New South Wales
Law Reform Commission

Report
98

Surveillance: an interim report

February 2001

New South Wales. Law Reform Commission.
Sydney 2001
ISSN 1030-0244 (Report)

National Library of Australia
Cataloguing-in-publication entry

New South Wales. Law Reform Commission.
Surveillance: an interim report.

Bibliography
Includes index
ISBN 0 7313 0448 9

1. Electronic surveillance – New South Wales. 2. Electronics in criminal investigation – New South Wales. 3. Privacy, Right of – New South Wales. I. Title. (Series : Report (New South Wales. Law Reform Commission) ; 98).

345.94052

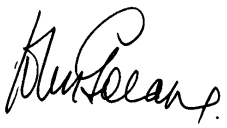
New South Wales
Law Reform Commission

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

Dear Attorney

Surveillance: an interim report

We make this interim Report pursuant to the reference to this Commission dated 2 July 1996.



His Honour Judge Jack Goldring
Commissioner-in-Charge

The Hon Justice Michael Adams

Professor Reg Graycar

Vice President Iain Ross

February 2001

Contents

Terms of reference

In a letter to the Chairperson of the New South Wales Law Reform Commission dated 2 July 1996, the Attorney General, the Hon J W Shaw QC, MLC, required the Commission to inquire into and report on the following matters:

- *the current 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 this review the Commission should have regard to:

- *the protection of the privacy of the individual;*
- *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.*

In making this reference the Attorney draws the Commission's attention to the Government's proposals for the introduction of privacy and data protection legislation and to the current review of the issue of the regulation of workplace visual surveillance being conducted by the Department of Industrial Relations.

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
*His Honour Judge Jack Goldring**
Professor Reg Graycar
Vice President Iain Ross

(denotes Commissioner-in-Charge)*

Officers of the Commission

Executive Director
Mr Peter Hennessy

Legal Research and Writing
Ms Gillian Ferguson
Ms Catherine Gray
Ms Donna Hayward
Mr Ani Luzung
Ms Judy Maynard

Research Assistance
Ms Laurie Berg
Ms Tamara Pallos
Ms Kaye Sato

Librarian
Ms Dita Kruze

Desktop Publishing
Ms Rebecca Young

Administrative Assistance
Ms Wendy Stokoe

EXECUTIVE SUMMARY

The term "surveillance" is a colourful one, often giving rise to exotic images involving hidden microphones, telephoto lenses and perhaps even elaborate spy rings. Two of the many preconceptions people may have concerning surveillance, fostered largely by action/science fiction films and novels, are that it is conducted only with expensive, highly technical equipment, and happens only to people involved in criminal or other underworld activity. Increasingly, however, what was once the realm of science fiction is becoming fact. The technological boom in recent times, coinciding with the development and growth of the internet and e-mail systems, has made surveillance equipment more affordable and available than ever before.

All of us, at some time in our lives, are affected by surveillance. Most people are familiar with day-to-day surveillance: they are subject to it in banks, at service stations, on railway platforms. These particular examples are of the unconcealed use of visual surveillance equipment, most commonly by means of a closed circuit television (CCTV) system. Surveillance today, however, can take forms which many would find surprising, and may be carried out, enhanced or recorded by a staggering array of devices, such as:

- *binoculars and telescopes;*
- *listening devices or "bugs";*
- *video cameras;*
- *audio-visual devices;*
- *computers;*
- *tracking devices;*
- *biometric identification systems, which use personal characteristics (such as retina or fingerprints, palm verification, voice and facial recognition, and signature verification) to verify identity; and*

- *various technologies (such as x-ray imaging) developed to detect concealed weapons.*[1]

Surveillance is conducted routinely by law enforcement officers, private investigators, employers, the media, and private individuals, for diverse purposes: crime prevention and detection, protection of private property, the performance of employees and investigating matters of public interest, to name but a few. Despite the range of surveillance equipment and the myriad ways in which it may be used, there is currently very little in the way of legislative regulation of surveillance: only the general covert use of listening devices,[2] *and the covert use of video surveillance in the workplace,*[3] *has received any specific legislative recognition in New South Wales.*[4] *There is no existing regulation of overt surveillance.*

While surveillance is often legitimate and beneficial, it is also open to abuse and may present a significant intrusion into personal privacy. The Commission is of the view that, in recommending a broad-based system of regulation for surveillance, personal privacy should be the paramount concern. Intrusions into it by way of surveillance may sometimes be necessary, but should be supported by clear rules and only occur when justified as being for the greater public benefit.

The recommendations in this Report would, if implemented, provide New South Wales with an extremely comprehensive system of surveillance regulation. The Commission recommends the introduction of a new Surveillance Act which, among other things, would replace the Listening Devices Act 1984 (NSW) and the Workplace Video Surveillance Act 1998 (NSW). In making its recommendations, the Commission takes the approach that, in order to be optimally effective, any new legislation designed to

---

1. *See ch 1 for more details of the nature, type, uses and origins of surveillance.*
2. *Listening Devices Act 1984 (NSW).*
3. *Workplace Video Surveillance Act 1998 (NSW).*
4. *See para 1.36-1.58 for a discussion of the current statutory and common law regulation of surveillance in New South Wales and other jurisdictions.*

govern surveillance should be as broad in scope as the nature of surveillance itself. The legislation should not be device specific to ensure that the law is not outpaced by technological developments. As a result, any device used to conduct surveillance (according to the definition recommended by the Commission) would be caught by the terms of the proposed Act. 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]

The Commission is of the view that the broad approach reflected by this definition avoids the arbitrary gaps and anomalies that characterise existing surveillance laws, and extends privacy protection to as wide a range of activity as reasonably possible. The Commission's recommended regime includes surveillance conducted overtly (ie with the knowledge of the person being monitored) or covertly. It covers surveillance regardless of where it is conducted (both public and private places are covered,[6] *as well as the workplace*[7]*), or who it is conducted by (law enforcement officers, employers, private investigators, the media, and any person conducting surveillance in the public interest are all included in the proposed legislative regime). The Commission's recommended*

---

5. *The term "monitoring" for the purpose of the Commission's recommended definition includes "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": see para 2.37-2.39.*
6. *See para 2.20-2.27 for a discussion of the public/private distinction. A private place also includes a private home: see para 2.51-2.55.*
7. *Although the Commission refrains from using the term "workplace", preferring "employment" or "employment context", as this emphasises that it is the relationship between the employer and employee that is the significant factor in determining the type of regulation that should apply, rather than the physical location of the workplace: see para 2.108-2.113 and ch 7.*

regime will also cover aspects of internet and e-mail surveillance[8] *and data surveillance.*[9]

Under the Commission's recommendations, surveillance should be considered to be overt where adequate notice is given to the subject prior to, or simultaneously with, the occurrence of the surveillance. Notice would be proven where there are clearly visible signs or other warnings, such as audio announcements etc, that are widely understood and indicate that surveillance is, or may be, occurring.[10] *Where surveillance of employees is conducted by an employer, the Commission recommends that an additional notice requirement should apply in order for the surveillance to be considered overt, due to the added rights and responsibilities inherent in the employer/employee relationship.*[11] *Surveillance conducted in circumstances that do not meet these notice requirements would be considered to be covert.*

So far as overt surveillance is concerned, the Commission recommends that this should be regulated flexibly, requiring adherence to eight legislative principles to be supplemented by codes of practice for those conducting a significant amount of overt surveillance. The principles are as follows:

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.*

---

8. *The recommendations concerning internet and e-mail surveillance are discussed at para 2.43-2.50.*
9. *The recommendations concerning data surveillance are discussed at para 2.68-2.76.*
10. *See para 2.78-2.79.*
11. *That is, that all employees must be notified in writing at least 14 days prior to the commencement of the surveillance: see para 2.80-2.82.*

5. *Surveillance users must be accountable for their surveillance devices 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 must be destroyed within a specified period.*[12]

Failure to comply with the principles would expose those conducting overt surveillance to the threat of a civil action under the proposed surveillance legislation.[13]

Since covert surveillance is conducted without the knowledge of the subject, and is thereby more intrusive than surveillance conducted overtly, it should be regulated more stringently. The Commission recommends that the approval of an independent arbiter should have to be obtained before any covert surveillance may occur under the proposed Surveillance Act. In circumstances where such prior approval is not possible or practicable, it may, where appropriate, be obtained retrospectively. The Commission has isolated three main areas where covert surveillance may legitimately be conducted. Those are law enforcement, in the course of employment, and in the public interest.[14]

- *Covert surveillance by, or on behalf of, law enforcement officers should be regulated by a warrants procedure similar to that currently operating in the Listening Devices Act 1984 (NSW), with applications made to and warrants issued by "eligible judges" in the courts system.*[15]

---

12. *See ch 4 for more details of the regulation of overt surveillance.*
13. *See ch 10.*
14. *While the Commission acknowledges that covert surveillance conducted by, or on behalf of, law enforcement officers and employers has a public interest element, the term "public interest" is used in this context to refer to covert surveillance which can be justified in any circumstance outside law enforcement and employment: see ch 6.*
15. *See ch 5.*

- *Covert surveillance by, or on behalf of, employers should be authorised by members of the Industrial Relations Commission.*[16]
- *Covert surveillance conducted in the public interest by anyone other than law enforcement officers or employers (or people acting on their behalf), must be authorised by an appropriate issuing authority, being either members of a court or a tribunal.*[17]

The proposed Surveillance Act should also specify measures to promote accountability for the conduct of covert surveillance and the use of material obtained as a result.[18] *Breach of the provisions of the proposed Surveillance Act regarding covert surveillance would give rise to a criminal offence. In addition, liability for a civil action resulting in damages or other appropriate remedies may be incurred as a result of a breach of the Act.*[19]

16. *See ch 7.*
17. *See ch 6.*
18. *See ch 8 and 9.*
19. *See ch 10.*

THE COMMISSION'S RECOMMENDATIONS

Part One: Preliminary and Definitional Issues

Chapter Two

Recommendation 1 (page 55)

The proposed Surveillance Act should define "surveillance device" to mean any instrument, apparatus or equipment used either alone, or in conjunction with other equipment, which is being used to conduct surveillance.

Recommendation 2 (page 58)

The proposed Surveillance Act should define "surveillance" 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.

Recommendation 3 (page 58)

The proposed Surveillance Act should define "monitor" (as used in the definition of surveillance) 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 4 (page 71)

The proposed Surveillance Act should exempt from its scope surveillance conducted under a Commonwealth law.

Recommendation 5 (page 72)

The proposed Surveillance Act should regulate all surveillance activity within its scope, unless other New South Wales laws specifically exempt the operation of the surveillance legislation.

Recommendation 6 (page 76)

The random or overt collection, retrieval and matching of information on computer databases should be excluded from the scope of the proposed Surveillance Act.

Recommendation 7 (page 76)

The covert use of a surveillance device to monitor data relating to particular individuals or groups, as it is entered into a technology system or stored on a database, should be regulated under the proposed Surveillance Act.

Recommendation 8 (page 78)

Data surveillance of employees conducted by employers, either overtly or covertly, should be regulated by the proposed Surveillance Act.

Recommendation 9 (page 79)

The proposed Surveillance Act should define overt surveillance to be surveillance which occurs in circumstances where adequate notice of the surveillance has been given prior to, or simultaneously with, the occurrence of the surveillance.

Recommendation 10 (page 80)

For the purpose of Recommendation 9, adequate notice is 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.**

Recommendation 11 (page 81)

Surveillance in the employment context should be considered overt if employees are provided with written notification of the intended surveillance at least 14 days (or, if the employer has obtained the consent of the employee to a lesser period of notice, that period) prior to its commencement.

In the case of new employees, where surveillance has already commenced, surveillance in the employment context would be considered overt if they are provided with written notification of the surveillance at the time when an offer of employment is made.

Recommendation 12 (page 82)

For the purposes of overt surveillance in employment, written notice should contain the following information:

(a) the location of the surveillance;

(b) the nature and capacity of the surveillance devices;

(c) whether the surveillance will be continuous and, if not, the hours of operation;

(d) the purpose of the surveillance; and

(e) the person responsible for the conduct of the surveillance.

Recommendation 13 (page 85)

Any surveillance conducted in circumstances that fail to satisfy the notice requirements for overt surveillance should be considered to be covert for the purposes of the proposed Surveillance Act.

Recommendation 14 (page 94)

The proposed Surveillance Act should not contain participant monitoring provisions with regard to covert surveillance. Covert surveillance should be permitted only when justified and authorised in particular circumstances, regardless of whether the monitoring is conducted by a party or an outsider.

Recommendation 15 (page 96)

In the proposed Surveillance Act, employment specific provisions should apply:

(a) when an employer is undertaking surveillance of an employee on work premises; or

(b) when an employer is undertaking surveillance of an employee not on work premises but for an employment-related purpose.

Recommendation 16 (page 98)

"Employer" and "employee" should be defined in the proposed Surveillance Act by reference to a contract of employment or apprenticeship, to which both are parties.

Part Two: Overt Surveillance

Chapter 4

Recommendation 17 (page 172)

The use of overt surveillance otherwise than in accordance with the proposed Surveillance Act, should be unlawful. This will entail compliance with the overt surveillance principles (see paragraph 4.38 and following).

Recommendation 18 (page 174)

In certain cases specified in the proposed Surveillance Act, surveillance will be regarded as overt, notwithstanding the absence of notification to potential surveillance subjects.

Recommendation 19 (page 178)

"Relevant surveillance users" (defined in the proposed Surveillance Act according to criteria such as the number of devices operated) should be required to formulate and act in accordance with a code of practice consistent with the overt surveillance principles. A relevant surveillance user should make its code available for perusal by any member of the public subjected to its surveillance.

Recommendation 20 (page 186)

All public sector surveillance users, as well as all "relevant surveillance users" operating within the private sector, should maintain a register containing details of the number, types and locations of all their overt surveillance devices, together with any other details from time to time required by the Privacy Commissioner. Such registers should be available for inspection by the Privacy Commissioner at any time.

Recommendation 21 (page 189)

Staff operating equipment in control rooms (or in similar circumstances) with which to conduct overt surveillance, should be licensed in accordance with the *Security Industry Act 1997* (NSW). The *Security Industry Act 1997* (NSW) should be amended to provide that "security activity" is defined as including the monitoring or operating of a surveillance device or system.

Part Three: Covert Surveillance

Chapter 5

Recommendation 22 (page 206)

Law enforcement officers should be required to obtain a warrant in order to carry out covert surveillance. The provisions of the proposed Surveillance Act regulating covert surveillance by law enforcement officers should be based on Part 4 of the *Listening Devices Act 1984* (NSW).

Recommendation 23 (page 211)

"Law enforcement officer" should be defined in the proposed Surveillance Act to include 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 and the Police Integrity Commission. It should also include any office holder specifically empowered to enforce a particular law.

Recommendation 24 (page 214)

The proposed Surveillance Act should allow an application for a warrant to be made with respect to any offence.

Recommendation 25 (page 218)

The proposed Surveillance Act should empower the Attorney General to declare Supreme Court judges as "eligible judges" for the purpose of deciding applications for surveillance warrants. The proposed Surveillance Act should also authorise the Attorney General to nominate District Court judges and Magistrates as "eligible judicial officers" who may exercise the functions of an "eligible judge".

Recommendation 26 (page 220)

In determining whether a warrant should be granted, the eligible judge should have regard to:

- **the nature of the offence in respect of which the warrant is sought;**
- **the extent to which the privacy of any person is likely to be affected;**
- **whether other investigative procedures have been tried but have failed; or other investigative procedures are unlikely to succeed or likely to be too dangerous to adopt in the particular case; or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative techniques;**
- **the evidentiary value of any evidence sought to be obtained; and**
- **any previous warrant sought or granted in connection with the same offence.**

Recommendation 27 (page 222)

"Premises" should be defined in the proposed Surveillance Act to include any object, thing or place where the eligible judge, in the exercise of his or her discretion, authorises a device to be installed.

Recommendation 28 (page 224)

The eligible judge should have the discretion to issue a warrant permitting surveillance of a particular person or thing without reference to specific premises if the applicant satisfies the eligible judge that such a warrant is justified in the particular circumstances, subject to any conditions which the eligible judge deems fit to impose.

Recommendation 29 (page 225)

The proposed Surveillance Act should contain a provision similar to section 16(3) of the LDA, expressly authorising entry by the warrant-holder onto authorised premises for the purpose of installation and retrieval of the surveillance device, notwithstanding that such entry might otherwise be unlawful.

Recommendation 30 (page 226)

An eligible judge should have the power to authorise the warrant-holder to enter upon any other premises as may be necessary for the purpose of gaining access to the premises where the surveillance device is to be installed and retrieved, notwithstanding that such entry might otherwise be unlawful.

Recommendation 31 (page 228)

An eligible judge should have the power to authorise entry to the relevant premises to enable the warrant-holder to repair, test, maintain, move and replace the surveillance device after it was installed, nothwithstanding that such entry might otherwise be unlawful.

Recommendation 32 (page 228)

If the warrant-holder exercises an authority given under the warrant to move a device to premises not specified in the warrant, the warrant-holder must report the move to the eligible judge as soon as reasonably practicable.

Recommendation 33 (page 230)

The eligible judge should have the power to authorise the warrant-holder to employ all reasonable means, not including force against a person, necessary in order to gain entry to premises where the surveillance devices are to be installed, retrieved, repaired, tested, moved, maintained or replaced, as well as other premises where the warrant-holder has been authorised to enter for those purposes, whether or not the means employed would otherwise amount to damage or trespass to property.

Recommendation 34 (page 231)

The proposed Surveillance Act should empower the eligible judge to authorise the use of electricity connected to the premises to power the surveillance device.

Recommendation 35 (page 234)

The person primarily responsible for the execution of the warrant should be named in the warrant. The eligible judge should have the power to authorise that person to seek whatever assistance is necessary to execute the warrant.

Recommendation 36 (page 235)

The proposed Surveillance Act should contain a provision similar to section 20A(1) of the LDA permitting the use of assumed names or code names in a warrant.

Recommendation 37 (page 235)

The names of all persons who were involved in executing the warrant should be provided to the eligible judge as soon as reasonably practicable after the completion of the surveillance.

Recommendation 38 (page 238)

The period for which a warrant can be in force should be 30 days. Further warrants, each for a maximum period of 30 days, should be able to be applied for in respect of the same offence upon lodgement of a new application.

Recommendation 39 (page 239)

The warrant should specify:

(a) the offence in respect of which the warrant is granted;

(b) where practicable, the name of any person who is to be the subject of surveillance;

(c) the period (being a period not exceeding 30 days) during which the warrant is in force;

(d) the name of the person primarily responsible for the execution of the warrant;

(e) the premises on which the surveillance device(s) are to be installed or used, except in cases where the eligible judge has determined that it is justified not to specify the premises;

(f) the type(s) of surveillance device(s) to be used;

(g) any conditions subject to which the premises may be entered, or the surveillance device(s) may be used pursuant to the warrant;

(h) any conditions subject to which any information obtained as a result of the surveillance may be used, released or published; and

(i) the time within which the person authorised to use the surveillance device(s) pursuant to the warrant is required to report to the eligible judge and the Attorney General.

Recommendation 40 (page 240)

Where a warrant authorises the installation of one or more surveillance devices, the eligible judge should have the power to authorise:

(a) the retrieval of the surveillance device;

(b) the repair, testing, movement, maintenance and/or replacement of the surveillance device;

(c) entry onto the premises where the surveillance device is installed, and onto other premises, for the purpose of installation, retrieval, repair, testing, movement and/or replacement of the surveillance device;

(d) the person executing the warrant to employ such means as is necessary and reasonable for the purpose of executing the warrant, not including force against a person;

(e) the warrant-holder to seek whatever assistance is necessary to execute the warrant; and

(f) the use of electricity to power the surveillance device(s).

The eligible judge should also have the power to order retrieval of a surveillance device.

Recommendation 41 (page 243)

Except where the proposed Surveillance Act allows an application to be made by telephone or radio, applications for a covert surveillance warrant should be in writing supported by an affidavit attesting to the following:

- **the name of the person or organisation requesting the warrant and the name of any person acting, or making an application, on behalf of an organisation;**
- **the names of all persons who will be involved in the execution of the warrant, or their codenames and the reasons for the use of codenames, and whether the assistance of other persons in the execution of the warrant is likely to be required;**
- **if known, the identity of the person who will be the subject of the surveillance;**
- **a general description of all surveillance devices intended to be used;**
- **where the surveillance device will be installed and used, or, if it is not possible to nominate an exact location, why this is so;**
- **the length of time (not exceeding 30 days) for which the applicant seeks that the warrant be in force;**
- **details of any previous warrants sought or granted in connection with the same offence; and**
- **evidence in support of the matters to which the legislation requires that the eligible judge, in determining the application, shall have regard.**

Recommendation 42 (page 244)

In the case of applications made by telephone or radio, the applicant should furnish the eligible judge, either orally or in writing as the eligible judge may direct, all the information which a written application is required to contain.

Recommendation 43 (page 244)

The eligible judge should have the discretion to require information in addition to that which is prescribed by the legislation, if it is deemed necessary to determining the application.

Recommendation 44 (page 246)

The proposed Surveillance Act should permit one warrant to be issued authorising the use of more than one surveillance device, or a surveillance device which has more that one kind of function, provided that the warrant specify all devices which will be used in the law enforcement operation.

