accountability requirements set out in Report 98, such as record keeping and reporting, document inspection and restrictions on the use of the material obtained as a result of covert surveillance. Renewal of the authorisation at the completion of the 12 month period would be contingent upon the accountability requirements having been met.

5.69 This option has the advantage of applying only to insurance-related covert investigations, and provides greater certainty for individual investigators as to when they need to obtain an authorisation: when they are contracted by an insurer, there is no need to obtain an authorisation, but in all other circumstances a prior authorisation will be necessary.

Recommendation 7

The Commission recommends that insurers be granted a 12 month authorisation to conduct covert surveillance. That authorisation should be contingent on insurers having a demonstrated policy or Code of Practice concerning the conduct of covert surveillance, including provisions relating to privacy protection, and a restriction on contracting work out only to reputable, suitably licensed investigators.

The Commission further recommends that insurers and private investigators should be required to comply with the recommendations in Report 98 concerning record keeping, inspection and reporting, and restrictions on the use of material obtained as a result of the use of covert surveillance. The renewal of the 12 month authorisation should be dependent on compliance with those accountability procedures.

COVERT SURVEILLANCE IN EMPLOYMENT

Recommendations in Report 98

5.70 The Commission's approach in Report 98 was that the general recommendations made in relation to overt and covert surveillance should also apply to surveillance in the workplace, except where the particular rights and responsibilities of employers and employees justified the application of special provisions. Recommendations 57 to 66 in Report 98 deal specifically with covert surveillance in an employment context. Those recommendations accord for the most part

with the two other arms of covert surveillance discussed above, and with the authorisation and accountability procedures in the *Workplace Video Surveillance Act 1998* (NSW).

5.71 In particular, the Commission recommended that an employer is only entitled to obtain a covert surveillance authorisation if:

(a) unlawful activity on work premises is reasonably suspected;

(b) employment-related unlawful activity is reasonably suspected; or

(c) serious misconduct justifying summary dismissal is reasonably suspected.[133]

5.72 Further, the Commission recommended that there should continue to be an express prohibition on the use of covert surveillance by employers for the purpose of monitoring employee performance,[134] and that covert surveillance of employees by employers in toilets, showers and change rooms should be prohibited.[135]

5.73 In the course of writing Report 98, the Commission consulted with, and received submissions from, employers and their representative organisations, as well as union groups. In making its recommendations in the Interim Report, the Commission was cognisant of the need to provide effective privacy protection for employees, yet also devise a regime flexible enough to allow employers to pursue legitimate business interests.[136] The only negative comment received in submissions concerning covert surveillance in employment was from News Limited. They were of the view that the recommendations should not apply to the workplace, as the requirements would impinge on "normal business practice and performance management activities".[137]

The Workplace Surveillance Amendment Bill

5.74 The *Workplace Surveillance Amendment Bill 2004* (NSW) ("the Workplace Surveillance Bill") was released for public comment in June 2004. The Workplace Surveillance Bill extends the coverage of the *Workplace Video Surveillance Act 1998* (NSW) to include additional forms of surveillance such as email and internet monitoring and the use of tracking devices.

5.75 The Workplace Surveillance Bill follows the form of the existing Act, prohibiting covert surveillance in the workplace unless employees have been previously notified,[138] or an

133. Recommendation 58.
134. Recommendation 59.
135. Recommendation 60.
136. The uses of surveillance in the workplace, and the competing interests and objections arising from that use, are discussed at para 7.1-7.14 of Report 98. For a further discussion, see Victorian Law Reform Commission, *Workplace Privacy: Options Paper* (2004).
137. News Limited *Submission* at 1.
138. The notice requirements are set out in cl 5 of the *Workplace Surveillance Bill 2004* (NSW). In addition to the requirements in the *Workplace Video Surveillance Act 1998* (NSW), the Bill provides that tracking surveillance will be deemed to be notified if a notice is placed in a clearly visible manner on the vehicle or other thing in which the device is located. Further,