Recommendation 45 (page 248)

The eligible judge should have the power to authorise or order retrieval of a device.

Recommendation 46 (page 248)

If a device is capable of continuing to transmit information after the expiry of the warrant, then the warrant-holder must obtain permission from the eligible judge not to retrieve it.

Recommendation 47 (page 249)

The proposed Surveillance Act should contain a provision similar to section 18 of the LDA, but should include complaint by facsimile or other electronic means as methods by which an application for a warrant can be made under the proposed section.

Recommendation 48 (page 250)

The proposed Surveillance Act should enable warrants to be applied for within 24 hours of the surveillance taking place and issued retrospectively to law enforcement officers where:

- **evidence of an offence is obtained by covert surveillance incidentally during the investigation, pursuant to a warrant, of another offence; or**
- **it was not possible or practicable to obtain a warrant before conducting or continuing covert surveillance of an offence without prejudicing the investigation or endangering the officers or other parties involved.**

Chapter 6

Recommendation 49 (page 263)

The proposed Surveillance Act should permit covert surveillance to be conducted in the public interest only when it is judged to be justified by an appropriate issuing authority. The proposed Surveillance Act should provide that anyone, apart from:

- **an employer in the course of an employment relationship;**
- **a law enforcement officer in the course of his or her duty; or**
- **anyone acting on behalf of an employer or a law enforcement officer in the above circumstances,**

may apply for authorisation to conduct covert surveillance in the public interest. This should include journalists, media organisations, private investigators and any other person.

Recommendation 50 (page 263)

The term "public interest" should be interpreted broadly by the issuing authority, and may include private rights and interests where appropriate.

Recommendation 51 (page 264)

The Privacy Commissioner should develop guidelines to assist the issuing authority to determine the types of circumstances which may give rise to significant public interest concerns (see paragraph 6.11).

Recommendation 52 (page 271)

The appropriate authority for issuing authorisations to conduct covert surveillance in the public interest should be either "eligible judges" or members of a tribunal such as the Administrative Decisions Tribunal. Regardless of which forum is considered to be most appropriate, the authorisation process should be accessible, affordable, expeditious and impartial.

Recommendation 53 (page 272)

The proposed Surveillance Act should require an application for an authorisation to conduct covert surveillance in the public interest to contain information similar to an application for a warrant made by a law enforcement officer (see Recommendation 41).

Recommendation 54 (page 272)

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; and**
- **whether the public interest (or interests) involved justifies the displacement of individual privacy in the circumstances.**

Recommendation 55 (page 275)

The proposed Surveillance Act should provide that an authorisation permitting covert surveillance in the public interest may specify:

- **the circumstances in respect of which the authorisation is granted;**
- **where practicable, the name of any person who is to be the subject of surveillance;**
- **the various public interests considered;**
- **the period (being a period not exceeding 30 days) during which the authorisation may be in force;**
- **that the surveillance device(s) may be repaired, tested, moved, maintained, replaced and/or retrieved during the duration of the authorisation;**
- **the name(s) of the person(s) who may use the surveillance device(s), or who may repair, test, move, maintain, replace or retrieve the surveillance device(s), pursuant to the authorisation;**
- **if practicable, the premises on which the surveillance device(s) are to be installed or used;**
- **that entry onto premises for the purpose of installing, repairing, testing, moving, replacing or retrieving the surveillance device(s) is permitted, provided no trespass is committed;**
- **the type(s) and number of surveillance device(s) to be used;**
- **any conditions subject to which the surveillance device(s) may be used pursuant to the authorisation;**

- **any conditions subject to which any information obtained as a result of the use of the surveillance device(s) may be used, released or published; and**
- **the time within which the person authorised to use the surveillance device(s) pursuant to the authorisation is required to report to the issuing authority and the Attorney General (see recommendation 68).**

An authorisation permitting covert surveillance in the public interest may enable the use of more than one device.

Recommendation 56 (page 277)

Covert surveillance in the public interest must be authorised by the appropriate body prior to the surveillance being conducted. Where such prior authorisation is not possible or practicable, it may be obtained retrospectively (preferably within 24 hours) following the conclusion of the surveillance.

Chapter 7

Recommendation 57 (page 299)

Surveillance in the employment context should be addressed as part of the general framework proposed by the Commission, with the creation of employment specific provisions where necessary.

Recommendation 58 (page 303)

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.

Recommendation 59 (page 304)

There should continue to be an express prohibition on the use of covert surveillance by employers for the purpose of monitoring employee performance.

Recommendation 60 (page 305)

Covert surveillance of employees by employers in toilets, showers and change rooms should be prohibited.

Recommendation 61 (page 306)

When considering an application by an employer for a covert surveillance authorisation that will involve surveillance in recreational or meal rooms, regard must be had to the employees' heightened expectation of privacy.

Recommendation 62 (page 307)

Applications by employers for covert surveillance authorisations should be determined by an Industrial Magistrate or a Judicial Member of the Industrial Relations Commission.

Recommendation 63 (page 308)

The current provisions governing an application by an employer for a covert surveillance authority should be continued. Accordingly, an application by an employer for a covert surveillance authorisation must be in writing, supported by an affidavit, and contain the following information:

(a) the grounds the employer or employer's representative has for suspecting that a particular employee is or employees are involved in unlawful activity or serious misconduct;

(b) whether other managerial or investigative procedures have been undertaken to detect the unlawful activity or serious misconduct and if so, what was the outcome;

(c) who and what will regularly or ordinarily be in view of the cameras;

(d) the dates and times during which the covert surveillance is proposed to be conducted; and

(e) the licensed security operator who will oversee the conduct of the covert surveillance operation.

The issuing authority should have the power to seek further information.

Recommendation 64 (page 310)

In determining whether to grant an authorisation to conduct covert surveillance in the employment context, the issuing authority must have regard to:

(a) the matters listed in the application;

(b) the extent to which the privacy of an employee or employees is likely to be affected; and

(c) the extent to which the privacy of a third party or third parties is likely to be affected.

When considering an application by an employer for a covert surveillance authorisation that will involve surveillance in recreational or meal rooms, the issuing authority must have regard to the employees' heightened expectation of privacy.

The issuing authority must be satisfied that the application shows that reasonable grounds exist to justify its issue.

Recommendation 65 (page 311)

An authorisation permitting covert surveillance in the employment context should specify:

(a) the purpose for which the authorisation is granted;

(b) the licensed security operator who is to oversee the conduct of the surveillance;

(c) where practicable, the name of any person who is to be the subject of surveillance;

(d) the period (being a period not exceeding 30 days) during which the authorisation may be in force;

(e) that the surveillance device(s) may be repaired, tested, moved, maintained, replaced and/or retrieved during the period that the authorisation is in force;

(f) if practicable, the premises on which the surveillance device(s) are to be installed or used;

(g) the type(s) and number of surveillance device(s) to be used;

(h) any conditions on the use of the surveillance device(s);

(i) any conditions on the use, release or publication of any information obtained as a result of the use of the surveillance device(s); and

(j) the time within which the person authorised to use the surveillance device(s) is required to report to the issuing authority and the Attorney General.

Recommendation 66 (page 312)

Where covert surveillance in an employment context is commenced prior to obtaining authorisation, the employer must apply for authorisation as soon as practicable following the commencement.

An application for retrospective authorisation must specify why covert surveillance was commenced prior to obtaining an authorisation.

Part Four: Mechanisms for Ensuring Accountability

Chapter 8

Recommendation 67 (page 320)

The proposed Surveillance Act should not require an applicant for a warrant or authorisation to notify the Attorney General of the application, subject to the following:

- **the issuing authority must notify the Attorney General when an application raises an issue of legal professional privilege; and**
- **the issuing authority may notify the Attorney General or any other person of an application, if the issuing authority deems it appropriate to do so in the circumstances.**

Recommendation 68 (page 325)

The proposed Surveillance Act should require every holder of a warrant or public interest authorisation or employment authorisation to make a report in writing to the Attorney General stating whether or not the surveillance device was used pursuant to the warrant or authorisation. The report should be made within the period specified in the warrant or authorisation, with provision for the Attorney General to approve an extension. If the surveillance device was used, the report should include the following information:

(a) the name, if known, of any person whose private conversation or activity was recorded by the use of the surveillance device;

(b) the period during which the surveillance device was used;

(c) particulars of the types of premises in which the surveillance device was installed or the place where any device was used;

(d) particulars of the general use made or to be made of any evidence or information obtained from the use of the device;

(e) particulars of any previous use of a surveillance device with respect to the same offence or activity subject of the warrant or authorisation;

(f) the type of surveillance device(s) used;

(g) details of any conditions placed by the issuing authority on the exercise of the warrant or authorisation and whether or not those conditions were complied with;

(h) the number of, and reasons for, any warrant or authorisation renewals;

(i) whether the device was retrieved and, if not, the reasons why it was not retrieved; and

(j) any other information requested by the Attorney General.

In the case of surveillance conducted pursuant to a retrospective warrant or authorisation, the report should include, in addition to all the information specified above, information containing the particulars of the circumstances on which a retrospective warrant or authorisation application was based.

Failure to comply with these requirements should constitute an offence.

Recommendation 69 (page 327)

The proposed Surveillance Act should require holders of warrants or public interest authorisations or employment authorisations to report to the issuing authority within the period specified in the warrant or authorisation, with provision for the issuing authority to approve an extension. The report should contain the same information required in the report to the Attorney General. Failure to comply with this requirement should constitute an offence.

Recommendation 70 (page 327)

The proposed Surveillance Act should provide that the registry of the issuing authority should forward annually to the Attorney General such information about applications for warrants or authorisations as it deems appropriate, including:

(a) the number of applications received, granted or refused, and the reasons for refusal;

(b) the number of renewal applications received, granted or refused, and the reasons for refusal;

(c) the number of retrospective warrants granted or refused, and the reasons for refusal; and

(d) any discrepancies the court may have noticed between the affidavit supporting a warrant application and the information provided by the warrant holder concerning the results of the surveillance.

Recommendation 71 (page 328)

The proposed Surveillance Act should provide that the issuing authority:

- **may direct that any record of evidence or information obtained by the use of the surveillance device to which the report relates be brought before it;**
- **may keep such record in its custody; and**
- **may make an order that the evidence or information may be made available to such persons or organisations as the issuing authority directs.**

Recommendation 72 (page 331)

The proposed Surveillance Act should provide that all law enforcement agencies, private individuals and organisations authorised to apply for either warrants or authorisations, should keep records pertaining to the use of surveillance devices. The records should include:

(a) each application for warrants or authorisations;
(b) a statement as to the result of the application;

(c) the warrant or authorisation issued to the person or organisation;

(d) copies of the reports on the warrant to the Attorney General and to the issuing authority;

(e) particulars of each use by the person or organisation of the information obtained by the use of a surveillance device(s);

(f) particulars of each occasion when the information was communicated to a person or organisation, not being a warrant-holder or authorisation-holder;

(g) particulars of each occasion when, to the knowledge of the person or an officer of the agency or organisation, the information was given in evidence in legal proceedings;

(h) details of instances when the activities of persons other than those named in warrants or authorisations were recorded;

(i) particulars of all cases when surveillance devices were used without a warrant or authorisation, including details of the subjects, dates, times and places of the surveillance, the persons who used the devices and the reasons for their use;

(j) particulars of persons whose private activities were monitored or recorded by the use of surveillance devices, but against whom no criminal proceedings had been instituted or were likely to be instituted; and

(k) particulars of the destruction of the information in compliance with the provisions concerning destruction.

Recommendation 73 (page 332)

The proposed Surveillance Act should provide that the inspecting authority (the Privacy Commissioner or Ombudsman) should be required to:

(a) inspect the records of the relevant law enforcement agencies and private individuals or organisations for the purpose of ascertaining:

- **the accuracy of the entries in the records;**
- **the extent of compliance with the requirements of the proposed surveillance legislation including, but not limited to, those concerning the use, communication or publication of surveillance information, storage and security of information, destruction of information; and**
- **whether notice should be given to a subject of the surveillance;**

(b) report to the Attorney General about the result of inspections; and

(c) do anything incidental or instrumental to the performance of any of the preceding functions.

Recommendation 74 (page 333)

The proposed Surveillance Act should provide that the inspecting authority may, at any time, inspect the records of the relevant agencies, organisations or individuals to ascertain compliance with the proposed Surveillance Act. The inspecting authority should inspect records of law enforcement agencies at least once during each financial year.

Recommendation 75 (page 333)

The proposed Surveillance Act should provide that the inspecting authority may, at any time, report the results of the inspection to the Attorney General and shall do so at least once a year and whenever requested to do so by the Attorney General.

Recommendation 76 (page 334)

The proposed Surveillance Act should give the inspecting authority the power to:

(a) enter, at any reasonable time, premises occupied by any relevant agency, organisation or individual, provided reasonable notice is given;

(b) have full and free access, at reasonable times, to their records;

(c) make copies of, and take extracts from, their records; and

(d) require any person to give such information as the inspecting authority considers relevant to the inspection.

Recommendation 77 (page 334)

The proposed Surveillance Act should provide that the communication of surveillance information:

- **to the inspecting authority for purposes of inspection of records; and**
- **by the inspecting authority to the Attorney General for purposes of complying with the reporting requirements**

should be exempted from the general prohibition on the communication or publication of surveillance information. The inspecting authority should ensure that the privacy of individuals to whom the surveillance information relates be respected at all times.

Recommendation 78 (page 334)

The office of the inspecting authority should be given sufficient resources to enable it to discharge effectively its duties under the proposed Surveillance Act.

Recommendation 79 (page 344)

The proposed Surveillance Act should require the Attorney General to include, whenever possible, the following information in the annual report to Parliament:

with respect to warrants for the use of surveillance devices:

(a) the total number of applications for warrants, including the number of radio, telephone, facsimile or other electronic applications, which organisations made the requests and the number of applications that were granted, refused or withdrawn;

(b) the number of applications for retrospective warrants, by whom they were made and the number of those that were granted, refused or withdrawn;

(c) the number and type of offences for which warrants were issued, and the number of warrants issued for each type of offence;

(d) the number of each type of surveillance device used;

(e) the average period of time each warrant was in force;

(f) the number of renewal applications received, granted, refused or withdrawn;

(g) the number of warrants authorising the installation of devices in premises, an indication of the type of premises where devices were installed and the number of warrants authorising surveillance of a particular individual;

(h) the number of warrant applications requesting entry to premises and the number of warrants granted, refused or withdrawn;

(i) the number of warrants issued specifying conditions or restrictions and the type of conditions or restrictions applied;

(j) the number of devices not removed following the completion of surveillance and the reasons why the devices were not removed;

(k) the general use to which information obtained pursuant to surveillance devices has been put, including the number of arrests, prosecutions and convictions in which the information was used; and

(l) the annual cost of the covert use of surveillance devices by the different law enforcement agencies;

with respect to public interest authorisations for the use of surveillance devices:

(a) the total number of applications for public interest authorisations, including the number of radio, telephone, facsimile and other electronic applications, the types of organisations that made the requests and the number of applications that were granted, refused or withdrawn;

(b) the number of applications for retrospective authorisations and the number of those that were granted, refused or withdrawn;

(c) the number of each type of surveillance device used;

(d) the average period of time each authorisation was in force;

(e) the number of renewal applications received, granted, refused or withdrawn;

(f) the number of authorisations issued specifying conditions or restrictions, and the type of conditions or restrictions applied;

(g) the number of devices not removed following the completion of surveillance and the reasons why the devices were not removed; and

(h) the general use to which information obtained pursuant to the surveillance has been put;

with respect to employment authorisations for the use of surveillance devices:

(a) the total number of applications for employment authorisations, including the number of radio, telephone, facsimile and other electronic applications and the number of applications that were granted, refused or withdrawn;

(b) the number of applications for retrospective authorisations and the number of those that were granted, refused or withdrawn;

(c) the number of each type of surveillance device used;

(d) the average period of time each authorisation was in force;

(e) the number of renewal applications received, granted, refused or withdrawn;

(f) the number of authorisations issued specifying conditions or restrictions, and the type of conditions or restrictions applied;

(g) the number of devices not removed following the completion of surveillance and the reasons why the devices were not removed; and

(h) the general use to which information obtained pursuant to the surveillance has been put; and

generally:

(i) the extent of compliance with the requirements of the proposed Surveillance Act including, but not limited to, those concerning the keeping and inspection of records, the use, communication or publication of surveillance information, storage and security of information and destruction of information;

(j) the number of notifications to the subject of the surveillance;

(k) a general account of the extent to which "incidental" information is obtained and used, including, for example, information relating to the commission of an offence by a person not identified in the warrant or authorisation was obtained as a result of the authorised use of a surveillance device;

(l) details of breaches of the proposed Surveillance Act, including actions taken, such as criminal, civil or disciplinary proceedings;

(m) any changes to the proposed Surveillance Act during the year in review;

(n) comparative statistics from previous years; and

(o) any general comments on the operation of the proposed Surveillance Act.

Recommendation 80 (page 356)

The proposed Surveillance Act should provide that where a surveillance device has been used to record the private conversation or activity of a person, the issuing authority may:

- **direct the person or organisation which used the device to supply to the subject of the surveillance, within a period specified by the issuing authority, such information regarding the use of the device as the issuing authority may specify, including details about the surveillance such as the date, time, place and type of devices used;**
- **upon motion, make available to the subject for inspection such portions of the recorded private conversation or activity, applications for the warrant or authorisation and the warrant or authorisation as the issuing authority determines to be in the interest of justice; and**
- **either upon the recommendation of the inspection authority or on its own motion, direct that notice is required to be given, if satisfied that notice is necessary under the circumstances. The issuing authority must give the person or organisation who will be required to give notice an opportunity to be heard on the matter. Failure to comply with a direction to give notice should constitute an offence.**

Chapter 9

Recommendation 81 (page 367)

The proposed Surveillance Act should contain a general prohibition on the publication or communication of all information obtained as a result of the conduct of surveillance, whether the surveillance has been authorised or not, subject to the following exceptions. The prohibition should not apply where the communication or publication of the information is made:

(a) by a law enforcement officer:

- **to another law enforcement officer for the purpose of investigating or prosecuting an offence;**
- **to the DPP or other prosecuting officer for the purpose of prosecuting an offence; or**
- **is otherwise made in the performance of his or her duty;**

(b) in the course of, or for the purposes of, legal proceedings, including proceedings for the prosecution of offences, bail proceedings and those involving confiscation or forfeiture of property in relation to an offence;

(c) in the course of, or for the purposes of, investigations or criminal, civil or disciplinary proceedings related to any violation of the proposed Surveillance Act;

(d) in the belief based on reasonable grounds that it was necessary in connection with an imminent threat of serious violence to persons, or of substantial damage to property;

(e) with the consent of all of the parties to the conversation or activity.

Breach of this provision should be an offence.

Recommendation 82 (page 369)

The proposed Surveillance Act should provide that when a public interest or employment authorisation is made, the order must specify the purposes for which the information obtained though the conduct of surveillance may be used and the circumstances under which the information may be published or communicated. Breach of the terms of the authorisation should constitute an offence. The proposed Surveillance Act should provide that the issuing authority may authorise, at the completion of the surveillance, the use of information obtained by the surveillance for a purpose other than that specified in the authorisation.

Recommendation 83 (page 380)

The admission of evidence obtained in violation of the proposed Surveillance Act should be governed by the *Evidence Act 1995* (NSW) and the general law on evidence.

Recommendation 84 (page 383)

The proposed Surveillance Act should provide that where a private conversation or activity has inadvertently or unexpectedly come to the knowledge of a person as a result of the conduct of surveillance pursuant to a warrant or authorisation:

(a) evidence of the conversation or activity; and

(b) evidence obtained as a consequence of the conversation or activity

may be given by that person in any criminal proceedings even if the warrant or authorisation was not issued for the purpose of allowing that evidence to be obtained.

This should be subject to the proviso that such evidence will not be admissible if the application upon which the warrant or authorisation was granted was not, in the opinion of the court, made in good faith.

Recommendation 85 (page 396)

The proposed Surveillance Act should provide that any court, in any proceedings where evidence obtained through the conduct of surveillance is relevant or admitted in evidence, has the power to suppress the publication of reports of any part of the proceedings, where such publication would create a substantial risk of prejudice to the administration of justice, either generally, or in relation to specific proceedings (including the proceedings in which the order is made). The power should apply in both civil and criminal proceedings and should extend to suppression of publication of the evidence as well as material which would lead to the identification of parties and witnesses involved in

proceedings before the court. Breach of a suppression order should constitute a criminal offence.

Recommendation 86 (page 398)

The proposed Surveillance Act should provide that a person who has obtained material through the conduct of surveillance must ensure that the material and all copies, extracts, summaries or reports of it must be kept in a secure place that is not accessible to people who are not entitled to deal with it. Breach of this requirement should be an offence.

Recommendation 87 (page 409)

The proposed Surveillance Act should provide that every person who obtains information through the conduct of surveillance is required to destroy the information and any record of it as soon as it appears that none of the information directly or indirectly relates to the commission of an offence.

The proposed Surveillance Act should also provide that every person who obtains information through the conduct of surveillance that relates wholly or partly to the commission of an offence is required to destroy the information and any record of it as soon as it appears that no investigations or proceedings will be taken in which the information would be likely to be relevant.

The requirements in these provisions should apply in all cases where information is obtained through the conduct of surveillance, whether the surveillance is authorised or not.

These provisions should be subject to three provisos:

(1) The information should not be destroyed if the person who obtained it is notified that it may be required in criminal, civil, administrative or disciplinary proceedings in connection with the breach of the proposed Surveillance Act. In such case, the information should be destroyed as soon as the proceedings are terminated or it becomes clear that none of them will proceed.

(2) Where the information was gathered under the authority of a public interest or employment authorisation, the information and every record of it should be destroyed as soon as it appears that:

- **the material is not likely to be relevant or useful to the purpose for which the authorisation was issued; or**
- **the purpose for which the authorisation was issued has been accomplished.**

(3) A person who was the subject of surveillance need not destroy the information about him or her obtained as a result of the surveillance and which is in his or her possession unless the information affects or concerns another person.

Information obtained through the conduct of surveillance should not be retained for a period of more than 5 years, unless it remains relevant as provided in the preceding paragraphs. Where information is stored for such length of time, the relevant organisation should conduct periodic reviews to confirm that the justification for its retention remains valid.

The proposed Surveillance Act should provide that the requirements to destroy surveillance information do not apply to material which has been received into evidence in legal proceedings.

Breach of these provisions should constitute an offence.

Chapter 10

Recommendation 88 (page 418)

A breach of an overt surveillance provision of the proposed Surveillance Act should give rise to civil liability.

Recommendation 89 (page 420)

A breach of a covert surveillance provision of the proposed Surveillance Act should constitute a criminal offence.

Recommendation 90 (page 423)

A breach of a provision of the proposed Surveillance Act in the workplace should constitute either a civil breach, if the surveillance was overt, or a criminal offence, if the surveillance was covert.

Recommendation 91 (page 428)

A complaint relating to a breach of an overt surveillance provision of the proposed Surveillance Act should be made to the Privacy Commissioner.

Recommendation 92 (page 428)

The proposed Surveillance Act should give standing to make a complaint to the Privacy Commissioner to the following:

- **a person affected to some degree by the conduct of the surveillance; and**
- **where the surveillance has taken place in the workplace, an industrial organisation on behalf of the employee(s) who have been affected by the conduct of surveillance.**

Recommendation 93 (page 429)

Where the Privacy Commissioner dismisses or declines to entertain a complaint for any reason, the complainant should be able to require the Privacy Commissioner to refer the complaint to a specialist division of the Administrative Decisions Tribunal.

Recommendation 94 (page 429)

The Privacy Commissioner should, in the first instance, conciliate a complaint. Where a complaint remains unresolved 12 months after the date of lodgement of the complaint:

- **either party to the complaint should be able to make a request in writing to the Privacy Commissioner to refer the matter to a specialist division of the Administrative Decisions Tribunal for hearing;**
- **the Privacy Commissioner should be required to refer the complaint within 28 days of such a request, unless the Privacy Commissioner believes the complaint can be conciliated;**
- **where the complainant objects to the referral of the complaint and the Privacy Commissioner is satisfied that the complaint cannot be conciliated, the complaint should lapse.**

Recommendation 95 (page 429)

The Privacy Commissioner should have the power, of his or her own motion, to conduct inquiries and initiate investigations into surveillance related matters, including breaches, or threatened breaches, of the proposed Surveillance Act.

Recommendation 96 (page 430)

An agreement reached pursuant to conciliation should be enforceable by the Privacy Commissioner.

Recommendation 97 (page 430)

The Privacy Commissioner should have the power to decide not to proceed with a complaint where:

- **the dispute has been settled or resolved by agreement between the parties;**
- **the complainant, or person on whose behalf the complaint was made, does not wish to proceed with the complaint; or**

- **the complainant has allowed the complaint to remain inactive for an extended period of time or abandoned the complaint.**

Recommendation 98 (page 430)

The Privacy Commissioner should have the power to refer a complaint to the Administrative Decisions Tribunal at any time if he or she is satisfied that the nature of a complaint is such that it should be referred. The Privacy Commissioner should be able to exercise this power whether or not an investigation into the complaint has been undertaken or completed. The Privacy Commissioner should not refer a complaint without the consent of the complainant unless there are exceptional circumstances. The respondent should be given the opportunity to be heard on why a complaint should not be referred, but should only be able to resist referral on the grounds that the complaint has been settled by agreement and the respondent remains ready, willing and able to abide by the terms.

Recommendation 99 (page 431)

The proposed Surveillance Act should give standing to bring proceedings in the Administrative Decisions Tribunal to the following:

- **a person affected to some degree by the conduct of the surveillance;**
- **the Privacy Commissioner, including in a representative capacity; and**
- **where the surveillance has taken place in the workplace, an industrial organisation on behalf of the employee(s) who have been affected by the conduct of surveillance.**

Recommendation 100 (page 431)

The Administrative Decisions Tribunal should have the power to grant the Privacy Commissioner leave to intervene on behalf of a complainant, where considered appropriate, in proceedings before it.

Recommendation 101 (page 431)

The *Administrative Decisions Tribunal Act 1997* (NSW) should adopt a comprehensive set of procedural and machinery provisions, similar to the provisions contained in the *Federal Court of Australia Act 1976* (Cth), to deal with the conduct of representative complaints under the proposed Surveillance Act.

Recommendation 102 (page 432)

The proposed Surveillance Act should contain provisions similar to the Anti-Discrimination Act regulating procedural requirements in relation to complaints and the practices and procedures governing the conduct of proceedings.

Recommendation 103 (page 433)

Prosecution for a breach of a covert surveillance provision of the proposed Surveillance Act, or for breach of a provision which the proposed Surveillance Act specifies will give rise to a criminal offence, should be through the criminal justice system.

Recommendation 104 (page 433)

Offences against the proposed Surveillance Act generally should be prosecuted summarily, before a Local Court constituted by a Magistrate sitting alone, or before the Supreme Court in its summary jurisdiction. There should be provision within the proposed Surveillance Act for prescribed offences to be able to be prosecuted either summarily or on indictment. There should

also be provision in the proposed Surveillance Act for summary proceedings to become committal proceedings if the court decides that the offence should be dealt with as an indictable offence, and no evidence has been led by the defendant.

Recommendation 105 (page 434)

A person aggrieved by the conduct of covert surveillance, or a breach of a provision giving rise to a criminal offence, should have access to the complaints and review processes available in relation to breaches of overt surveillance provisions, both generally and in the workplace.

Recommendation 106 (page 438)

A person aggrieved by a breach of the provisions of the proposed Surveillance Act in the workplace should have access to the complaints and review processes available for surveillance generally, or, if the person so chooses, should be able to pursue the complaint in the Industrial Relations Commission.

Recommendation 107 (page 438)

The *Industrial Relations Act 1996* (NSW) should be amended to enable the Industrial Relations Commission to hear complaints under the proposed Surveillance Act.

Recommendation 108 (page 438)

The *Industrial Relations Act 1996* (NSW) should be amended to provide that an issue that is the subject of proceedings under the proposed Surveillance Act before the Administrative Decisions Tribunal may, with the Commission's leave, be the subject of proceedings before the Industrial Relations Commission. It should be a condition of granting leave that any relief received previously is not duplicated and that granting the relief sought would not cause undue prejudice to the respondent.

Recommendation 109 (page 439)

The proposed Surveillance Act should provide that an issue that is the subject of proceedings under that Act before the Industrial Relations Commission may, with the leave of the Administrative Decisions Tribunal, be the subject of proceedings before the Tribunal. The proposed Surveillance Act should provide expressly that it be a condition of granting leave that any relief received previously is not duplicated and that granting the relief sought would not cause undue prejudice to the respondent.

Recommendation 110 (page 439)

The Administrative Decisions Tribunal should have the power to transfer proceedings brought under that Act to the Industrial Relations Commission on the application of the complainant or in any such circumstances as to the Tribunal seems just.

Recommendation 111 (page 439)

The Industrial Relations Commission should have the power to transfer proceedings brought under the proposed Surveillance Act to the Administrative Decisions Tribunal on the application of the complainant or in any such circumstances as to the Commission seems just.

Recommendation 112 (page 446)

The proposed Surveillance Act should provide that in proceedings brought under that Act, the Administrative Decisions Tribunal should have the power to grant the following relief:

- **an award of damages to the limit of $150,000, except in cases where the panel has a District Court judge as its presidential member where the limit should reflect the jurisdiction of the District Court;**
- **an injunction;**
- **a mandatory order;**

- **a declaration that certain conduct is unlawful under the Surveillance Act;**
- **an order that a respondent publish an apology or retraction in relation to unlawful conduct under the proposed Surveillance Act;**
- **an order that a respondent implement a program or policy aimed at eliminating all forms of unlawful conduct under the proposed Surveillance Act;**
- **an order that the respondent not disclose information obtained as a result of the surveillance; and**
- **such other orders as seems to the Administrative Decisions Tribunal to be just and appropriate in the circumstances.**

Otherwise, the powers of the Administrative Decisions Tribunal with respect to orders should be those available under the *District Court Act 1973* (NSW).

Recommendation 113 (page 446)

The Administrative Decisions Tribunal should have the power to make interim orders to preserve the rights of the parties, on the application of either the Privacy Commissioner or a party to the proceedings.

Recommendation 114 (page 447)

The Administrative Decisions Tribunal's power to award damages should not be limited to financial loss, but should include the power to award damages for psychological or physical harm resulting from the unlawful surveillance.

Recommendation 115 (page 447)

The Administrative Decisions Tribunal should have the power to grant an injunction which extends to the conduct of surveillance affecting persons other than the individual complainant in the following circumstances:

- **where the complaint has been lodged in a representative capacity;**
- **where the Privacy Commissioner has been notified and given the opportunity to make submissions; or**
- **in any other case, where the Tribunal believes that the particular circumstances warrant such action.**

Recommendation 116 (page 447)

Where the Administrative Decisions Tribunal makes a mandatory order which is not by consent and the cost of compliance would exceed the statutory maximum, the respondent should have a right of appeal in relation to the appropriateness of the order.

Recommendation 117 (page 448)

The proposed Surveillance Act should give the Privacy Commissioner the power to monitor compliance with mandatory and injunctive orders made by the Administrative Decisions Tribunal.

Recommendation 118 (page 448)

The proposed Surveillance Act should give the Privacy Commissioner standing to apply for injunctive, mandatory and declaratory orders, whether or not proceedings have been instigated by a complainant.

Recommendation 119 (page 448)

Where proceedings have been brought by an industrial organisation or by the Privacy Commissioner in a representative capacity, the Administrative Decisions Tribunal should have the power to make similar orders for relief as is available in representative proceedings under the *Federal Court of Australia Act 1976* (Cth).

Recommendation 120 (page 448)

The proposed Surveillance Act should give the Privacy Commissioner the power:

- **in the case of an individual complaint, to take steps to enforce an order on behalf of a complainant with their consent; and**
- **in the case of a representative complaint (or in any other case where the Privacy Commissioner believes that the public interest demands), to take steps to enforce an order on his or her own motion.**

Recommendation 121 (page 450)

The proposed Surveillance Act should provide for criminal penalties in line with the framework contained in the LDA.

1. Introduction

[N]umerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

Samuel D Warren and Louis D Brandeis, in 1890[1]

- Background to this reference
- Privacy
- Surveillance
- Uses of surveillance devices
- Existing regulation of surveillance
- The structure of this paper

1. *S D Warren and L D Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193 at 195.*

BACKGROUND TO THIS REFERENCE

1.1 In 1996 the Commission received a reference from the then Attorney General, the Hon Jeff Shaw QC MLC, to inquire into and report on matters pertaining to the Listening Devices Act 1984 (NSW), the use of visual surveillance equipment, and any related matter. In May 1997 the Commission released an Issues Paper ("IP 12"),[2] inviting submissions from the public. Over thirty-seven submissions were received.[3]

1.2 It was anticipated at that time that IP 12 would be followed by a final report. However, as submissions were received on IP 12, and additional research and consultation were undertaken, the Commission concluded that the scope of the surveillance project was much wider than was originally envisaged. The pace of technological change was such that any attempt to limit surveillance legislation to specific types of devices would be fruitless, and the proliferation of surveillance equipment in the retail sector and in public places meant that greater consideration needed to be given to the appropriate regulatory framework. The Commission considered publishing a discussion paper and engaging in further community consultation, but decided that it was preferable to publish an interim report. This reflected the fact that the Commission had reached final views on the regulatory scheme to be recommended, but had not proceeded to develop draft legislation which would set out all of the detail of the scheme. The Commission will consult with the Attorney General to decide what, if any, further work should be undertaken by the Commission on this project.

PRIVACY

1.3 The terms of reference direct the Commission to have regard to the protection of the privacy of the individual. However, while the issue of privacy is fundamental to any consideration of the

2. *New South Wales Law Reform Commission, Surveillance (Issues Paper 12, 1997) ("IP 12").*
3. *See Appendix B.*

surveillance spectrum, it is important to note that the Commission is not conducting an inquiry into privacy as such.

What we think of as privacy

1.4 Since the famous dictum of Judge Cooley, that privacy is the right "to be let alone",[4] many definitions and formulations have been proposed, yet it is a concept each of us readily understands in one way or another. Privacy is a collective term for a number of interests, which the Australian Law Reform Commission, in its Report on Privacy,[5] identified as follows:

- *the interest in controlling entry to personal territory;*
- *the interest in freedom from interference with one's person, including "personal space";[6]*
- *the interest in controlling one's personal information; and*
- *the interest in freedom from surveillance and the interception of one's communications.*

1.5 Surveillance can affect all of these interests. Very often, the goal of surveillance is to pierce the privacy shield, sometimes justified by the view that "if you have done nothing wrong you should have nothing to hide". Apart from the enormous faith this places in the benevolence and objectivity of the watcher, this view is simplistic and narrow. As one American jurist put it:

> *Most people in no wise deformed or disfigured would*

---

4. *Warren and Brandeis at 195.*
5. *Australian Law Reform Commission ("ALRC"), Privacy (Report 22, 1983) at para 46.*
6. *"[T]his sense of privacy transcends the physical and is aimed essentially at protecting the dignity of the human person. Our persons are protected not so much against the physical search ... as against the indignity of the search, its invasion of the person in a moral sense": Canada, Department of Communications and Department of Justice, Privacy and Computers: a report of a Task Force established jointly by the Department of Communications and the Department of Justice (Ottawa, 1972) at 13-14.*

> *nevertheless be deeply upset if nude photographs of themselves were published in a newspaper or book. They feel the same way about photographs of their sexual activities, however "normal," or about a narrative of those activities, or about having their medical records publicised. Although it is well known that every human being defecates, no adult human being in our society wants a newspaper to show a picture of him defecating. The desire for privacy illustrated by these examples is a mysterious but deep fact about human personality. It deserves and in our society receives legal protection. … An individual, and more pertinently perhaps the community is most offended by the publication of intimate personal facts when the community has no interest in them beyond the voyeuristic thrill of penetrating the wall of privacy that surrounds a stranger.*[7]

1.6 Jeffrey Rosen provides another analysis of the potential detriment of privacy loss:

> *Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge. True knowledge of another person is the culmination of a slow process of mutual revelation. ... When intimate personal information circulates among a small group of people who know us well, its significance can be weighed against other aspects of our personality and character. By contrast, when intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences.*[8]

1.7 If there are dangers, as Rosen foresees, in glimpsing such slivers of a person's life, others find no more comforting the prospect of potential mass surveillance systems capable of delivering slabs of information about an individual and how he or she spent the day.[9]

---

7. Haynes v Alfred A Knopf Inc (1993) 8 F3d 1222 at 1229, 1232 (Posner J).

8. J Rosen, The Unwanted Gaze: the Destruction of Privacy in America (Random House, New York, 2000) at 8-9.

9. For examples of such systems see J Robotham, "Weaving the Tangled Web" Sydney Morning Herald (16 December 1995,

"Orwellian" is a favourite adjective appearing in works on this subject.

A "right" of privacy?

1.8 Undoubtedly, all persons have an interest in preserving their privacy. Moreover, it is reasonable to regard privacy as a basic human right. This is not the same, however, as enjoying a right to privacy, which would afford an enforceable remedy for interference with one of the privacy interests.[10] Indeed, in Australia there is no general legal right to privacy.[11] However, certain privacy interests do find protection. At common law, for example, the law of trespass protects, inter alia, an interest in territorial privacy. A range of privacy interests is protected in various Commonwealth[12] and State[13] statutes. Information privacy, in particular, finds some protection in both Commonwealth[14] and State[15] legislation. We return to a more detailed discussion below at paragraph 1.36 and following.

1.9 Australia is also a party to a number of international conventions that provide some protection for privacy. Perhaps the most significant of these is the International Covenant on Civil and Political Rights ("ICCPR"). Article 17 of the Convention provides:

Spectrum) at 7; S McKenzie, "Enjoy Your Flight ... We've Got You Already" Daily Telegraph (29 January 1997) at 11.

10. *ALRC Report 22 at para 45.*
11. *Victoria Park Racing and Recreation Grounds Company Ltd v Taylor (1937) 58 CLR 479 at 496.*
12. *Eg Aboriginal and Torres Strait Islander Commission Act 1989 (Cth) s 7(1)(h) and 142A(6); Customs Act 1901 (Cth) s 219M(2) and 219Q(2).*
13. *Eg Adoption Information Act 1990 (NSW) s 3; Anti-Discrimination Act 1977 (NSW) s 31; Births, Deaths and Marriages Registration Act 1995 (NSW) s 48.*
14. *Privacy Act 1988 (Cth).*
15. *Privacy and Personal Information Protection Act 1988 (NSW).*

> 1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
> 2. *Everyone has the right to the protection of the law against such interference or attacks.*

1.10 Generally speaking, in order for the provisions of an international convention to become legally binding in Australia, they must be incorporated into our law by statute.[16] The Privacy Act 1988 (Cth) does this to the extent of applying to information held by Commonwealth government agencies.[17]

1.11 In Minister of State for Immigration and Ethnic Affairs v Ah Hin Teoh[18] the High Court of Australia held that the ratification of the United Nations Convention on the Rights of the Child gave rise to a legitimate expectation that in making deportation decisions, the Minister would act in conformity with it. In their reasons for holding that the Court had denied Mr Teoh the opportunity to present his case against an adverse decision which had not taken into account the rights of his children, Mason CJ and Deane J stated:

> *Junior counsel for the appellant contended that a convention ratified by Australia but not incorporated into our law could never give rise to a legitimate expectation. No persuasive reason was offered to support this far-reaching proposition. The fact that the provisions of the Convention do not form part*

---

16. *Cf Minister of State for Immigration and Ethnic Affairs v Ah Hin Teoh (1995) 183 CLR 273 at 286-287.*
17. *To this extent the Act also ensures that the Commonwealth's responsibilities as a member of the Organisation for Economic Co-operation and Development (OECD) are met, in taking into account the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The passing of the Privacy Amendment (Private Sector) Act 2000 (Cth) in December 2000 amends the principal Act, so that it will, upon commencement in December 2001, apply to most private sector organisations as well. It is based on the Privacy Commissioner's January 1999 voluntary National Principles for the Fair Handling of Personal Information: see the Australian Privacy Commissioner's website at «www.privacy.gov.au».*
18. *(1995) 183 CLR 273.*

> *of our law is a less than compelling reason – legitimate expectations are not equated to rules or principles of law. Moreover, ratification by Australia of an international convention is not to be dismissed as a merely platitudinous or ineffectual act, particularly when the instrument evidences internationally accepted standards to be applied by courts and administrative authorities in dealing with basic human rights affecting the family and children. Rather, ratification of a convention is a positive statement by the executive government of this country to the world and to the Australian people that the executive government and its agencies will act in accordance with the Convention.*[19]

1.12 Another way in which the ratification of international conventions can have implications for Australians, where the convention has not otherwise been incorporated into Australian law by statute, is by way of a decision of the United Nations Human Rights Committee. Australia became a party to the First Optional Protocol to the ICCPR which entered into force in December 1991. As a result, Australia recognises the competence of the Human Rights Committee to receive and consider communications from individuals claiming that their rights under the Convention have been violated. Tasmanian Nicholas Toonen submitted a communication to the Committee arguing (inter alia) that the provisions of the Tasmanian Criminal Code that proscribed

---

19. Minister of State for Immigration and Ethnic Affairs v Ah Hin Teoh (1995) 183 CLR 273 at 290-291 (Mason CJ and Deane J). In a ground-breaking decision handed down in December 2000, the English Court of Appeal found that the actors Catherine Zeta-Jones and Michael Douglas had a "powerful prima facie claim to redress for invasion of their privacy as a qualified right recognised and protected by English law." This was possible because less than three months earlier, the Human Rights Act 1998 (UK) had come into force, giving effect to rights guaranteed under the European Convention on Human Rights, including a right to privacy and a right to freedom of expression. The couple were granted the right to sue Hello! magazine for invasion of privacy, after it published pictures of their wedding ahead of a rival publication which had paid for the exclusive right to do so: F Gibb, "New Privacy Right Won by Zeta-Jones" The Times «www.thetimes.co.uk/article/0,,2-57584,00.html».

consensual sexual activity between men violated his right to privacy under Article 17 of the ICCPR and in 1994, the Human Rights Committee upheld his claim.[20] While a decision of that Committee is not binding or enforceable in Australia, the Human Rights Committee considered that an effective remedy would be the repeal of the relevant provisions of the Tasmanian law. When Tasmania initially failed to respond, the Commonwealth government passed the Human Rights (Sexual Conduct) Act 1994 with the intention of, in effect, "overruling" the Tasmanian legislation by the use of section 109 of the Commonwealth Constitution.[21] In the event, the provisions were finally repealed in 1997, after the High Court agreed to hear an action brought in relation to the Toonen matter in February 1997.[22]

An expectation of privacy

1.13 In most societies people have an expectation that they will enjoy some degree of privacy. In this Report we are concerned principally with the fourth of the privacy interests identified by the ALRC, appearing at paragraph 1.4, the interest in freedom from surveillance. The Irish Law Reform Commission ("ILRC"), in its Report on privacy and surveillance, uses the shorthand term "surveillance privacy". The expression "reasonable expectation of privacy"[23] is used by the ILRC and in this Report (at paragraph 4.41) as a yardstick by which to measure the acceptable boundaries of surveillance use. The ILRC, for example, defines surveillance

---

20. He also argued that the Act violated his right to equality under Article 26, but the Committee decided there was no need to consider that, given its view on Article 17. For a discussion of this see W Morgan, "Identifying Evil For What it is: Tasmania, Sexual Perversity and the United Nations" (1994) 19 Melbourne University Law Review 740.