authorisation from a magistrate is obtained for the purpose of establishing whether or not an employee is engaged in unlawful activity at work.[139] Work is defined to mean at a workplace, or any other place where an employee is working (and so covers employees working from home).[140] The Bill also contains a new provision prohibiting employers from blocking an employee's Internet access, or emails sent to or from an employee, unless the employer is acting in accordance with a publicised policy relating to Internet or email use, and the employee is immediately notified that the email has been has blocked. The Bill further prohibits an employer's Internet or email policy from blocking emails or Internet access merely because the content relates to industrial matters.[141] Like the *Workplace Video Surveillance Act 1998* (NSW), the Workplace Surveillance Bill contains measures aimed at promoting the accountability of employers conducting covert surveillance, including restrictions on the use and disclosure of material obtained as a result of covert surveillance.[142]

The Commission's views

5.76 While the Workplace Surveillance Bill differs in a number of respects from the Commission's recommendations, the overall framework of the legislation largely follows the same pattern as that recommended in Report 98. The Bill is based on an overt/covert distinction, and relies on a system of prior judicial authorisation before covert surveillance may occur. The Bill also contains reporting and record keeping provisions designed to promote accountability, backed up by offences and penalties. Also in keeping with the Commission's recommendations, the Workplace Surveillance Bill prohibits covert surveillance of employees' change rooms or shower or toilet facilities.[143]

5.77 There are also several differences between the Workplace Surveillance Bill and the approach taken by the Commission in Report 98. For example:

- The Bill regulates only workplace surveillance, while the Commission advocated that surveillance in the context of employment should be addressed as part of its general recommended framework, with the creation of employment specific provisions where necessary.[144]

---

computer surveillance will be considered to be notified if the employee is given prior notice of the nature of the surveillance, either by means of a written notice on or near the computer, or an audible announcement or written notice that appears when the employee logs onto the computer or starts a program that is the subject of the surveillance.

139. *Workplace Surveillance Bill 2004* (NSW) cl 13.
140. *Workplace Surveillance Bill 2004* (NSW) cl 4.
141. *Workplace Surveillance Bill 2004* (NSW) cl 11.
142. For a detailed discussion of the provisions of the Workplace Surveillance Bill, see L Roth, *Workplace Surveillance*, NSW Parliamentary Library Research Service (Briefing Paper No 13/04, October 2004).
143. *Workplace Surveillance Bill 2004* (NSW) cl 9; and Report 98 Recommendation 60.
144. Report 98 Recommendation 57.

- The Bill regulates only covert surveillance,[145] whereas the Commission recommends that overt surveillance should also be regulated.

- The Bill is device specific, in contrast with the Commission's broader approach.

- The Bill permits covert surveillance only for the purpose of establishing whether or not an employee has engaged in unlawful activity, whereas the Commission recommends that covert surveillance may also be permitted under an authorisation where serious misconduct justifying summary dismissal is reasonably suspected.[146]

- The Bill proposes to regulate the *blocking* of email and internet websites, which is an area not directly referred to by the Commission.[147]

- The Bill provides for an authorisation to be issued by a Magistrate, whereas the Commission recommends that Industrial Magistrates or Judicial Members of the Industrial Relations Commission be responsible for issuing authorisations.[148]

- The Commission recommends that retrospective authorisations should be available to permit covert surveillance in exceptional circumstances (for example, where the health or welfare of other employees is at risk and there is not time to obtain prior authorisation),[149] while the Bill does not make provision for this.

- The accountability and offence provisions recommended by the Commission are more stringent than those in the draft Bill.

- The Commission recommends that breaches of the overt and covert surveillance provisions should give rise to liability for a civil action to be brought.[150]

---

145. Except insofar as cl 9 (prohibiting surveillance of an employee in a change room, toilet, shower or other bathing facility) purports to apply to notified, as well as covert, surveillance.
146. Report 98 Recommendation 58.
147. In most cases, generic blocking of access to websites, for example, due to illegal or offensive content, would not amount to surveillance within the Commission's definition since it is a blanket, gateway control placed on the technology, rather than an attempt to monitor specific employees. An analogy would be blocking employees from having STD or international dialling access on their telephones. The blocking of emails relates more directly to individual employees and is therefore more likely to constitute surveillance according to the Commission's definition. In circumstances where email and web blocking do amount to surveillance, the Commission's recommendations regarding overt and covert surveillance would apply.
148. Report 98 Recommendation 62.
149. Report 98 Recommendation 66.
150. The bringing of a civil action for both overt and covert surveillance would involve a complaints and review mechanism as set out in Recommendations 91-102. In relation to covert surveillance generally, and in the workplace, the Commission recommends that a civil action should be able to lie concurrently with a criminal prosecution: Recommendations 105 and 106.