21. Section 109 provides: "When a law of a State is inconsistent with a law of the Commonwealth, the latter shall prevail, and the former shall, to the extent of the inconsistency, be invalid."

22. Croome v Tasmania (1997) 71 ALJR 430.

23. The "reasonable expectation of privacy" test was coined in the leading American case of Katz v United States 389 US 347 (1967).

privacy, or freedom from privacy-invasive surveillance, as "that freedom which a reasonable person in the circumstances of the case is entitled to expect".[24]

SURVEILLANCE

1.14 Surveillance might conjure in some minds an image of a private eye shadowing his or her prey, a security camera silently recording the scene below, or even the long-range lens of a paparazzo protruding from the lush undergrowth of some exclusive hideaway. These more colourful examples are gleaned from films, action novels and daily tabloid offerings. Many people probably do not think of themselves as the targets of surveillance, yet this is increasingly the case.

1.15 Most people are familiar with day-to-day surveillance: they are subject to it in banks, at service stations, on railway platforms. These particular examples are of the unconcealed use of visual surveillance equipment, most commonly by means of a closed circuit television (CCTV) system. Surveillance today, however, can take forms which many would find surprising. The author of the following scenario[25] *says that, while it is fictional, he believes it to be "much nearer to reality than fantasy":*

> *At approximately 2.15 am, in response to an anonymous tip about an indoor marijuana growing operation, two agents from the Drug Enforcement Agency (DEA) pull up to the curbside fronting the home of William "Billy" Oldman. For the past decade, marijuana growers have been forced to bring their operations indoors in an attempt to avoid detection by low-flying DEA airplanes and helicopters. … The agents know that indoor marijuana growers often attempt to insulate their houses to avoid law enforcement detection of the heat from the*

---

24. Ireland, Law Reform Commission, Report on Privacy: Surveillance and the Interception of Communications (LRC 57, 1998) at para 2.10.

25. M L Zabel, "A High-Tech Assault on the 'Castle': Warrantless Thermal Surveillance of Private Residences and the Fourth Amendment" (1995) 90 Northwestern University Law Review 267 at 267 and 268 note 1.

> *high-wattage "grow lamps" necessary for indoor growing operations. [One of the agents] removes the DEA's most dependable portable thermal imager from its carrying case and raises the handheld device to eye level. To obtain the necessary baseline reading and to fine-tune the unit, the agent aims the imager at the residence adjacent to Oldman's. After turning down the sensitivity level on the unit to correct an over-exposed view … he observes in one room of a neighbouring house what appears to be two concentrated, abnormally high heat patterns, identifiable as humans, moving in tandem – apparently a couple captured in a moment of intimacy. Then, once trained on another nearby house, the imager reveals two focused heat patterns seemingly chasing one another from room to room – probably a domestic disturbance, the agent imagines, considering the area of town.*

1.16 Surveillance can take place through a person's unaided senses. Alternatively, it can be carried out, enhanced and recorded, by an array of devices, such as:

- *binoculars and telescopes;*
- *listening devices or "bugs";*
- *video cameras;*
- *audio-visual devices;*
- *computers*[26]*;*
- *tracking devices*[27]*;*

---

26. Computer surveillance can refer to accessing information stored in the computer or to monitoring the behaviour of the person operating the computer. One computer software company has developed a product to analyse a "customer's" reaction to internet advertising when viewing it on his or her monitor. This product goes further than merely counting the number of "hits", or visits, made by all viewers to an internet page. It registers "the time a user spends looking at a specific ad. It also uses hidden touchpoints in the advertisement to record how long the cursor lingers over a specific message in the text as the user decides whether or not to click onto it for more information. … every move of every user can be watched and recorded …": H Sher, "Net Income" Jerusalem Report (7 August 1997) at 36-37.

- *biometric identification systems, which use some personal characteristic to verify identity*[28]*; and*
- *various technologies of the type developed to detect concealed weapons.*[29]

1.17 Most of these can be deployed either overtly or covertly. By the former we mean that the fact that surveillance is taking place is known, or expected, or readily able to be known by most of those subjected to it. Covert surveillance is, to the contrary, surveillance which is carried out in secret. Definitions of these terms, and of "surveillance" and "surveillance device" are found in Chapter 2.

---

27. For example, in December 1995 a State-wide network of cameras, Safe-T-Cam, commenced operation in New South Wales. It "tracks the movements of trucks across NSW by using artificial computer sight to recognise their number plates and relaying those details to a central computer in Sydney. Safe-T-Cam determines 'whether any potential travel time or speeding violation may have occurred', according to an RTA spokesman.": J Robotham, "Weaving the Tangled Web" Sydney Morning Herald (16 December 1995, Spectrum) at 7.

28. For example, fingerprint and palm verification, voice and facial recognition, signature verification, and "even body odours sensed through the palm": SJB Services, "The Biometrics Report: News Release" «www.sjb.co.uk/pr/pr_tbr2.txt». "Biometric technologies – the logging of unique personal measurements – are already emerging as the next wave of public surveillance … In Massachusetts, State authorities use the Eigen Faces system, which maps areas of light and shade to collect uniquely identifiable facial images of all registered drivers. Biometrics would not be possible without computer programs, called algorithms, for recognising particular patterns from vast backgrounds of white noise, and this is one of computing's fastest advancing technologies. These algorithms can, literally, pick a face in a crowd.": J Robotham, "Weaving the Tangled Web" Sydney Morning Herald (16 December 1995, Spectrum) at 7.

29. For example, back-scattered x-ray imaging and passive millimetre wave imaging: M Hansen, "No Place to Hide" (August 1997) 83 ABA Journal 44 at 47.

Origins

1.18 The tale of the Trojan horse and the biblical account of Moses sending spies into Canaan[30] show that surveillance is at least as old as recorded history. Espionage and military intelligence are still the source of much of the surveillance technology in use today.[31] In the United States the earliest systematic collection of military intelligence took place during the Civil War,[32] employing such surveillance techniques as signal intercepts. Further developments have continued apace, limited, it would seem, only by imagination. In the 1960s tiny waterproof bugs disguised as martini olives (the toothpick acting as the antenna) had made their appearance in spy fiction.[33] In the 1990s, in real life, "smart dust" commenced development, to be used for such military applications as battlefield surveillance and "scud hunting".[34]

1.19 As the use of surveillance technology for military purposes has grown, its greater affordability and accessibility has allowed it to be

---

30. *Numbers XIII:2.*
31. *Night viewing devices, for example, resulted from technology developed during the Vietnam War: G Yost, Spy-Tech (Harrap, London, 1985) at 206.*
32. *M Nieto, Public Video Surveillance: is it an Effective Crime Prevention Tool? (California Research Bureau, California State Library, Sacramento, 1997) at 2.*
33. *G Yost, Spy-Tech (Harrap, London, 1985) at 176.*
34. *Smart dust "relies on the convergence of three technologies: digital circuitry, laser-driven wireless communications, and something called MEMS (Micro ElectroMechanical Systems) to pack enough equipment into a space no more than one or two cubic millimeters in size": J Flint, "Smart Dust" «www.telepolis.de/tp/english/inhalt/co/5269/1.html». The inventors claim numerous applications for their product, including inventory control and product quality monitoring, but acknowledge that as they are funded by DARPA, the US Defence Department's central research and development organisation, they are working on military applications: University of California at Berkeley, Department of Electrical Engineering and Computer Sciences, "Smart Dust: Autonomous Sensing and Communication in a Cubic Millimetre" «robotics.eecs.berkeley.edu/~pister/SmartDust».*

imported into civilian life. Video surveillance technology, introduced in 1956, was one of the first examples.[35] Burrows claims that by 1984 video surveillance systems in a number of districts in the United States were being dismantled because of their failure to lead to arrests and convictions.[36] In recent years, however, the use of closed-circuit television (CCTV) systems has mushroomed. In fact, nowadays such equipment can be purchased by anyone from specialty shops or through the internet. While it is difficult to quantify the extent of video surveillance usage in any part of the world, one commentator[37] estimated that in 1997, 300,000 cameras had been installed in public places throughout the United Kingdom. According to an industry spokesman,[38] Sydney alone may have more than 30,000 surveillance cameras.

1.20 The manner in which surveillance is being used in public places today has altered since the early years. It is more likely to be promoted as just one of several measures in an approach termed "situational crime prevention". This focuses on the context in which crime occurs, and in reducing opportunities for crime, rather than in the detection and punishment of offenders.[39] Accompanying the burgeoning use of CCTV systems are other measures, such as defensible space architecture in public housing, improved stocktaking and record keeping procedures, electronic access for cars and telephone systems, and alcohol controls at public events.[40] The Byron Bay Safe Celebration Project, replicated at Sydney's

---

35. D Diamond (ed), The Cambridge Factfinder (Cambridge University Press, 1994) at 526.

36. Hoboken (New Jersey), Olean and Mount Vernon (New York), Times Square (Manhattan, NY) and Miami Beach (Florida): Q Burrows, "Scowl Because You're on Candid Camera: Privacy and Video Surveillance" (1997) 31 Valparaiso University Law Review 1079 at 1103.

37. T Dixon, "Who Will Watch the Watchers" Sydney Morning Herald (17 February 1997) at 17.

38. John Date, quoted by D Murphy, "Council Pays $1.5m to Keep Eye on City" Sydney Morning Herald (18 December 1998) at 6.

39. R V Clarke, Situational Crime Prevention: Successful Case Studies (2nd ed, Harrow and Heston, NY, 1997) at 2.

40. Clarke at 2.

Bondi Beach, is an example, following New Year's Eve disturbances in the past.[41] The City of Sydney, too, has devised a 10-point plan it hopes will protect personal safety in the central business district, of which the installation of a CCTV network is but a part.[42]

1.21 Other forms of sophisticated technology can be pressed into service for relatively prosaic purposes. For example, advertisements appear in non-specialist magazines for tracking and recovery systems for stolen vehicles, based on what is claimed to be latest military tracking technology. Combining technologies produces new opportunities and scenarios, for example:

> *You have been pulled over for speeding by police using a laser gun. A zoom video camera in the squad car is recording the whole incident, and miniature radio microphones on the police officer's lapel are capturing your conversation. While you are talking, your blood alcohol level is measured on a "passive direct" breathalyser powered by a space-age fuel cell. With a hand-held, pen-operated computer, the officer checks your licence and registration number and knows within three seconds whether you are wanted for any outstanding offences. Meanwhile, details of the speeding offence are digitally beamed by satellite or radio wave from the video-laser/radar unit in the police car to a central processing office. Far-fetched science fiction? A glimpse into the future? Perhaps even technology that's just around the corner? It's none of those. It's technology that is being used by police*

41. *New South Wales, Crime Prevention Division, "Developing Local Crime Prevention Plans: Why Should a Local Council Care About Crime Prevention?" «www.lawlink.nsw.gov.au/cpd.nsf/pages/ cpddevelop3».*
42. *The other nine points are: emergency video phones, improved street lighting, graffiti removal, upgrading city streets to encourage greater public use, crime prevention through environmental design, consultation between Police and licensed premises regarding the serving of alcohol, community safety education, increasing the number of personnel in a City Safety Taskforce, and developing supervised recreational activities in the Central Sydney area: City of Sydney, Report to Ratepayers 1997-98 at 22-23.*

right now, somewhere in Australia, today.[43]

1.22 So-called "smart highways" may be able to produce a number of desirable outcomes, including improving traffic flow by deducting tolls from prepaid accounts and monitoring congestion.[44] *Critics, however, see in them a sinister potential for a mass surveillance system.*[45]

1.23 The etymological origin of surveillance – a "watch kept over a person or thing"[46] *– is also instructive. Surveillance in a societal context had a target, such as a suspect or prisoner, the distinction between the two probably counting for little in terms of privacy. Today, the word has an additional, more passive sense, as in the monitoring of a scene without any particular target, by which means any untoward activity, such as a skirmish or vehicle collision, can be noted. The operation of surveillance is not, however, a neutral concept, as the decision to install a surveillance device is not taken randomly. The presence of a device implies some foreseeable risk of wrongdoing or accident in the area under surveillance. Individuals whose images are captured by surveillance may be considered potential suspects in yet-to-be committed crimes.*

1.24 For a society that used surveillance to counter the threat posed by the enemy, without or within, privacy may not have been seen as an important issue. Today, however, the potential "threat" upon which surveillance focuses is much more diverse: the shoplifter, the international terrorist, the traffic snarl. The use and development of surveillance devices and systems have spread apace in pursuance of many legitimate interests. Left behind has

---

43. H Grennan, "Cops and robots" Bulletin (17 June 1997) at 18.

44. Safe-T-Cam (see note 27 above) is one example, described in the Transport Workers' Union newspaper as a way to "reduce the economic pressure on the majority of drivers by modifying the behaviour of those who compete unfairly by speeding and driving long hours": J Robotham, "Weaving the Tangled Web" Sydney Morning Herald (16 December 1995, Spectrum) at 7.

45. J Robotham, "Weaving the Tangled Web" Sydney Morning Herald (16 December 1995, Spectrum) at 7.

46. C T Onions (ed), Oxford Dictionary of English Etymology (Oxford, 1978) at 890.

been a serious and detailed appraisal of whether they can be used in a way that does not present an unacceptable threat to privacy, and a consideration of how the potential subject of that surveillance – the general public – is affected by it.

USES OF SURVEILLANCE DEVICES

1.25 Surveillance is used routinely for the following purposes:

- *law enforcement, as carried out by police, the New South Wales Crime Commission, Australian Security Intelligence Organisation and other such agencies;*
- *private investigation, most commonly in relation to suspected insurance frauds related to motor vehicle accident and workers compensation claims, but also in family law cases and other matters;*[47]
- *workplace monitoring by employers;*
- *media reportage;*
- *enhancing public safety through traffic and crowd control; and*
- *protection of private property.*

1.26 Any of the above examples can be abused. Most obviously, surveillance can be used illegitimately for high-tech prying. An article in The New Yorker magazine, with resonances of Hitchcock's Rear Window, makes the point that a hundred telescopes are purchased each week in New York City, or approximately 5000 a year: "To see what? Most people haven't seen a star since the great blackout in 1977".[48]

Law enforcement

1.27 Surveillance is used for a number of law enforcement

47. M Dapin, "P I Blues" Sun Herald Sunday Life Supplement (8 March 1998) at 10.

48. B Buford, "Thy Neighbour's Life" New Yorker (5 January 1998) at 36.

functions.

Deterrence

1.28 It is thought that the warning, or visible presence, of cameras can have a deterrent effect on the commission of crime. This is the principal rationale underlying the use of the majority of unconcealed surveillance devices. A would-be offender, mindful of such consequences as the revelation of his or her identity, and the possibility of arrest and punishment, may think again before committing an illegal act.

On the spot policing

1.29 Of greater facility is the use of surveillance in on-the-spot policing. A vivid example is given by Ben Brown[49] in his series of case studies on the use of CCTV in three town centres in the United Kingdom:

> *Just after 11.00 pm one Sunday evening the CCTV operator noticed a person lying in the street. He looked around the area and then noticed two people who appeared to be attacking members of the public indiscriminately. One of the assailants then walked up to another person at a bus stop and hit him. The victim fell over and, as he fell he knocked his head on the curb. At this moment a bus drew up. The assailants then got on bus (sic), but by this time the CCTV operator had alerted police officers. The officers arrived on the scene just as the bus was leaving and they managed to stop the bus and arrest the assailants. The victim later died of his injuries.[50]*

As Brown notes, through surveillance it was possible for the police to be at the scene rapidly and apprehend the assailants, obviating the need to mount a lengthier and less certain search. It should be noted, however, that this was possible because the scene was being observed by the CCTV operator at the time, and not merely

---

49. B Brown, CCTV in Town Centres: Three Case Studies (Home Office Police Department, Police Research Group Crime Detection and Prevention Series No 68, London, 1995).

50. Brown at 24.

videotaped for later viewing after the incident.[51]

Evidence

1.30 One of the most important uses for surveillance is in the area of evidence gathering for investigation and possible prosecution of a crime. Video recordings of offences are crucial in assisting police in their investigations, notably in identifying offenders, the time at which the offence was committed, the modus operandi, and so on. The use of the product of surveillance as evidence will be discussed in Chapter 9. The material can also be very useful in finalising investigations. Suspects given the opportunity to view themselves in incriminating video footage are more likely to plead guilty, thus dispensing with the need for a trial, with its attendant financial and time costs. Such evidence can also clear a suspect of a false accusation. Justice Wood gave this ringing endorsement:

> *The Royal Commission found that its use of electronic surveillance was the single most important factor in achieving a breakthrough in its investigations.*[52]

1.31 International examples of the successful deployment of video evidence include the apprehension of those responsible for the theft of Edvard Munch's painting "The Scream" (Norway), the murder of James Bulger (United Kingdom), and the bombing of a federal building in Oklahoma City (United States).[53] *The presence of the surveillance cameras, however, did nothing to prevent the commission of these crimes.*

Public safety and crowd control

1.32 Surveillance cameras are used to monitor traffic routes, major sporting events and other public spectacles. They can play an effective part in identifying trouble spots so that an appropriate

---

51. One might also note that this is also an example of CCTV failing to act as a deterrent.

52. New South Wales, Royal Commission into the New South Wales Police Service, Final Report Vol 2: Reform (Sydney, 1997) ("Wood Report") at para 7.82.

53. Burrows at 1123.

response can be made. The use of surveillance for this purpose is rarely controversial, especially to monitor a crowd at large, or to home in on familiar troublespots. For example, computerised cameras using face recognition software installed at Manchester's Main Road football stadium scan the ground for known hooligans, identifiable even if disguised.[54]

Protection of personal safety and private property

1.33 Many businesses and residents use surveillance for personal and property protection. While such use is generally unobjectionable, especially when targeted against trespassers, the situation is less clear in the case of invited guests or employees, such as babysitters, who may be unaware that they are under surveillance.

Media interests

1.34 An important contribution that a free media can make to society lies in its ability to investigate subjects of public importance. The public interest may be well served by exposing, for example, fraudulent or corrupt practices by government or business. While such "scoops" are often the result of sensitive documents being leaked, sometimes they are the product of genuine investigative journalism. In recent years the practices engaged in by some branches of the media, especially the tabloid press, have come under greater public scrutiny.

---

54. J Robotham, "Weaving the Tangled Web" Sydney Morning Herald (16 December 1995, Spectrum) at 7. However, civil libertarians criticised the covert videotaping of football fans attending the Super Bowl in Tampa, Florida, in January 2001. The images captured were fed into computers which, in under a second, compared them with thousands of digital portraits of known criminals and suspected terrorists contained in a database assembled from law enforcement agency files: P Slevin, "Police Video Cameras Taped Football Fans: Super Bowl Surveillance Stirs Debate" Washington Post (1 February 2001) at A1.

Employer interests

1.35 Employers may install surveillance devices in shops and factories, in an effort to uncover theft and fraud on the part of both customers and employees.

EXISTING REGULATION OF SURVEILLANCE

New South Wales

1.36 The Listening Devices Act 1984 (NSW) ("LDA") prohibits the use of listening devices to record private conversations, except in the circumstances outlined by the Act, without the use of a warrant granted by a judge. To be authorised under the LDA, the piece of equipment used to conduct surveillance must fall within a category defined in the legislation. The legislation currently defines "listening device" 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.*[55]

1.37 The LDA was amended in 2000 to clarify that a listening device may also have a visual or tracking capacity.[56] *The definition does not cover computer or enhancement equipment.*

1.38 The Workplace Video Surveillance Act 1998 (NSW) regulates the use of video surveillance in the workplace. It defines video surveillance as surveillance by a closed-circuit television system or other electronic system for visual monitoring of activities on the workplace.[57] *It allows video surveillance in the workplace if the employee has been given prior written notice of the surveillance, the*

---

55. *LDA s 3(1).*
56. *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.*
57. *Workplace Video Surveillance Act 1998 (NSW) s 3.*

surveillance cameras are clearly visible and there are visible signs notifying people that they may be under surveillance.[58] Surveillance that does not satisfy these criteria is considered covert video surveillance under the Act and is unlawful, unless an authorisation has been issued be a magistrate.[59]

1.39 There are some legislative restrictions with respect to use of personal data. The Crimes Act 1900 (NSW) makes it an offence for a person to gain access to information stored in a computer.[60] The provisions in the Act have could be used to prosecute people who use data stored in computers for the purpose of monitoring individuals. The Privacy and Personal Information Act 1998 (NSW) introduces a set of principles that regulate the way public sector agencies should deal with personal information. The principles 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.

Commonwealth

1.40 The Telecommunications (Interception) Act 1979 (Cth) ("Interception Act") regulates the interception (listening to or recording) of a communication passing over a telecommunication system.[61] As well as applying to Commonwealth bodies, the Interception Act applies to New South Wales agencies using telephone interception devices to investigate offences under New South Wales law.[62] It has been held that the Interception Act "covers the

---

58. Workplace Video Surveillance Act 1998 (NSW) s 4.

59. Workplace Video Surveillance Act 1998 (NSW) Part 2 and 3.

60. Crimes Act 1900 (NSW) s 309, 310.

61. Telecommunications (Interception) Act 1979 (Cth) s 6(1). This legislation was enacted pursuant to the Commonwealth's power to regulate "postal, telegraphic, telephonic and other like services": Constitution (Cth) s 51(v).

62. See Telecommunications (Interception) Act 1979 (Cth) s 34;

field" so far as telephone interceptions are concerned, thus displacing, by virtue of section 109 of the Commonwealth Constitution, any state legislation purporting to regulate the same.[63] *Furthermore, certain Commonwealth laws regulate the use of listening devices by specific Commonwealth organisations, such as the Australian Federal Police, customs officials, and the Australian Security Intelligence Organisation (ASIO).*[64]

1.41 There are Commonwealth statutes that regulate the use of data that relates to individuals. The Commonwealth Privacy Act 1988 (Cth) lays down strict privacy principles which Commonwealth government agencies must observe when collecting, storing and using personal information.[65] *This Act and others*[66] *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.*[67] *The Crimes Act 1914*

Telecommunications (Interception) (New South Wales) Act 1987 (NSW).

63. *Edelsten v Investigating Committee of New South Wales (1986) 7 NSWLR 222 at 230; Miller v Miller (1978) 141 CLR 269.*
64. *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).*
65. *As of December 2001, certain private sector organisations will also be subject to privacy regulation courtesy of the Privacy Amendment (Private Sector) Act 2000 (Cth).*
66. *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).*
67. *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.*

(Cth) makes it an offence for a person to gain access or damage to information stored in a Commonwealth computer.[68] *The provisions in the Act, like their counterpart in the Crimes Act 1900 (NSW) could be used to prosecute persons who use data stored in (Commonwealth) computers for the purpose of monitoring individuals.*

Other Australian states and territories

1.42 Queensland, South Australia, Tasmania, and the Australian Capital Territory, like New South Wales, all have legislation that generally regulates only the use of listening devices.[69] *However, in 1997, Queensland enacted the Police Power and Responsibilities Act which regulates the use of a wider array of devices – listening, tracking and visual surveillance devices – by the police. This law does not cover the use of those devices by private individuals.*

1.43 Western Australia, Victoria and the Northern Territory have recently introduced legislation to regulate surveillance activity beyond the use of listening devices. The Surveillance Devices Act 1998 (WA) regulates listening devices, optical surveillance devices and tracking devices.[70] *The Act defines optical surveillance device as one that is capable of being used to record visually or observe a private activity and a tracking device as one that is capable of being used to determine the geographical location of a person or object.*[71] *The Surveillance Devices Act 1999 (Vic) 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.*[72] *The Surveillance Devices Act 2000 (NT) covers listening*

68. *See Crimes Act 1914 (Cth) Part VIA.*
69. *Invasion of Privacy Act 1971 (Qld) Part 4; Listening Devices Act 1972 (SA); Listening Devices Act 1991 (Tas); Listening Devices Act 1992 (ACT).*
70. *Surveillance Devices Act 1998 (WA) s 5-7.*
71. *Surveillance Devices Act 1998 (WA) s 3.*
72. *Surveillance Devices Act 1999 (Vic) s 3 and 9.*

devices, optical surveillance devices, tracking devices and data surveillance devices.[73]

1.44 The recent surveillance devices statutes in other Australian jurisdictions are all device-specific. By this we mean that they all specify the type of surveillance devices to which the legislation relates. They do not cover many types of device currently in use, such as laser, infra-red, satellite and thermal-imaging equipment, nor those that may be developed in the future. Moreover, these laws deal generally with the covert monitoring of private conversations and activities. They do not provide guidance for overt surveillance or surveillance conducted with the knowledge of the subject. The Commission discusses the drawbacks of this approach in Chapter 2.

The common law

1.45 There are laws generally applicable in New South Wales that may impact on surveillance. The laws of trespass, nuisance and defamation, while not specifically relating to electronic surveillance, may regulate activities associated with surveillance in certain circumstances and provide the subject of the surveillance with some redress. What follows is a brief survey of the relevant common law and an examination of its efficacy in regulating the use of surveillance devices.

Trespass

1.46 An action may lie for trespass to land, goods or to the person.[74] *Trespass to land occurs where a person directly, unlawfully and either intentionally or negligently, enters and/or remains on, or causes any physical matter to come into contact with, another person's land (in respect of which that person must be entitled to*

73. Surveillance Devices Act 2000 (NT) s 3 and 5.

74. Trespass to the person involves direct physical interference with another, such as assault or battery. Trespass to goods applies to a similar direct interference with property other than land or buildings. See R P Balkin and J L R Davis, Law of Torts (2nd ed, Butterworths, Canberra, 1996) at 35-58, 97-103; See also R P Handley, "Trespass to Land as a Remedy for Unlawful Intrusion on Privacy" (1988) 62 Australian Law Journal 216.

exclusive possession).[75] *An action for trespass may be available in relation to surveillance if, for example, a photographer climbed over a person's fence and hid in the garden, with the intention of capturing that person's movements on video camera. In such a case, trespass to land could be made out on the ground that the actions of the photographer intentionally and directly interfered with the owner's possession of his or her land.*[76] *The courts have shown an inclination to find trespass to land in cases where camera crews have entered premises illegally in order to obtain interviews and film footage.*[77]

Nuisance

1.47 The tort of private nuisance occurs where an occupier of land has his or her beneficial use and enjoyment of the land impeded by the actions of another person. Those actions must be substantial[78] *and unreasonable,*[79] *may be tangible or intangible*[80] *and must cause actual harm, which may include a disturbance to the occupier's comfort, health or convenience.*[81] *In certain circumstances,*

---

75. *Balkin and Davis at 114.*
76. *In Greig v Greig [1966] VR 376 at 380-381, Gillard J held that entering a house without consent to install a microphone in the chimney amounted to trespass to land.*
77. *See Lincoln Hunt Australia Pty Ltd v Willesee (1986) 4 NSWLR 457; Emcorp Pty Ltd v Australian Broadcasting Corporation [1988] 2 Qd R 169; Whiskisoda Pty Ltd v HSV Channel 7 Pty Ltd (Victoria, Supreme Court, McDonald J, 9417/93, 5 November 1993, unreported).*
78. *In Walter v Selfe (1851) 64 ER 849, Knight-Bruce VC noted that the interference with the occupier's enjoyment of his or her land must be "more than fanciful, more than one of mere delicacy or fastidiousness, as an inconvenience materially interfering with the ordinary comfort physically of human existence…": at 852.*
79. *In Sedleigh-Denfield v O'Callaghan [1940] 3 All ER 349, Lord Wright stated that it was "impossible to give any precise or universal formula [in relation to unreasonableness], but it may be broadly said that a useful test is perhaps what is reasonable according to the ordinary usages of mankind living in society.": at 364.*
80. *The loss of a night's sleep has been held to amount to nuisance: Munro v Southern Dairies Limited [1955] VLR 332 at 335.*
81. *See Balkin and Davis at 443-464. See also K Koomen, "Under Surveillance: Fergie, Photographers and Infringements on Freedom"*

surveillance activity may amount to nuisance. In Lord Bernstein v Skyviews and General Limited,[82] it was held that the taking of a single aerial photograph of a house from a plane did not amount to nuisance, as the interference with the owner's right to enjoy his land was not substantial. That case left open the potential, however, for constant aerial surveillance to be actionable as nuisance.[83] In Raciti v Hughes,[84] the complainant brought an action for nuisance in relation to a video surveillance security system that directly overlooked his yard, activating the camera and floodlights each time the complainant or one of his family entered the yard. This was held to constitute a private nuisance.

Defamation

1.48 A person who is the subject of surveillance activity may bring an action for defamation if material obtained from the surveillance is published and is considered to be damaging to that person's reputation.[85] It has been held that a nude photograph taken without the subject's knowledge or consent, which is subsequently published in a magazine and exposes that person to ridicule, is capable of being defamatory.[86]

(1993) 17 University of Queensland Law Journal 234 at 239-240.

82. *[1977] 2 All E R 902.*
83. *[1977] 2 All E R 902 at 909 (Griffiths J).*
84. *(NSW, Supreme Court, EQD 3667/95, 19 October 1995, unreported).*
85. *See Defamation Act 1974 (NSW) s 9.*
86. *Ettingshausen v Australian Consolidated Press Limited (1991) 23 NSWLR 443.*

Breach of confidence

1.49 In Creation Records Ltd v News Group Newspapers Ltd[87] *a photo shoot for the cover of pop group Oasis's new album took place around a hotel swimming pool. A photographer from The Sun newspaper, while lawfully at the scene as a hotel guest, took photos, one of which was similar to that chosen by the group for its album cover. This unauthorised photograph was published in The Sun and was the subject of a poster which the paper invited readers to purchase. The record company successfully argued that the photograph had been taken in breach of confidence, and was granted an interlocutory injunction restraining the paper from further publication of unauthorised photographs, damages being regarded as an inadequate remedy in this case. It was found that the circumstances of the shoot, eg the security measures imposed, made it arguable that it was intended to be confidential. The photographer had acted surreptitiously in taking the photographs, knowing that he would be allowed to remain at the scene only if he refrained from so doing.*

The general law is inadequate

1.50 The general laws described above may not offer adequate protection against the effects of unjustified surveillance, nor do they provide an effective regulatory structure for surveillance in circumstances where the use of surveillance might be justified.

1.51 Trespass to land is only actionable where there has been a direct interference with the plaintiff's land. There would be no trespass where a person becomes the subject of surveillance on land or in premises which he or she does not own or is not entitled to occupy exclusively.[88] *Similarly, it would not amount to trespass for a person to use a video camera with a telephoto lens to observe someone's movements from across the street, as there would be no interference with that person's land:*

> *When a person takes a photograph of someone else's yard, he does not have to go onto that yard, but by standing on a public street or on adjoining land, he permits light travelling from*

87. *[1997] TLR 221.*
88. *Handley at 221-222.*

> *objects on the yard being photographed to pass onto the film on his camera. This does not amount to any trespass either to land or to airspace.*[89]

1.52 As surveillance technology becomes increasingly sophisticated, it is conceivable that the opportunities for monitoring a person's movements without any direct interference with his or her land will escalate:

> *The advances in technology which now enable private behaviour to be recorded in the course of a trespass by way of photographs and film, combined with the evolution of a sophisticated and internationally linked media, have substantially changed the nature of privacy invasions and affronts to dignity involving trespass to land. The reluctance of the judiciary to prevent the publication of recorded material obtained in the course of a trespass indicates the failure of the tort to adapt to the realities of our technological age. As a result of this failure an individual's right to a degree of privacy when on private property, which the tort of trespass has traditionally protected, seems to have been lost to a bygone era.*[90]

1.53 So far as nuisance is concerned, a person who is subjected to surveillance may not have the requisite ownership or interest in the land upon which the surveillance occurred to be able to bring an action. Even if a person does own or occupy the land where the surveillance takes place, if the act constituting the surveillance is not considered to be substantial or unreasonable enough,[91] *it will not constitute a nuisance.*

1.54 An action for defamation will not arise unless the material is considered to be damaging to a person's reputation and it is published in some way. Consequently, a person would have no action in defamation against someone possessing a video tape or photograph that is embarrassing, but not defamatory, or which is

---

89. Bathurst City Council v Saban (1985) 2 NSWLR 704 at 706 (Young J).

90. Koomen at 238.

91. Such as the taking of a single photograph: Lord Bernstein v Skyviews and General Ltd [1977] 2 All ER 902.

defamatory but not published.[92] Even if the circumstances surrounding an act of surveillance satisfy the elements of defamation, there may be defences to that action which would defeat the plaintiff's claim. For example, the defendant publisher may assert that the published material is substantially true and is of public interest, in which case the defamation action will fail.[93] In recent times, the High Court has also developed what is known as the "public figure test" in relation to political officials, whereby an allegation of defamation can be defended successfully by reliance on an implied freedom of political communication in the Australian Constitution.[94] As a result, it has become harder for political figures to bring defamation actions.

1.55 Even if a breach of an as aspect of general law is proved, the remedies available may be unsatisfactory. Injunctions are available in relation to trespass and nuisance to prevent acts continuing. However, the standard for granting injunctions is quite high. In Lincoln Hunt Australia Pty Ltd v Willesee,[95] Justice Young refused to grant an injunction to prevent the televising of material obtained by a television crew after entering the plaintiff's premises without permission, on the ground that an injunction should only be granted if the circumstances would make the publication "unconscionable", by which he meant that the plaintiff would suffer "irreparable damage" if the injunction were not granted,[96] and "that the balance of convenience favours the granting of an injunction".[97] It is arguably quite difficult to demonstrate "irreparable damage". The court may also refuse an injunction if it considers damages to be a more appropriate remedy, although these may be difficult to

---

92. Publication is the communication of defamatory material concerning the plaintiff to some person other than the plaintiff: Consolidated Trust Co Ltd v Browne (1948) 49 SR (NSW); Toomey v Mirror Newspaper Ltd (1985) 1 NSWLR 173.

93. Defamation Act 1974 (NSW) s 15(2).

94. See Theophanous v Herald and Weekly Times Ltd (1994) 182 CLR 104, and Lange v Australian Broadcasting Corporation (1997) 148 ALR 96.

95. (1986) 4 NSWLR 457.

96. (1986) 4 NSWLR 457 at 464.

97. (1986) 4 NSWLR 457 at 464.

quantify. Damages will often be an inadequate remedy if lasting harm has been occasioned as a result of the surveillance.

1.56 The shortcomings in the existing laws as they relate to surveillance highlight the fact that they were meant to protect interests other than freedom from unwarranted surveillance. Nuisance and trespass, for example, are based in land ownership or right to occupation. Such actions only deal in a peripheral way with privacy issues.

The LDA is outdated

1.57 The equipment that is now available is considerably more sophisticated than it was when the LDA came into force in 1984. Many devices are capable of recording sound as well as visual images and other signals. Several submissions consider that the limited operation of the LDA is inadequate in the light of technology currently being used to monitor activity.[98] *It seems illogical that the use of some types of surveillance equipment is regulated while the use of others is not. The lack of comprehensive coverage of all surveillance equipment may result in uncertainty on the admissibility of evidence obtained through equipment other than listening devices. It has also been suggested that the fact that only some areas are the subject of legal regulation further undercuts the effectiveness of even those areas of regulation:*

> *Once one form is subject to legal regulation, failure to control other forms not only becomes morally indefensible, but also in practice undermines the protection granted. This arises from the simple behavioural prediction that, assuming equal effectiveness, measures that can be undertaken free of*

98. NSW Nurses' Association, Submission at 1; Price Waterhouse, Submission at 14, NSW *Council for Civil Liberties, Submission at 4; NSW Crime Commission (NSWCC), Independent Commission Against Corruption (ICAC), Police Integrity Commission (PIC) and National Crime Authority (NCA) ("Joint Law Enforcement Agencies"), Submission at 4; Privacy Committee of NSW, Submission at 28-29.*

> *oversight will be much more attractive to people doing the work than those which are subject to restriction or review.*[99]

1.58 The arguments for and against the comprehensive regulation of surveillance devices, and not just listening devices, are examined in greater detail in the next chapter.

THE STRUCTURE OF THIS PAPER

1.59 This paper is divided into three parts. Part 1 deals with the background to and objectives of the reference and with the fundamental principles that should govern the use of surveillance devices.

- *Chapter 2 outlines the broad scope and framework of the proposed surveillance legislation.*

Part 2 deals with overt surveillance.

- *Chapter 3 outlines the issues raised by the use of overt surveillance, and the arguments for and against its regulation.*
- *Chapter 4 sets out the proposed regulatory scheme for overt surveillance, which includes a set of basic principles that need to be observed in the overt use of surveillance devices.*

Part 3 deals with covert surveillance.

- *Chapter 5 examines the system of warrants that will allow law enforcement agencies to use surveillance devices covertly.*
- *Chapter 6 discusses the system of public interest authorisations that will allow individuals and organisations other than law enforcement agencies and employers to use surveillance devices covertly.*
- *Chapter 7 examines and makes recommendations on covert surveillance conducted in the employment context.*

---

99. L Lustgarten and I Leigh, In from the Cold: National Security and Parliamentary Democracy (Clarendon Press, Oxford, 1994) at 44.

Part 4 deals with the mechanisms for ensuring that those who use surveillance devices are accountable for their actions.

- *Chapter 8 looks at the reporting and record keeping requirements for covert surveillance, as well as the need for notice to be given to the surveillance subject.*
- *Chapter 9 examines the use of information obtained as a result of covert surveillance, such as the publication or communication of such information and its use as evidence in legal proceedings. It also looks at whether there should be obligations concerning storage and destruction of covert surveillance information.*
- *Chapter 10 makes recommendation on the complaints and review procedures for overt and covert surveillance. It also looks at the range of sanctions and remedies that should apply for breaches of the proposed legislation.*

2. Framework for a new surveillance law

The Commission's approach

Scope of the proposed legislation

Regulation of overt and covert surveillance

2.1 In Chapter 1, the Commission discusses the fragmented and inadequate nature of the current laws governing surveillance. This lack of adequate regulation has spurred momentum in many States and Territories for the introduction of more comprehensive surveillance legislation. Until recently, the law in each State and Territory governed only the use of listening devices. Since 1997, additional laws in some States have regulated the use of video cameras[1] and tracking devices[2] in limited circumstances. The latest legislative moves have been in Western Australia[3], Victoria[4] and the Northern Territory,[5] which have recently introduced surveillance devices laws covering listening, optical surveillance and tracking devices, and, in some cases, computer or data surveillance devices.[6] These laws deal generally with the covert monitoring of private conversations and activities.

2.2 This chapter presents a framework for the recommendations made throughout this Report which, if implemented, will provide New South Wales with an extremely comprehensive system of surveillance regulation. It recommends that surveillance and surveillance device be defined broadly to have maximum application to activities that may impinge on the privacy of others. Rather than targeting particular devices or activities, the legislation recommended by the Commission will provide a broad scheme of regulation to deal with both overt and covert surveillance, applying generally and more specifically in the context of employment.[7] The Commission recommends that surveillance should be considered to be overt when conducted with the knowledge of the subject, and should be regulated flexibly by eight

1. *See Workplace Video Surveillance Act 1998 (NSW); Police Powers and Responsibilities Act 1997 (Qld) Schedule 3.*
2. *Police Powers and Responsibilities Act 1997 (Qld) Schedule 3.*
3. *Surveillance Devices Act 1998 (WA).*
4. *Surveillance Devices Act 1999 (Vic).*
5. *Surveillance Devices Act 2000 (NT).*
6. *Surveillance Devices Act 2000 (NT). Computer surveillance is regulated by the Surveillance Devices Act 1999 (Vic) only when conducted by law enforcement officers: s 9.*
7. *The Commission explains what is meant by "employment context", "employer" and "employee" at para 2.108-2.113.*

legislative principles supplemented by Codes of Practice.[8] *Where surveillance is conducted covertly without the subject's knowledge, prior authorisation will be required.*[9] *The regulatory scheme recommended in this Report will apply to any person wishing to conduct overt or covert surveillance for any purpose, including law enforcement officers, private investigators, the media, retail traders or employers. It will cover the use of a CCTV camera in a service station through to the bugging of a politician's home by the police or an investigative journalist.*

2.3 The legislative framework recommended by the Commission differs from surveillance devices legislation in other Australian jurisdictions, both in scope and approach. Those differences, and the reasons for them, are highlighted in this chapter.

THE COMMISSION'S APPROACH

Privacy and surveillance

2.4 Most people, if asked to focus on the issue, would probably assert the importance of respect for personal privacy. In response to the question of whether surveillance technology should be used legitimately to deter crime or other anti-social behaviour and promote the public interest, the same number of people would probably answer in the affirmative. Initially, the Commission held the view that regulating surveillance would be an exercise in achieving a balance between protecting privacy and permitting surveillance for legitimate purposes. During the course of its research and enquiries, however, the Commission has developed the view that this balancing approach is inherently flawed.