5.78 Since most of the provisions of the Workplace Surveillance Bill are similar to those in the *Workplace Video Surveillance Act 1998* (NSW), the Commission's recommendations differ from the Bill in largely the same respect in which they differ from the original Act. As such, the Commission's rationale for its approach to the regulation of workplace surveillance is discussed in Report 98 at Chapter 7. Most of the other provisions of the Bill are either not inconsistent with the Commission's recommendations, or operate outside the scope of the Commission's recommended regulatory structure. Consequently, the Commission is of the view that there are no compelling reasons offered by the Workplace Surveillance Bill, or by the submissions or other feedback received in relation to the Interim Report, to warrant making any amendments to the recommendations regarding workplace surveillance in Report 98.

Appendix

- List of submissions

List of submissions to Interim Report 98

Australian Broadcasting Corporation (9 May 2003)

Australian Press Council (13 June 2003)

Special Broadcasting Services Corporation (May 2003)

John Fairfax Holdings (27 May 2003)

Commercial Television Australia Limited (30 April 2003)

News Limited (30 May 2003)

Privacy New South Wales (28 June 2002)

Roads and Traffic Authority (3 June 2003)

Centrelink (8 November 2002)

Mr Chris Jones (6 September 2002)

Mr GJ Fox (1 July 2002)

Minorplanet Asia Pacific Pty Limited (15 May 2002)

Insurance Council of Australia Limited (16 October 2002)

Peter A Cox and Associates Pty Limited (2 October 2002)

Rumore and Associates Pty Limited (9 October 2002)

Gary Cox Investigations Pty Limited (25 September 2002)

Investment and Financial Services Association Limited (12 September 2002)

SurfControl (downloaded from their website 3 May 2004)

Tables

- *Table of cases*
- *Table of legislation*

Table of cases

Table of legislation

Commonwealth

New South Wales

Queensland

South Australia

Tasmania

Victoria

Western Australia

Australian Capital Territory

Northern Territory

Bibliography

AUSTRALIA, SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE, *Provisions of the Telecommunications Interception Legislation Amendment Bill 2002* (May 2002)

AUSTRALIA, SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE, *Provisions of the Telecommunications (Interception) Amendment Bill 2004* (March 2004)

AUSTRALIA, SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE, *Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* (July 2004)

AUSTRALIA, SENATE SELECT COMMITTEE ON INFORMATION TECHNOLOGIES, *In the Public Interest: Monitoring Australia's Media* (Senate Printing Unit, Canberra, 2000)

AUSTRALIA, SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS, *Off the Record: Shield Laws for Journalists' Confidential Sources* (Senate Printing Unit, Canberra, 1994)

AUSTRALIAN BROADCASTING CORPORATION, Code of Practice 2004 «www.abc.net.au/corp/codeprac04.htm»

AUSTRALIAN BROADCASTING CORPORATION, Editorial Policies «abc.net.au/corp/edpol02.pdf»

AUSTRALIAN PRESS COUNCIL, *Australian Press Council News* vol 16(2) May 2004

AUSTRALIAN PRESS COUNCIL, "Statement of Principles" «www.presscouncil.org.au/pcsite/complaints/sop.html»

DOYLE C AND BAGARIC M, ""The right to privacy and corporations" (2003) 31 *Australian Business Law Review* 237

FREE TV AUSTRALIA, "Commercial Television Industry Code of Practice July 2004" «203.147.163.200/documents/Code_of_Practice_July_2004.pdf»

FREE TV AUSTRALIA, "Commercial Television Industry Annual Code Complaints Report 2002-2003" «www.ctva.com.au/documents/Annual_Code_Complaints_Report_2002-2003.pdf»