---

8. *Only larger users of overt surveillance, such as retailers, need have a Code of Practice, although all users of overt surveillance must comply with the legislative principles in the proposed legislation: see para 2.86-2.87 and ch 3 and 4 regarding the regulation of overt surveillance.*
9. *See para 2.89-2.98 and ch 5, 6 and 7 regarding the authorisation procedures recommended for covert surveillance.*

2.5 True balance assumes equal weight on either side. In reality, however, this is not the case. The unprecedented development of surveillance technology, particularly in the last decade, has resulted in its increased availability and use (beyond those considered to be "traditional" users, such as law enforcement agencies). Surveillance devices are also becoming more sophisticated, making it possible to monitor, retain and match every detail of a person's life, down to his or her DNA profile, without the subject having the slightest awareness. The law has lagged behind this technological explosion, leaving most surveillance activity completely unregulated. The growth of the internet has taken the capacity to monitor and disseminate personal details to a new level. This convergence of events has come at a cost to personal privacy, tipping the scales so far in favour of surveillance that the concept of true balance is no longer possible, if indeed it ever was.[10]

2.6 Surveillance is undoubtedly gathering momentum. There are those who would argue that this indicates that public acceptance of surveillance has increased in inverse proportion to the diminished public perception of the importance of privacy: that even those against surveillance view it as a "necessary evil", and that the legislation should reflect this public acceptance. Pinning down public opinion or acceptance levels is at best, difficult, and at worst, can be dangerous. In many cases, the public has no choice but to accept that privacy has to some extent become a tradeable commodity.[11] *Further, the proliferation of surveillance and the corresponding lack of privacy has not happened because of public acceptance, but, as outlined above, because the availability of affordable technology and the lack of adequate regulation has allowed it to happen. Privacy, as a principle, and as a legislative touchstone, has not become less valuable simply because the means*

---

10. See discussion in D H Flaherty, "Controlling Surveillance: Can Privacy Protection Be Made Effective?" in Agre and Rotenberg (eds), Technology and Privacy: The New Landscape (Massachusetts Institute of Technology Press, 1997) at 167-190.

11. For example, it cannot be argued conclusively that people accept the presence of video surveillance cameras in service stations because they continue to buy petrol, since there is no alternative if one has to run a car.

for its easy violation exist.

2.7 In making recommendations for comprehensive proposed surveillance legislation, the Commission has taken the 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. This approach may be criticised by those who consider it to be too weighted towards privacy, or too restrictive.[12] *Given that most surveillance activity in New South Wales is currently unregulated, it is understandable that any curb on its use may be interpreted by some as unduly restrictive. Criticism may also come from those who consider the Commission's recommended regime to be too liberal in permitting surveillance to occur at all.*[13] *The Commission considers, however, that the recommendations in this Report represent the best way of giving effect to the two propositions mentioned at the start of this section: namely, facilitating and controlling legitimate surveillance within the over-arching consideration of respect for personal privacy.*

SCOPE OF THE PROPOSED LEGISLATION

2.8 This chapter contains the Commission's recommendations for wide-ranging surveillance laws covering all types of surveillance,[14] *regardless of who conducts it, whether it is conducted covertly or openly in public, or the type of device used. Definitions of surveillance, surveillance device, overt and covert surveillance are*

---

12. *The Commission notes in this regard the views of the Registered Clubs Association of NSW, Submission at 2-4; Publishing and Broadcasting Limited, Submission at 2; and Retail Traders' Association, Submission at 10-11.*
13. *See* NSW *Council for Civil Liberties, Submission at 1 and 5.*
14. *That is, all types of surveillance that New South Wales is constitutionally empowered to regulate: see para 2.46 concerning the Commonwealth's telecommunications powers and its impact on surveillance.*

set out below later in this chapter.[15] *Such a broad regulatory regime was not originally envisaged, and many other options were examined. After much research and consideration, however, the broad approach seemed the most effective way of achieving comprehensive privacy protection and flexible regulation of legitimate surveillance. Before launching into the detail of the recommended reforms, it may help to explain the reasoning process that led to the adoption of this approach.*

Background

2.9 The Commission's Terms of Reference require consideration of the current scope of the Listening Devices Act 1984 (NSW) ("LDA"), the need to regulate visual surveillance equipment, and any related matter. In considering the LDA, it became immediately clear that the legislation is deficient in at least the following two respects:

- *it fails to recognise other types of surveillance beyond the use of listening devices;*[16] *and*
- *it operates to prohibit covert or secretive surveillance, subject to exceptions, with no application to broader issues of overt surveillance.*

2.10 It was apparent that the LDA needed expanding and updating to reflect developments in surveillance technology: that it should include the use of audio, visual, audio-visual, tracking, computer equipment (and equipment to enhance the use of these), if used covertly to monitor the activity of a person, place or thing. This view was supported by the majority of submissions received by the Commission that responded on the question raised in the Issues Paper ("IP 12").[17] *Those against the extension of the LDA to cover*

---

15. See para 2.34-2.39, 2.78-79, 2.88.

16. Ch 1 outlines the current law and discusses its deficiencies.

17. New South Wales Law Reform Commission, Surveillance (Issues Paper 12, 1997) ("IP 12"). Submissions in support of a broad-based surveillance law included M L Sides, Submission at 17; Director of Public Prosecutions, Submission at 3-4 and 8; NSW Police Service,

other types of surveillance devices argued that it was unnecessary,[18] that the regime would be too restrictive,[19] or that the use of listening devices was more invasive of privacy than the use of other devices, and warranted separate regulation.[20] The Commission deals with these objections in more detail at paragraphs 2.15-2.19 below.

2.11 The visual surveillance element of the Terms of Reference required examination of issues beyond those which could be dealt with by expanding the LDA. Visual surveillance is used widely, with Closed Circuit Television ("CCTV") or security cameras in banks, railway stations, streets, shops and office buildings having become commonplace. Such use is usually visible and random, may be for purposes as diverse as crime prevention, public safety, or even employee monitoring, and, as noted in Chapter 1, is currently unregulated by law. It would not be appropriate or practical to regulate such use through a warrants system (as used in the LDA), since that presupposes an identifiable target and purpose. The options for dealing with such public or overt surveillance were, therefore, to leave it unregulated by legislation, to prohibit its use outright, or to develop a way to regulate it in a manner more flexible than that required for covert surveillance.

Special Services Group, Submission at 14; Price Waterhouse, Submission at 14; NSW Ombudsman, Submission at 3; NSW Young Lawyers Criminal Law Committee, Submission at 8; NSW Crime Commission (NSWCC), Independent Commission Against Corruption (ICAC), Police Integrity Commission (PIC) and National Crime Authority (NCA) ("Joint Law Enforcement Agencies"), Submission at 3-4; Privacy Committee of NSW, Submission at 11 and 28.

18. *Registered Clubs Association of NSW, Submission at 1 and 4.*
19. *Registered Clubs Association of NSW, Submission at 2-4; Publishing and Broadcasting Limited, Submission at 2; and Retail Traders' Association, Submission at 10-11.*
20. *Registered Clubs Association of NSW, Submission at 4; Law Society of NSW, Submission at 6.*

2.12 Recommending a complete prohibition of CCTV and other forms of overt visual surveillance would not only be unrealistic, but unsound given its potential benefit. Leaving it unregulated by legislation is problematic in that visual surveillance, even when conducted overtly, may still present a significant privacy threat and would leave those affected by breaches of privacy without a legal remedy.[21] *The Commission concluded that a new form of legislative regulation for overt surveillance was needed, and not just for visual surveillance. Overt surveillance may be conducted with devices apart from visual ones, just as covert surveillance involved the use of equipment other than listening devices.*

2.13 Therefore, the Commission developed the view that a dual system of legislative regulation should be developed:

- *one based on the warrants system in the LDA, but expanded to cover other devices, to regulate covert surveillance; and*
- *another, more flexible system to regulate the overt use of any surveillance device.*

2.14 Regulatory models in other jurisdictions were examined, particularly Victoria, Western Australia and the Northern Territory, which have replaced their LDAs with broader legislation covering some other surveillance devices. Despite these initiatives, no model covered the breadth of activity contemplated by the Commission. All existing legislative models are limited in scope in three main areas:

- *the type of devices covered;*
- *the type of activity covered; and*
- *the category of people who may conduct surveillance.*

These points are discussed and critiqued in turn.

---

21. See ch 3 for the Commission's discussion of why overt surveillance should be regulated.

Restricting the type of device

2.15 Apart from the LDA in New South Wales, other surveillance legislation covers listening devices,[22] video,[23] tracking[24] and computer or data surveillance devices,[25] or a combination of these, to varying degrees.[26] There can be little doubt that the use of these devices should be regulated to the same extent as listening devices. Listening devices are not inherently distinct from other forms of surveillance devices, nor do they pose a greater threat to privacy than other electronic devices with surveillance capabilities. Indeed, visual surveillance can be extremely invasive and can identify individuals more clearly than audio devices, leading to the comment in R v McNamara[27] that "the use of a video camera … is in some respects a more intrusive device than a sound transmitter".[28]

2.16 The major rationale for limiting the legislative scope to

---

22. *See eg, Listening Devices Act 1972 (SA); Listening Devices Act 1991 (Tas); Listening Devices Act 1992 (ACT); Invasion of Privacy Act 1971 (Qld); Surveillance Devices Act 1998 (WA); Surveillance Devices Act 1999 (Vic); Surveillance Devices Act 2000 (NT). See also Customs Act 1901 (Cth) s 219A-219K; Australian Federal Police Act 1979 (Cth) s 12B-12L; Australian Security Intelligence Organisation Act 1979 (Cth) s 26; Police Powers and Responsibilities Act 1997 (Qld).*
23. *See eg, Workplace Video Surveillance Act 1998 (NSW); Surveillance Devices Act 1998 (WA); Surveillance Devices Act 1999 (Vic); Surveillance Devices Act 2000 (NT); Australian Security Intelligence Organisation Act 1979 (Cth) s 26(1); Police Powers and Responsibilities Act 1997 (Qld) Sch 3.*
24. *See eg, Australian Security Intelligence Organisation Act 1979 (Cth) s 26A; Police Powers and Responsibilities Act 1997 (Qld); Surveillance Devices Act 1998 (WA); Surveillance Devices Act 1999 (Vic); Surveillance Devices Act 2000 (NT).*
25. *See eg, Australian Security Intelligence Organisation Act 1979 (Cth) s 25 and 25A; Surveillance Devices Act 1999 (Vic) (but only in relation to law enforcement officers: s 9); Surveillance Devices Act 2000 (NT).*
26. *See para 1.36-1.56 for an overview of the current surveillance laws in Australia.*
27. *[1995] 1 VR 263.*
28. *R v McNamara [1995] 1 VR 263 at 271.*

specific, identifiable devices would appear to be that it brings an element of certainty to the regulatory scheme. In an era where it is impossible to identify with any accuracy the nature and capacity of surveillance devices currently in use, let alone anticipate future developments, it is tempting to limit legislation to cover only those devices which are considered familiar. The Commission considers that while certainty is a desirable goal for legislation, surveillance presents such a threat to privacy, and is in such widespread use, that its effective regulation should not be compromised for the sake of certainty alone.

2.17 Technology has developed to such an extent that an individual's privacy may be invaded through the use of computer, digital, laser, infra-red and satellite equipment to the same, or greater, extent as through the use of video or sound equipment. It seems as illogical to exclude such devices from the scope of the legislation as it does to restrict legislation to listening devices alone. The LDA was technologically obsolete almost from the moment it was enacted. Any device-specific surveillance legislation will meet the same fate and require constant updating as technological developments inevitably outpace the law. Furthermore, the arbitrary regulation of particular devices will lead to the same gaps and anomalies that characterise the LDA.[29] *Why should surveillance conducted with a video camera or a tracking device be regulated when surveillance conducted by thermal-imaging equipment has no controls placed upon it? The Commission can find no valid policy rationale for drawing such a distinction. A breach of privacy occasioned through the use of a surveillance device has occurred in both cases.*

2.18 Globalisation and convergence of technology further erode the effectiveness of device-specific legislation in preventing privacy

---

29. See 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" in the LDA. That decision resulted in the LDA being amended to clarify that a listening device could have other capacities: see Listening Devices Act 1984 (NSW) s 3(1A).

breaches.[30] Globalisation and convergence refer to the interlinking of device capacities, enabling recordings, images or data obtained in one form to be transmitted or transformed into another. Both of these factors, enhanced significantly by the boom in internet use, have removed the technological barriers between surveillance devices and the international flow of information obtained as a result of their use. It is possible to record an activity with a video camera, for example, and display the results on a website which may be accessed by millions of people worldwide. From there, the images could be downloaded to a computer database and stored, or matched electronically with other information to form a profile of the subject of the initial surveillance. Another possibility is that a remote scanning device could be used to read the electromagnetic radiation emitted by the computer screen and convert it back to its original form.[31] In this example, controlling the use of video cameras but not computer or scanning equipment, would not represent sufficient privacy protection or adequate regulation of surveillance devices.

2.19 Ultimately, surveillance and the use of surveillance devices defies technical limitations and makes precise delineation impossible. It is for this reason that any attempt to regulate it through legislation limited to a few devices will inevitably be ineffectual. Consequently, the Commission recommends a broad definition that is not device-specific and which encompasses any equipment which is being used to conduct surveillance.

---

30. These factors are discussed as significant threats to privacy in D Banisar and S Davies, "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments" (1999) 18(1) John Marshall Journal of Computer and Information Law 1 at 5. See also «www.gilc.org/privacy/survey/intro.html».

31. This technology is known as Transient Electromagnetic Pulse Emanation Surveillance Technology (TEMPEST): see P N Grabosky and R G Smith, Crime in the Digital Age (The Federation Press, Sydney, 1998) at 38. Monitoring packages called "Screen to Screen" also allow network administrators to monitor computer screens remotely: S Hayes, "School accused of using 'spy' software" The Australian (Tuesday, 8 August 2000) at 39.

The recommended definitions of surveillance and surveillance device are discussed below at paragraph 2.33-2.39.

Restricting the type of activity covered

The public/private distinction

2.20 There is a view that in regulating surveillance, a distinction should be made between surveillance of activity in private and public places.[32] According to this view, surveillance in a public place should not be regulated because individuals do not have a reasonable expectation of privacy in such a place. It is said, for example, that if a person can overhear the conversation or observe the activities of another person in a public place, it would be unrealistic to require a person listening to the same conversation or observing the same activity to obtain prior authority to monitor it electronically.[33] The Australian Law Reform Commission ("ALRC"), in its report on privacy, took the position that it is neither desirable nor feasible to regulate the use of surveillance or recording by means of optical devices in streets, parks and other such public places. The Report stated that people in a public place "must anticipate that they may be seen, and perhaps recorded, and must modify their behaviour accordingly".[34]

2.21 All legislative models examined by the Commission, including the current LDA in New South Wales, reflect this thinking in regulating only private conversations or activity. The core elements of the definition of private conversation and private activity are similar across jurisdictions, with minor variations. Generally, a private conversation or activity is defined

---

32. See M Colvin, Under Surveillance: covert policing and human rights standards (Justice, London, 1998) at 33.

33. J Broome, "Electronic Surveillance in Criminal Investigations: Balancing Law Enforcement with Civil Liberties" in Electronic Surveillance in Criminal Investigations: Balancing Law Enforcement with Civil Liberties (Institute of Criminology, Sydney, 1998) at 64 and 68.

34. Australian Law Reform Commission, Privacy (Report 22, 1983) Vol 2 at para 1185.

as one in which the parties reasonably expect, or is conducted in circumstances which may reasonably indicate, that the conversation or activity should be listened to or observed only by themselves.[35] *In addition, other legislation provides that a private conversation or activity is not one made in any circumstances in which the parties to it ought reasonably expect that it may be overheard (or observed) by someone else.*[36]

2.22 There are a number of difficulties with regulating only activity considered to be private or not conducted in a public place. First, determining exactly what a public place is can be a difficult exercise. Many places to which the public has free or conditional access are privately owned, or may have private areas within them, and may also be workplaces. This lack of clarity in determining the difference between a public and a private place may result in rather arbitrary delineations. An interesting example of a Code of Practice from the United Kingdom states that "public place" includes shopping centres, football fields, public houses, highways, parks and railway stations, and may extend to private land capable of being seen or overheard by the general public (such as front or back gardens or driveways).[37] *In New South Wales, a conversation between parties to litigation held in a private room in a court house was not considered to be "private" within the meaning of the LDA.*[38] *Conversely, but also in New South Wales, it was held that a conversation taking place in an office did not cease to be private because the door to the office was open and a passer-by may have*

35. *LDA s 3; Listening Devices Act 1972 (SA) s 3; Listening Devices Act 1992 (ACT) s 3; Listening Devices Act 1991 (Tas) s 3.*
36. *See eg, Invasion of Privacy Act 1971 (Qld) s 4; Surveillance Devices Act 1998 (WA) s 3; Surveillance Devices Act 1999 (Vic) s 3; Surveillance Devices Act 2000 (NT) s 3.*
37. *UK Code of Practice on Covert Surveillance undertaken by the National Crime Squad, the Scottish Crime Squad, The National Criminal Intelligence Service and Her Majesty's Customs and Excise (Note 1B).*
38. *Bedford v Bedford – Estate of Bedford (NSW, Supreme Court, BC 9805427, Windeyer J, 28-29 September 1998 and 20 October 1998, unreported).*

been able to overhear.[39] Consequently, public areas can be private and private areas can be public.

2.23 The concept of "private" areas is also becoming less meaningful as the traditional line between public and private space diminishes with technological advances. With the proliferation of CCTV and other types of "public" surveillance, intrusions into what used to be considered private spheres have become greater. The emergence of the internet and the consequent surveillance of web-sites and e-mails has raised new issues as to what, if anything, can be considered private in cyberspace.[40] Yet, as noted at paragraph 2.6 above, the fact that increasingly more surveillance is happening does not necessarily mean that this should dictate legislative policy.

2.24 It is similarly difficult to establish satisfactorily when a person "ought reasonably to expect" that a conversation or activity might be overheard or observed by another. One view is that one ought to expect that any activity or conversation outside the home or outside a closed office may be overheard or observed. This view lacks credence in today's society where, increasingly, business and personal dealings, which the parties would prefer to be kept to themselves, are conducted in public places such as restaurants, cafes, airport lounges and shops. In the United States, courts have held that people are reasonably entitled to expect a degree of privacy even in public places such as telephone booths[41] and public toilets.[42]

---

39. Miller v TCN Channel Nine (1988) 36 A Crim R 92 at 106 (Finlay J).

40. See J Rosen, "The Eroded Self" New York Times Magazine (30 April 2000) at 47. See also J Rosen, The Unwanted Gaze: The Destruction of Privacy in America (Random House, New York, 2000).

41. In the landmark ruling in Katz v United States 389 US 347 (1967), the US Supreme Court ruled that the covert use of a listening device in a public telephone booth infringed the appellant's reasonable expectation of privacy and constituted an "unreasonable search" within the meaning of the Fourth Amendment to the United States Constitution. The Court declared: "[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

In contrast, in a recent Australian case, a conversation held in an open area of a bridal shop was not considered to be private under the previous Victorian LDA[43] because the parties "ought reasonably" to have expected that they would be overheard by others.[44] In giving judgment, Justice Crispin described the behaviour of the defendants, in covertly recording the conversation and broadcasting it on national television, to be "generally reprehensible", yet the conduct was not regulated by the LDA, and consequently no relief was available under that Act.

2.25 In Victoria, legislators have attempted to introduce more certainty as to what activity is or is not covered by the Surveillance Devices Act 1999 (Vic) ("Victorian Act"). The Victorian Act states that activity is not private, and therefore not regulated by the Act, if it occurs "outside a building".[45] A possible rationale for such a provision may be that people should accept that activities conducted in the open are more susceptible to being observed by others than those conducted indoors. The Commission is of the view that this approach is unduly arbitrary and leaves a significant amount of invasive activity unregulated.[46] For example, why would activity conducted on a deserted beach be considered to be more public, and therefore open to unregulated visual surveillance, than the same activity conducted in a crowded movie theatre or restaurant? In the Second Reading Debate on the Bill, the point was made that video surveillance from a private home of people picnicking on a public

---

42. *See discussion in J R Scharrer, "Covert Electronic Surveillance of Public Rest Rooms: Privacy in the Common Area?" (1989) 6 Cooley Law Review 483.*
43. *Which contained a definition of private conversation identical to that in the Surveillance Devices Act 1999 (Vic).*
44. *Steiner Wilson & Webster Pty Ltd trading as Abbey Bridal v Amalgamated Television Services Pty Ltd (ACTSC, SC 717 of 1994, Crispin J, 18 November 1999).*
45. *A building is defined as "any structure": Surveillance Devices Act 1999 (Vic) s 3.*
46. *One commentator notes in relation to the Victorian Act that the "level of comfort afforded to citizens who fear an invasion of privacy is not as great as some might have argued for": J Cooper and A Goodvach, "Employment law" (May 1999) 51(4) Australian Company Secretary 184 at 186.*

beach is inappropriate and "un-Australian".[47] Yet, such behaviour would not be prohibited under the Victorian Act. Nor would the intrusive photographs taken of former Senator Bob Woods engaged in a painful and personal conversation with his wife in the backyard of the couple's home.[48]

2.26 The Commission is of the view, therefore, that surveillance legislation which includes in its scope only activity that is considered to be private, is weak and unsound in policy and practice. It leaves too much potentially inappropriate activity unregulated and provides insufficient privacy protection.[49] Apart from the difficulties outlined in the paragraphs above, such an approach is based on the flawed assumption that a person's legitimate expectation of privacy and freedom from surveillance depends on where they happen to be at any given time. Privacy is a personal, not a property interest,[50] and should not diminish because a person is in a public place.