FRIDMAN GHL, "A Scandal in Tasmania: The Tort That Never Was" (2003) 22(1) *University of Tasmania Law Review* 84

GIBSON S, "Emerging law of privacy in Australia" (2003) 16(5) *Australian Intellectual Property Law Bulletin* 65

GREENLEAF G, "Privacy at common law – not quite a dead possum" (2001) 8(7) *Privacy Law and Policy Reporter* 129

HARRIS B, "Privacy and 'possum' let the debate begin" (2002) 10 *elawpractice.com.au*

HEATH WM, "Possum Processing, Picture Pilfering, Publication and Privacy: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2002) 28(1) *Monash University Law Review* 162

HENDERSON A AND MCDONOUGH A, "Call monitoring – legalities and regulation" (February 1999) 2(8) *TeleMedia* 97

HEUZENROEDER H, "Brushtail Carnage: Privacy Interests and the Common Law" (2002) 24(1) *Law Society Bulletin* (SA) 22

HORTON J, "Common law right to privacy moves closer in Australia" (2001) 8(7) *Privacy Law and Policy Reporter* 144

HORTON J, "Towards a Real Right of Privacy" (2003) 29(2) *Monash University Law Review* 401

LAW COMMISSION TE AKA MATUA O TE TURE, *Intimate Covert Filming* (Study Paper 15, June 2004)

LAW REFORM COMMISSION OF HONG KONG, *Privacy and Media Intrusion* (Report, December 2004)

LINDSAY D, "Protection of privacy under the general law following ABC v Lenah Game Meats Pty Ltd: Where to now?" (2002) 9(6) *Privacy Law and Policy Reporter* 101

LINDSAY D, "Playing possum? Privacy, freedom of speech and the media following ABC v Lenah Game Meats Pty Ltd: Part 11- The future of Australian privacy and free speech law, and implications for the media" (2002) (September) *Media and Arts Law Review* 161

MARTIN R AND MACDONNELL J, "Privacy after Lenah Game Meats" (2001) 5(7) *Telemedia* 106

MEDIA ENTERTAINMENT AND ARTS ALLIANCE, "Australian Journalists' Association Code of Ethics" «www.alliance.org.au/hot/ethicscode.htm»

MOORE DJ, *Privacy: The Press and the Law*, Palladian Law Publishing Ltd, Isle of Wight, 2003.

NSW LAW REFORM COMMISSION, *Surveillance: An Interim Report* (1998, Report 98)

RICHARDSON M, "Whither Breach of Confidence: A Right of Privacy for Australia?" (2002) 26 *Melbourne University Law Review* 381

ROTH L, *Workplace Surveillance*, NSW Parliamentary Library Research Service (Briefing Paper No 13/04, October 2004)

SPECIAL BROADCASTING SERVICE, "Codes of Practice" «sbs.com.au/media/1706Codes.pdf»

STANDING COMMITTEE OF ATTORNEYS GENERAL AND AUSTRALASIAN POLICE MINISTERS' COUNCIL JOINT WORKING GROUP ON NATIONAL INVESTIGATIVE POWERS, *Cross-Border Investigative Powers for Law Enforcement* (November 2003)

STEWART D, "Protecting Privacy, Property, and Possums: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd" (2002) 30(1) *Federal Law Review* 177

TAYLOR G AND WRIGHT D, "Australian Broadcasting Corporation v Lenah Game Meats, Privacy, Injunctions and Possums: An Analysis of the High Court's Decision" (2002) 26 *Melbourne University Law Review* 707

TRINDADE F, "Possums, privacy and the implied freedom of communication" (2002) 10 *Torts Law Journal* 119

UNITED KINGDOM PRESS COMPLAINTS COMMISSION, "Code of Practice" «www.pcc.org.uk/cop/cop.asp»

WILSON T, "Does the decision in ABC v Lenah Game Meats Pty Ltd open the door to privacy rights?" (2002) 16(5) *Australian Property Law Bulletin* 45

VICTORIAN LAW REFORM COMMISSION, *Workplace Privacy: Options Paper* (2004)

WOOD F, "Your telephone calls: recording and monitoring" (1996) 3(1) *Privacy Law and Police Reporter* 14

Index