2.27 The Commission's recommendations on the scope of surveillance activity that should be regulated, differ from other surveillance legislation in two major respects. First, the public/private distinction is rejected for the reasons outlined above. Instead, the Commission considers that a more relevant distinction is whether the surveillance is conducted with (overtly) or without (covertly) the knowledge of the subject of the surveillance.[51] The second respect in

---

47. Victoria, Parliamentary Debates (Hansard) Legislative Assembly, 29 April 1999 at 552.

48. The photographs were printed in the Daily Telegraph (Friday, 7 February 1997). The Australian Press Council ruled that the photographs were in breach of its Statement of Principles regarding the privacy of individuals and not justified in the public interest: see Adjudication No 916 (April 1997).

49. See S Davies, "Privacy and Surveillance: The Surveillance Devices Act 1998" 27(1) Brief (February 2000) at 11. Davies notes that the largest gap in the Western Australian Act is that it only regulates private activity.

50. See Privacy Committee of NSW, Submission at 10-11.

51. The definitions of overt and covert surveillance and the system of regulation the Commission recommends for each are discussed at para 2.77-2.98.

which the recommendations in this Report differ in approach from that taken in existing surveillance legislation is that overt surveillance is included in the regulatory scheme.

Restricting who may conduct surveillance

2.28 Some surveillance legislation applies only to particular categories of people,[52] or restricts the category of people who may apply for a warrant to conduct covert surveillance.[53] The main category of people to whom surveillance is restricted in this way is law enforcement agencies. Some legislation also contains provisions allowing parties to a conversation or activity to monitor or record that conversation or activity, while prohibiting non-parties to conduct such surveillance. This is known as participant monitoring, and is discussed at paragraphs 2.99-2.107.

Some legislation limited to law enforcement agencies

2.29 The New South Wales LDA is not limited to law enforcement agencies, but members of such agencies are the only people recorded as applying for warrants.[54] There are a number of possible explanations for this, without assuming that surveillance activity is relevant only to law enforcement agencies. It is possible that others are using equipment apart from listening devices (for example, most private investigators use visual surveillance equipment) or it could be that listening devices are being used illegally.

---

52. *See eg, Customs Act 1901 (Cth); Australian Federal Police Act 1979 (Cth); Australian Security Intelligence Organisation Act 1979 (Cth); Casino Control Act 1992 (NSW); Police Powers and Responsibilities Act 1997 (Qld).*
53. *See eg, Invasion of Privacy Act 1971 (Qld) s 43 (2)(c)(i); Listening Devices Act 1972 (SA); Listening Devices Act 1991 (Tas); Surveillance Devices Act 1999 (Vic). The Surveillance Devices Act 2000 (NT) extends the category of persons who may apply for a warrant to those assisting or providing technical expertise to law enforcement officers: s 33.*
54. *See JW Shaw QC, Report by the Attorney General of New South Wales pursuant to section 23 of the Listening Devices Act 1984 for the year ended 31 December 1998 at (i). These are the latest figures available.*

2.30 Any new legislation that deals with all types of surveillance and surveillance devices will, therefore, impinge upon activity like that undertaken by private investigators or the media, unless the scope of the legislation is restricted to exclude this type of surveillance. As the Commission has shown, other jurisdictions, such as Victoria, provide only for law enforcement agencies to obtain warrants to conduct covert surveillance, and exempt from the scope of the legislation any activity conducted "outside a building".[55] *Consequently, law enforcement agencies must obtain a warrant in Victoria to conduct covert surveillance inside a building, whereas the media or a private investigator may conduct the same surveillance, equally covert and equally invasive of individual privacy, provided the activity in question occurs "outside".*

2.31 This example illustrates that, for the same reasons the Commission considers it arbitrary and artificial to regulate only certain types of surveillance activity, it is also inappropriately selective to regulate surveillance conducted only by particular categories of people. Surveillance is undoubtedly a beneficial crime-fighting tool, and surveillance legislation should facilitate its effective use by law enforcement agencies. Surveillance is not, however, the sole domain of law enforcement. Apart from creating anomalies, limiting regulation in this way could lead to surveillance work traditionally undertaken by law enforcement agencies being conducted by, or even out-sourced, to private investigators to avoid the legislative restrictions placed on enforcement agencies.[56]

2.32 In making recommendations for surveillance legislation, the Commission's main focus is on protecting privacy, and enabling surveillance to occur in circumstances where a breach of privacy is justified. In accordance with this view, the potential for privacy invasion through the use of surveillance equipment is the same

---

55. Surveillance Devices Act 1999 (Vic) s 3. See para 2.25.

56. Private investigators are already undertaking surveillance into matters traditionally investigated by police, due to the resource and time pressures experienced by police: see D Turner, "Out in the Cold" The Weekend Australian (4 October 1997) at 33; B Kucera, "Outsourcing the Nation's Policing – Business Opportunities for the Private Sector" 35(5) The Agent (Institute of Mercantile Agents Ltd, May 2000) at 6.

regardless of who is using the equipment. Surveillance legislation should, therefore, apply to every person or agency conducting surveillance. There may need to be different approaches to the way that surveillance is regulated depending on who is conducting it or the purpose for which it is being conducted. With regard to overt surveillance, different agencies or organisations will have their own Codes of Practice, based on principles set out in the legislation, to accommodate their particular needs.[57] *With covert surveillance, the Commission has developed three slightly different, but complementary, approaches to regulating surveillance depending on whether it is conducted by law enforcement agencies, in the public interest or in an employment context.*[58]

Definitions

2.33 For the reasons set out in the paragraphs above, the Commission recommends the introduction of broad, flexible legislation to regulate surveillance, both overt and covert, through the use of any surveillance device, regardless of who conducts it or the activity being observed. The recommended legislative definitions of surveillance device and surveillance follow.

Surveillance device

2.34 To satisfy the approach advocated by the Commission, the definition of surveillance device for the purpose of the proposed legislation must not be technology specific, but must be broad enough to cover all of the equipment that could conceivably be used to conduct surveillance now and in the future. The Commission is of the view that a list of technology would result in debates over whether a particular device falls within the ambit of the law,[59] *and could render the legislation obsolete as new technology emerges.*

---

57. See para 2.78-2.87 and ch 3 and 4.

58. See para 2.88-2.89 and ch 5, 6 and 7, respectively.

59. This type of debate has characterised the LDA in NSW and other jurisdictions, with litigation on whether equipment is a listening device for the purpose of the legislation: see R v McNamara [1995] 1 VR 263; and R v Peter Kay and Roula Kay (District Court of NSW, Viney J, 22 October 1999, unreported).

Nor, in the Commission's view, should the definition be limited only to electronic devices, as was suggested to the Commission.[60] While it is tempting to see surveillance devices in terms of highly technical electronic equipment, surveillance may be conducted through the use of other equipment which may best be described as electro-magnetic, acoustic, mechanical, etc. Spying on the activity of another may be conducted by a global positioning tracking device or a telescope.

2.35 In seeking a comprehensive definition of surveillance device, definitions in other legislation were examined. Given that most surveillance legislation is device-specific, their definitions are not completely relevant to the open-ended approach recommended in this Report. However, they provide a useful starting point. The common element in most definitions is the reference to a surveillance device as any "instrument, device or equipment" capable of being used either "alone or in conjunction with any other instrument, device or equipment" to record or monitor words, and in some cases, images.[61] This form of words is attractive in that it is not limited to devices of any particular type or nature (for example, electronic, mechanical, visual, etc), and includes devices with multiple capacities. It also covers equipment used to enhance the effectiveness of other surveillance devices, such as amplification equipment.

2.36 The key factor for the Commission in defining a surveillance device is not the nature or quality of the device itself, but the fact that it may be used for the purpose of conducting surveillance. The definition of surveillance device should therefore be linked to and dependent on the definition of surveillance, which is discussed in the section below. For example, medical imaging equipment, such as ultrasound and x-ray technology, is technically a surveillance device. Where, it is being used purely for diagnostic purposes and not for "surveillance" (according to the Commission's recommended definition), the use of such equipment would not be regulated by the

---

60. Director of Public Prosecutions, Submission at 3-4; Joint Law Enforcement Agencies, Submission at 3-4.

61. See eg Customs Act 1901 (Cth) s 219A(1); Australian Security Intelligence Organisation Act 1979 (Cth) s 22; Drugs Misuse Act 1986 (Qld) s 25.

proposed surveillance legislation.[62] *To take another example, a video camera will only be a surveillance device for the purpose of the proposed legislation where it is being used intentionally to monitor a person's activity in order to uncover information about that person.*[63] *It will not be a surveillance device under the proposed legislation where it is used to record a family picnic. Similarly, hearing aids used by a hearing-impaired person to raise hearing to a level considered to be normal will not be caught by the proposed legislation.*[64] *Where, however, a hearing aid is used to enhance hearing to a better than normal level for the purpose of eavesdropping, then it would be a surveillance device for the purpose of the proposed legislation.*[65]

Recommendation 1

The proposed Surveillance Act should define "surveillance device" to mean any instrument, apparatus or equipment used either alone, or in conjunction with other equipment, which is being used to conduct surveillance.

Surveillance

2.37 One of the most difficult tasks confronting the Commission during this inquiry has been formulating a precise definition of surveillance. While it is a commonly used and accepted term, surveillance is also an extremely nebulous concept.[66] *As such, it*

62. *See ch 4 for further discussion on this point.*
63. *See para 2.37-2.39 for the definition of surveillance.*
64. *See LDA s 3(2); Surveillance Devices Act 2000 (NT) s 3.*
65. *See eg Surveillance Devices Act 1998 (WA) s 3; Surveillance Devices Act 1999 (Vic) s 3; Criminal Code (Canada) 1985 s 183.*
66. *In the course of its inquiry, the Commission has uncovered definitions of surveillance used for various purposes. For example, surveillance in the context of military intelligence may be defined as the "continuous systematic watch over the battlefield area to provide timely information for combat intelligence": see M A Richardson, I C Luckraft, R S Picton, A L Rodgers and R F Powell, Surveillance and*

defies precise definition. Perhaps this is why the Commission has been unable to find a suitable definition of surveillance in any of the legislative models it examined. As noted in paragraph 2.36 above, however, a definition of surveillance, which complements and is dependent on the definition of surveillance device, needs to be formulated to help clarify the scope of the proposed legislation.[67] *The LDA does not define surveillance by means of a listening device. It prohibits the use of a listening device to "record or listen to" private conversations.*[68] *This is similar to equivalent legislation in other States and Territories,*[69] *and to Commonwealth legislation.*[70]

2.38 Breaking the concept down to its elements, it is apparent that

---

Target Acquisition Systems (Brassey's, UK, 1997).

67. *The majority of submissions received by the Commission that commented on this point considered that the proposed legislation should contain a broad definition of surveillance: see M L Sides, Submission at 9-10; Director of Public Prosecutions, Submission at 3-4; Price Waterhouse, Submission at 7; NSW Young Lawyers Criminal Law Committee, Submission at 3; Joint Law Enforcement Agencies, Submission at 4; Privacy Committee of NSW, Submission at 11 and 28-29. Of the submissions that opposed a definition, most did so because they were opposed to extending the scope of the LDA to include other surveillance devices: see Insurance Council of Australia Limited, Submission at 2; Registered Clubs Association of NSW, Submission at 4; Law Society of NSW, Submission at 2. The Commission dealt with this argument at para 2.15-2.19 above.*
68. *"Listen to" is defined to include "hear": LDA s 3(1).*
69. *Legislation in other States refers to a device used to "overhear, record, monitor or listen to a private conversation": Invasion of Privacy Act 1971 (Qld) s 4; Listening Devices Act 1972 (SA) s 3; Listening Devices Act 1991 (Tas) s 3; Listening Devices Act 1992 (ACT) s 2; Surveillance Devices Act 1998 (WA) s 3; Surveillance Devices Act 1999 (Vic) s 3; Surveillance Devices Act 2000 (NT) s 3.*
70. *Commonwealth legislation refers to "listening to or recording, by any means" of a communication "in its passage over [the] telecommunications system": Telecommunications (Interception) Act 1979 (Cth) s 6(1); "listening to or recording words, images, sounds or signals being communicated by another person": Australian Security Intelligence Organisation Act 1979 (Cth) s 26(1); "listening to or recording words while they are being spoken by a person": Australian Federal Police Act 1979 (Cth) s 12F and Customs Act 1901 (Cth) s 219B.*

surveillance involves using a surveillance device to monitor, either through listening to, watching, or collecting data (in whatever form) about, people, places or objects. It may or may not involve the recording of the conversation, activity or information monitored. Surveillance may be directed at a particular target or may be random, but is always a deliberate or intentional act of monitoring conducted for the purpose of acquiring information about the subject of the surveillance. It may be conducted with or without the knowledge of the subject. The information obtained may relate to the physical or genetic characteristics, behaviour or activity of a person, the whereabouts of a person or an object, or the compiling of a personal or consumer profile based on all of the above.

2.39 Surveillance is sometimes limited to "real time" activity, that is, activity that occurs simultaneously with the monitoring. For example, the LDA defines a listening or surveillance device in terms of its ability to listen to or record a conversation or activity "simultaneously with its taking place". The effect of including such a limitation in the proposed legislation would be that the use of a device to read or record material stored on a computer database, including e-mail stored in the mail box of the sender or recipient, would be excluded from the scope of the legislation and therefore unregulated.[71] *The Commission considers the limitation of surveillance to "real time" activity difficult to justify from a policy perspective. It is hard to see why the use of a surveillance device, such as a computer, to monitor stored data to uncover information about a person should be unregulated simply because the information had been entered into the computer's database prior to the monitoring occurring. Monitoring of stored material may be just as intrusive on individual privacy as observing or recording real time activity, and therefore, in accordance with the Commission's emphasis on privacy as the basis of the proposed legislation, should be included in the definition of surveillance.*

---

71. See para 2.43-2.53 and 2.68-2.76 for the Commission's recommendations concerning surveillance of e-mail and data protection issues.

Recommendation 2

The proposed Surveillance Act should define "surveillance" 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.

Recommendation 3

The proposed Surveillance Act should define "monitor" (as used in the definition of surveillance) 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.

What activity is covered by the definitions?

2.40 The advantages of the broad, inclusive approach recommended by the Commission include the elimination of the arbitrary gaps and regulatory anomalies discussed in this chapter, and the extension of privacy protection to as wide a range of activity as reasonably possible. The proposed approach provides those conducting surveillance with the security of knowing that they are acting within the law, and affords those who may be adversely affected by unlawful surveillance with an avenue of redress. The major disadvantage with this approach, however, is that it lacks a degree of certainty. As the Commission has pointed out, the very nature of surveillance is that it is uncertain and limitless. It is impossible, for example, to state exactly what type of device is included or excluded from the scope of the legislation. The important factor will be whether the use of any device amounts to surveillance as defined by the legislation.

2.41 Taking a broad legislative approach also means that the outer

scope of the Commission's recommendations blend into other regulatory regimes. For example, in regulating computer surveillance of stored e-mail and other material, the proposed surveillance legislation will complement the Telecommunications (Interception) Act 1979 (Cth) ("Interception Act") (since most e-mail travels along telephone lines),[72] the Privacy Act 1988 (Cth),[73] and the Privacy and Personal Information Protection Act 1998 (NSW) (as the line between data surveillance and data protection is blurred).[74] At first, the Commission viewed the hazy delineation between these regimes as a problem, and investigated ways to clarify the regulatory boundaries. Any attempt at clarification, however, resulted in the same arbitrariness which we have been at pains to avoid. The Commission considers that the surveillance, privacy and telecommunications regimes, while not duplicating one another, should link together to form a web of privacy laws to guard against activity falling through gaps between the laws.

2.42 Basically, therefore, all activity that meets the definitions of surveillance and surveillance device will fall within the ambit of the proposed legislation, unless specifically excluded. The following discussion expands on the areas of potential overlap already mentioned between surveillance and other regimes, and highlights two areas to be included within the scope of the proposed legislation which some may find controversial: surveillance in private homes and surveillance by the media.

The internet and e-mail

2.43 It is not an overstatement to say that the rise of the internet and the boom in e-mail traffic over the past decade has been something of a communications revolution, particularly in the workplace. Being an international network of interconnected computers, it is the most effective means of sending information to a large number of people at once. It is this interconnectedness which presents the greatest opportunity for surveillance and threat to privacy. Until recently, e-mail systems generated the illusion of

---

72. Not all e-mail travels along telephone lines: see footnote 90.

73. And also the Privacy Amendment (Private Sector) Act 2000 (Cth).

74. See para 2.68-2.76 for the Commission's recommendations concerning surveillance and data protection.

privacy. E-mail users often require a password to access their e-mail account. Messages appear to have no permanent existence unless they are printed out because the user has the option of deleting them from their computer. This apparent privacy can cause e-mail users to correspond in a manner more frank or personal than would be the case in a traditional letter.[75]

2.44 The assumption of internet and e-mail privacy has been shattered with the growing awareness that the very technology making communication easier is also making it easier to spy on personal communications.[76] *For example, "cookies" located on web servers may trace the web sites that a user has visited.*[77] *Other technology includes a "beacon" placed inside a target computer which "emits a signal whenever the user logs on to the internet", alerting the person conducting the monitoring and allowing him or her to "enter the computer's hard drive for as long as the user stays*

---

75. *See A Carson and D Farrant, "Saving Private E-mail" The Age (4 March 2000) at 3. This cites Margaret Jackson, Dean of Business at RMIT, as saying: "E-mail seems to have brought down people's personal inhibitions about how they communicate." See also K Davey, "Privacy Protection for Internet E-mail in Australia: Part 1" (1997) 33 Computers and the Law 7 at 10.*

76. *See eg, K Davey, "Privacy Protection For Internet E-mail in Australia: Part 2" (1997) 34 Computers and the Law 8 at 8; M Peyser & S Rhodes, "When E-mail is Oops-Mail" The Bulletin (17 October 1995) at 72; S D Balz and O Hance, "Privacy and the Internet: Intrusion, Surveillance and Personal Data" (1996) 10(2) International Review of Law, Computers and Technology 219 at 222; K Needham, "Your Secrets Are Out – The Snoops Are About" Sydney Morning Herald (10 October 1998); M Hudson, "Virtual Privacy: The Impact of Electronic Technology on Communications" (1998) 3(1) Media and Arts Law Review 18 at 19.*

77. *A cookie is a unique identifier that a web server places on a computer. It enables website hosts to identify people "hitting" their sites, and to exchange information with other sites visited by the same people or with companies that advertise on those sites: L Eichelberger, "The Cookie Controversy" «www.cookiecentral.com/ccstory/cc6.htm» at 1. See also J Kang, "Information Privacy in Cyberspace Transactions" (1998) 50 Stanford Law Review 1193 at 1227-1230.*

on-line".[78] In the United States, the Federal Bureau of Investigation uses a computer system, known as "Carnivore", capable of collecting e-mail and other cyber data by hooking on to the server of an Internet Service Provider.[79] Perhaps the most disturbing recent development has been a survey of employers which revealed that seventy-five per cent of Australian companies periodically monitor their employees' e-mails, usually by covert surveillance.[80] E-mail may not only be read while stored in a computer or on a server, but may be retrieved even if it has been deleted.[81]

78. *ASIO apparently uses this technology to access computers pursuant to the Australian Security Intelligence Organisation Act 1979 (Cth) s 25(5) and 25A: see A West, "The spy who bugged me" Sun-Herald (6 February 2000) at 41. These "beacons" are similar to "trojan horses", which sit in computers and send copies of every activity recorded to a computer hacker: D Braue, "Invasion of the data-snatchers" The Bulletin (9 May 2000) at 78.*
79. *D Q Wilber, "University to probe FBI's Canivorous habits" West Australian (5 August 2000) at 37.*
80. *This survey was conducted by the law firm Freehill, Hollingdale and Page and released in February 2000: see «www.freehills.com.au/4a25682400258290/Lookup/pdfguides/$file/Freehills_internet_privacy_survey.pdf». See also S Long, "Orwell and Your E-mail" Australian Financial Review (1 March 2000) at 17.*
81. *See Australia, Privacy Commissioner, "Guidelines on Workplace E-mail, Web Browsing and Privacy (30 March 2000)" «www.privacy.gov.au/issues/p.7_4.html». In her autobiography, Monica Lewinsky commented on the "violation" she felt during the Kenneth Starr investigation when deleted e-mails were retrieved from her home computer: see J Rosen, "Why Internet Privacy Matters" New York Times Magazine (30 April 2000) at 46.*

2.45 These threats to privacy have prompted calls to regulate internet and e-mail surveillance.[82] The question is, how? The United Kingdom has introduced legislation which extends telecommunications interception laws to cover internet communications at any time during their transmission, including when stored in the computer of the sender or recipient.[83] The United States is also looking to regulate internet and e-mail surveillance.[84]

2.46 The situation in Australia is more complicated due to the difference in Federal/State legislative powers. The Commonwealth Constitution gives the Commonwealth Government the power to regulate "postal, telegraphic, telephonic and other like services".[85] This power is not exclusive to the Commonwealth, and co-exists with the residual powers of the States.[86] The Commonwealth has used this power to enact the Interception Act, which prohibits, except where specifically authorised, the interception of

---

82. *See S Harris, "Privacy laws for e-mails" Sunday Telegraph (23 January 2000) at 30; Daily Telegraph, "Guide call for e-mail" (17 May 2000) at 9; J Norman, "Internet privacy? What privacy!" The Age (6 June 2000) at E1 and E8.*
83. *Regulation of Investigatory Powers Act 2000 (UK). This Act has attracted a fair degree of comment and criticism for encroaching too heavily on privacy: see Justice, "Regulation of Investigatory Powers Bill" «www.fipr.org/rip/JusticeRIP/audit1.htm»; L Rohde, "UK snoop law may conflict with EU Human Rights Act" «www.cnn.com/2000/TECH/computing/10/05/uk.snoop.v.eu.idg/index.html»; "RIP Bill to introduce far-reaching surveillance" «www.statewatch.org/news/ jun00/rip2.htm»; S Segan, "British Government to build major e-mail surveillance system" «www.abcnews.go.com/sections/tech/DailyNews/britishspies_000512.html».*
84. *In an attempt to "fix the inconsistent patchwork of laws that apply different standards to telephone, cable and other technologies with a single standard for those systems and the internet": see S Labaton, "Proposal Offers Surveillance Rules for the Internet" New York Times (17 July 2000) «www.nytimes.co/07/biztech/articles/18secure.html».*
85. *Constitution Act 1901 (Cth) s 51(v).*
86. *Constitution Act 1902 (NSW) s 5.*

communications passing over a telecommunication system.[87] The Interception Act applies only to interceptions conducted without the knowledge of the person making the communication, that is, covertly.[88] 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.[89]

2.47 As the internet and most e-mail systems operate through telephone lines, it is arguable that they could be caught by the Interception Act.[90] Being a relatively new and rapidly developing area there is no authority on this point.[91] The Interception Act is a law designed primarily to regulate the interception of voice communications. Whether or not the Interception Act is adequate in its current form to regulate internet and e-mail communications is

---

87. *Telecommunications (Interception) Act 1979 (Cth) s 7.*
88. *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.*
89. *Edelsten v Investigating Committee of New South Wales (1986) 7 NSWLR 222 at 230; Miller v Miller (1978) 141 CLR 269.*
90. *It should be noted that not all e-mail systems work in the same way. Some systems store e-mail on a network server, while others store it in the hard drive of individual computers. Similarly, not all e-mail systems operate through telephone lines. For example, a Local Area Network (or LAN) is a collection of computers linked directly, usually by cable, in a room or building. The connection enables users to share computer files and information, and hardware such as printers and scanners: M Neely, Australian Beginner's Guide to the Internet (6th edition, Maximag, Kiama, 1998) at 14.*
91. *K Davey, "Privacy Protection For Internet E-mail in Australia: Part 2" (1997) 34 Computers and the Law 8 at 18.*

not an issue for the Commission to determine.[92] *The safe assumption, however, is that the regulation of any interception of internet or e-mail communications occurring along a telephone line is a Commonwealth matter.*[93]

2.48 What role, then, can New South Wales have in regulating surveillance of internet and e-mail communications? The Interception Act applies only to communications in their passage across a telecommunications system. Surveillance of internet and e-mail communications may occur at points either before or after they have passed through the telecommunications system. For example, e-mail may be monitored, read or down-loaded when in the mailbox

---

92. For example, s 6(1) of the Interception Act refers to "listening to or recording" a communication. It would not, therefore, cover surveillance of an e-mail displayed on a computer screen as this is not listened to or recorded in any permanent form: see K Davey, "Privacy Protection for Internet E-mail in Australia: Part 1" (1997) 33 Computers and the Law 7 at 19; and P N Grabosky & R G Smith, Crime in the Digital Age (The Federation Press, Sydney, 1998) at 36. Section 6 also permits a person "lawfully on the premises to which a telecommunications system is provided" to intercept communications passing over that system. It has been argued that this section (assuming the Interception Act applies to e-mail) would offer little protection for e-mail surveillance in the workplace as it would enable employers to monitor employees' e-mail sent to and from premises lawfully occupied by the employer: See M Hudson, "Virtual Privacy: The Impact of Electronic Technology on Communications" (1998) 3(1) Media and Arts Law Review 18 at 19.

93. Although the Interception Act applies only to covert interceptions, and technically covers the field only to that extent, the Commission takes the view that any interception, whether overt or covert, of a communication in its passage along a telecommunications system, should be subject to Commonwealth regulation. Otherwise the following scenario could arise: the Commonwealth would regulate covert internet communications intercepted whilst travelling over a telecommunications system; the States could regulate overt internet communications intercepted whilst travelling over a telecommunications system, and covert internet communications intercepted at any point except when travelling over a telecommunications system.

or the hard drive of the sender or recipient, that is, before or after it has passed through the telecommunications system. The Commission is of the view that the proposed surveillance legislation should operate to regulate the monitoring of e-mail or internet communications at these points. As with any type of surveillance under the proposed legislation, the monitoring may be overt or covert, depending on whether the subject of the surveillance had prior knowledge. The Commission discusses the requirements for proving knowledge on the part of the subject, and different approaches to regulating overt and covert surveillance, later in this chapter.[94]

2.49 The interplay of State and Commonwealth laws in this respect would be somewhat analogous to the current situation whereby the interception of a telephone call at a point along the telephone line is regulated by the Interception Act, but using a tape recorder placed at the receiver to monitor the same call is regulated by the LDA.[95] *The Commission acknowledges that this two-tier system of regulation is not ideal. It places the onus on anyone wishing to conduct internet or e-mail surveillance to know the capacities of their monitoring software so that the point of surveillance could be determined, and this may not always be clear. For this reason, the Commission initially considered exempting internet or e-mail surveillance from the regulatory scope of the legislation. However, the law as it currently stands does not provide sufficient protection against the privacy threats presented by the internet. The Commission is of the view that it is better to sacrifice some clarity for the sake of comprehensive regulation.*

2.50 In the future, the Commonwealth may introduce comprehensive legislation to regulate all aspects of internet and e-mail communications. If that should occur, then the surveillance legislation recommended in this Report would have no application at all to such communications. A national, comprehensive regulatory scheme for the internet would certainly be attractive. The Commission cannot, however, recommend exempting internet and e-mail communications from the operation of the proposed

94. See para 2.78-2.82 and 2.86-2.98, respectively.
95. See T v Medical Board (SA) (1992) 58 SASR 382.

surveillance legislation based on a contingency that may or may not happen in the future. Until any further legislative moves are made by the Commonwealth, the proposed surveillance legislation should work as a "catch-all" to regulate the aspects of internet and e-mail surveillance not covered by the Interception Act.

Surveillance in private homes

2.51 The increased availability and affordability of surveillance technology has resulted in a growing number of people using surveillance equipment, video, audio-visual or sensor devices, usually in their homes. While primarily used for home security purposes, an emerging trend is to install video cameras to monitor baby-sitters, or even other family members.[96] *The Commission initially considered creating an exemption from the proposed legislation for surveillance conducted in private homes. On further reflection, however, the Commission realised that this could lead to serious breaches of privacy. For example, security cameras operating from a private home could be used to monitor activity in a neighbour's backyard. Complications also arise in multiple occupancy dwellings, where the interests of owners and residents may conflict. In one case reported to the Commission, the owners of a strata development installed video cameras in the common area to monitor people entering and leaving the lifts. The cameras were, however, trained on the front door of one of the home units, causing the resident to complain to the Privacy Committee of New South Wales (as it then was).*[97]

2.52 The adage that a "man's home is his castle" is all very well, but the rights of a property owner or resident must be measured against other legitimate interests. The Commission is of the view that the fact that a home is private does not mean that anyone who dwells, visits or works there (as in the baby-sitter example given above) must surrender their privacy. As the Commission noted

---

96. It was recently reported that sales of spy cameras in soft toys, clocks and smoke detectors jumped by 300% since 1997: see P Walsh, "Gotcha: Sales soar as parents resort to spy cameras" Daily Telegraph (16 October 2000). See also Privacy Committee of NSW, Submission at 11.

97. Privacy Committee of NSW, Submission at 11.

above,[98] privacy is a personal, not a property interest, and should not diminish because a person has entered the home of another. Accordingly, the Commission sees no reason to distinguish between regulating surveillance conducted in a private home and surveillance conducted anywhere else.

2.53 It should be remembered that the manner in which surveillance devices are used in homes in many cases would not amount to surveillance within the Commission's proposed definition, and would therefore not be regulated under any surveillance legislation. A video or sound recording of a child's birthday party, for example, would not fall within the definition of surveillance recommended by the Commission, as it is not made for the purpose of monitoring the children, but for recreational purposes[99] and as an electronic keepsake.

2.54 Where activity does fall within the Commission's recommended definition, compliance with the proposed legislation would not be unduly onerous for those conducting surveillance in a private home. The Commission considers that where surveillance is undertaken in a random, non-targeted fashion as part of a home security system, no prior authorisation should be needed. However, those conducting this type of surveillance must abide by the eight legislative principles[100] (preventing inappropriate use of surveillance equipment and the material obtained as a result) developed by the Commission to regulate overt surveillance.[101]

---

98. See para 2.26.

99. See para 2.66-2.67.

100. These principles must be supplemented by Codes of Practice for major users of overt surveillance, such as large retailers. Codes are not compulsory for smaller users or for surveillance conducted in private homes. All people conducting overt surveillance must, however, comply with the principles in the proposed legislation: see ch 3 and 4.

101. Generally, overt surveillance requires knowledge on the part of the subject to be demonstrated by clearly visible signs or equipment indicating that surveillance is occurring. The Commission recommends that non-targeted surveillance undertaken purely for home security purposes be exempt from this notice requirement: see

2.55 There may be occasions, however, where a resident wishes to conduct targeted surveillance of a particular subject within their home. To take the baby-sitter example again, a parent may have reason to suspect that the baby-sitter is harming the child and may wish to have video evidence before terminating the employment or calling the police, but not want the baby-sitter to be aware of the surveillance. In this situation, prior authorisation would be required under the Commission's recommendations. Indeed, this type of surveillance is already covered by the Workplace Video Surveillance Act 1998 (NSW) ("Workplace Video Surveillance Act") as it is in the context of an employment relationship.[102]

Surveillance by the media

2.56 The media are, of course, major users of surveillance technology. Microphones and cameras, with and without sound capacity, are the tools of the media's trade. In many cases, these cameras and microphones are used to film or record the views of people on particular subjects. At other times, hidden cameras or microphones are used, primarily with a view to exposing some scandal, corruption or cover-up. While it may not be readily apparent, the use of microphones and cameras by the media in this way amounts to surveillance within the Commission's recommended definition of surveillance,[103] *as it involves the use of a surveillance device to monitor people or places with a view to finding out information.*

2.57 The Commission has considered the issue of whether or not to exempt the media from the scope of its recommendations for proposed legislation. Media organisations strongly argued for an exemption, claiming that regulation under the proposed surveillance legislation would be contrary to the public interest and would compromise freedom of speech.[104] *The views in favour of and against*

---

ch 4.

102. *The Commission's recommendations for surveillance in an employment relationship subsume the Workplace Video Surveillance Act 1998 (NSW): see para 2.97 and ch 7.*
103. *See para 2.37-2.39.*
104. *Australian Broadcasting Corporation, Submission; Publishing and Broadcasting Limited, Submission; and Australian Press Council,*

regulation of the media are discussed extensively in Chapter 6.

2.58 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.

2.59 Compliance by the media with the proposed surveillance law need not be unduly onerous. So far as filming or recording conducted overtly is concerned, the media will be required to comply with the eight legislative principles recommended by the Commission,[105] and supplement those principles with a Code of Practice. This should present no difficulty since media industry Codes of Practice already exist.[106]

2.60 Of greater significance is covert surveillance undertaken by the media. Such surveillance, while undoubtedly valuable in revealing corrupt or illegal activity, also has an enormous capacity to invade privacy. Yet, it is not regulated by any statute in New South Wales. The Surveillance Devices Act 1998 (WA) ("Western Australian Act") contains a section permitting surveillance in the public interest.[107] Before material obtained as a result of such

---

Submission.

105. See ch 4.

106. For a discussion of Codes of Practice and the media, see ch 3 and 4.

107. Surveillance Devices Act 1998 (WA) Part 5.

surveillance may be published, authorisation must be obtained from a judge.[108] *This provision applies to, and has been used by, the media.*[109] *The Commission recommends that the proposed legislation should contain a separate part applying to anyone (including the media) wishing to conduct surveillance in the public interest, but should require authorisation prior to conducting the surveillance, rather than before publication occurs.*[110]

2.61 The Commission acknowledges that failing to exempt the media from its proposed regulatory scheme will generate controversy. However, the Commission does not accept the argument that including the media within the scope of new surveillance laws will act as a curb on freedom of speech or expression. It will merely ensure that, in upholding freedom of speech, the media respect other equally important public interests and act in accordance with the law.

What is not covered?

Telecommunication interception

2.62 As noted above, the Interception Act has been held to cover the field so far as telecommunications interception is concerned, making it a matter for the Commonwealth to legislate upon.[111] *Accordingly, the recommendations in this Report do not affect the interception of any communication in its passage along a telecommunications system.*

---

108. Surveillance Devices Act 1998 (WA) s 31.

109. The provisions of the Western Australian Act and the media's response to it are discussed in ch 6.

110. The Commission's views and recommendations concerning public interest surveillance are discussed in more detail at para 2.93-2.96 and in ch 6.

111. See para 2.46-2.47.

Surveillance provided for under a Commonwealth or another New South Wales law

2.63 Surveillance powers of various sorts are provided for under Commonwealth legislation and other New South Wales laws. At the Commonwealth level, the Interception Act, the Customs Act 1901 (Cth), the Australian Federal Police Act 1979 (Cth) and the Australian Security Intelligence Organisation Act 1979 (Cth) all contain surveillance powers. At the State level, the Casino Control Act 1992 (NSW) specifically provides for a casino surveillance system to be supervised by the Director of Casino Surveillance.[112] *Another example is the Road Transport (Safety and Traffic Management) Act 1999 (NSW) which provides for speed cameras.*

2.64 As the laws of New South Wales cannot bind the Commonwealth, the Commission is of the view that the proposed surveillance legislation should specifically exempt surveillance activity which is provided for under a Commonwealth law. The LDA currently contains a similar provision.[113] *Where surveillance is authorised under another law of New South Wales, however, the Commission considers that those laws should be amended specifically to provide that the proposed surveillance legislation has no application. The Commission favours this approach rather than providing for a general exemption in the proposed legislation for surveillance powers contained in other Acts. The requirement to amend existing legislation (or to insert a provision in future laws) stating that the surveillance legislation does not apply will help focus Parliamentary attention on the adequacy of surveillance powers and privacy protections in those other laws.*

Recommendation 4

The proposed Surveillance Act should exempt from its scope surveillance conducted under a Commonwealth law.

112. See Casino Control Act 1992 (NSW) Part 7.
113. LDA s 5(2)(a).

Recommendation 5

The proposed Surveillance Act should regulate all surveillance activity within its scope, unless other New South Wales laws specifically exempt the operation of the surveillance legislation.

Surveillance conducted without the use of a surveillance device

2.65 The definition makes it clear that the proposed legislation will only cover surveillance where a device is used. Direct observation by law enforcement agencies without the use of any device would, for example, be excluded.

Surveillance which is unintentional or for recreational purposes

2.66 Electronic equipment capable of being used as surveillance devices, once the domain of private investigators and police, has become more available and affordable for use as a recreational tool. The amateur photographer is now able to use sophisticated video and sound equipment with pan and zoom capacity in his or her weekend recreational pursuits. With the proliferation of this type of equipment, it is conceivable that private activity may be recorded or monitored accidentally or unintentionally. For example, a video camera being used to record a family outing may also film and record a private transaction in the background. Cameras and other equipment may also be left on accidentally. The LDA currently contains an exception in relation to the unintentional use of a listening device.[114] This type of activity would not be covered under the Commission's definition of surveillance, which requires monitoring to be intentional.

2.67 Similarly, amateur and professional photography or film-making would not be included in the Commission's definition of surveillance. These pursuits are for the purpose of recording events for posterity, and not the purpose of discovering information about the subject of the surveillance.

114. LDA s 5(2)(b).

Data surveillance

2.68 Specific issues arise concerning the inclusion of data surveillance within the scope of the proposed legislation. These are discussed below.

Surveillance and data protection

2.69 At one time, the distinction between surveillance and data protection was simple: surveillance involved the use of equipment such as cameras and listening devices while data protection regulated the use of personal information collected by agencies, either in paper form or on an electronic database. However, with rapid developments in, and convergence of technologies, the line between data surveillance and data protection has become difficult to decipher. Data surveillance can include the use of a computer to retrieve personal information from a database or to match information obtained from one database with that obtained from another. So can data protection. Data surveillance may involve the use of devices to obtain biometric information such as finger or retina prints, or genetic characteristics.[115] So can data protection. Even activity that appears clearly to be surveillance may impact on data protection, and vice versa. For example, surveillance video material may be converted into data and stored on a database, while information on a database or computer screen may be "read" by electro-magnetic devices and become surveillance material. In taking a broad regulatory approach, the Commission's recommendations encompass data surveillance. The difficult issue, however, is where to draw the line between data surveillance and data protection.

2.70 Limited data protection regulation already exists. The Privacy Act 1988 (Cth) ("Commonwealth Privacy Act") and the Privacy and Personal Information Protection Act 1998 (NSW) ("New South Wales Privacy Act") regulate the collection, storage, use and disposal of personal information about individuals held by certain

115. The Privacy and Personal Information Protection Act 1998 (NSW) specifically includes biometric information such as finger and retina prints and genetic characteristics: s 4(1).

Commonwealth and State government agencies, respectively.[116] *Both Acts define "personal information" to include information held on a "database" and need not be recorded in material form.* [117] *These Acts cover situations where information has been collected directly from individuals, stored on a database and retrieved at a later date. By regulating the use of the information collected, the Acts also cover data matching.*[118]

2.71 The data protection regime in Australia has been rightly criticised for covering only information held by public sector agencies. Increasing amounts of information is held on "corporate" databases, which may be shared, matched or "warehoused" without any regulation, prompting growing public concern over potential privacy threats.[119] *To address these concerns, and to satisfy the European Union Directive on data protection,*[120] *the Commonwealth*

116. *The Privacy Act 1988 (Cth) also applies to the private sector so far as credit reporting and tax file numbers are concerned.*
117. *Privacy Act 1988 (Cth) s 6 and Privacy and Personal Information Protection Act 1998 (NSW) s 4(1).*
118. *The Privacy Amendment (Private Sector) Act 2000 (Cth) provides that private sector agencies dealing with personal information must either develop a Code of Practice setting out proper collection, use and storage methods for that information, or follow the data protection principles included in the legislation. The Act applies only to private sector businesses with an annual turnover of more than $3 million, and exempts the media and political parties.*
119. *Public concern was raised in Australia over the proposal to establish a data warehousing company known as Acxiom. This company will collate information from various databases held by retailers, banks, post offices and electoral rolls, and cross-match it to form individual profiles of shopping trends and financial details. That information could then be sold to companies to build consumer profiles: see D Luff and M Farr, "Packer Files: Personal and financial details of 15 million Australians up for sale" Daily Telegraph (1 December 1999); "Urgent need to act on privacy" Australian Financial Review (2 December 1999); K Marshall, "Delay for Privacy Laws" Australian Financial Review (3 December 1999).*
120. *The European Union (EU) threatened to ban the export of data by EU countries to other countries that did not have adequate data protection legislation: Directive of the European Parliament and of the Council on the protection of individuals with regard to the*

has introduced the Privacy Amendment (Private Sector) Act 2000 (Cth), which extends information privacy principles to elements of the private sector. When it commences in December 2001, that legislation will extend regulation to the collection, storage and use of personal information held by applicable private sector organisations in New South Wales.

2.72 Whether or not that legislation will provide sufficient privacy protection has been significantly debated,[121] *and is not the focus of this Report. If the proposed surveillance legislation were to apply to the type of data surveillance covered by the New South Wales Privacy Act and the Commonwealth private sector legislation, the result would be that database managers would be required to comply with two regulatory regimes in relation to the collection, use and storage of the same data. This would not only be confusing, but would do little to enhance the privacy of the people who supplied the information. The Commission considers, therefore, that the collection, retrieval and matching of information on computer databases is more appropriately dealt with by way of data protection legislation rather than surveillance laws.*[122]

---

processing of personal data and on the free movement of such data (Directive 95/46/EC of 24 October 1995).

121. *The Privacy Amendment (Private Sector) Act 2000 (Cth) has been criticised for containing too many exemptions and for not applying broadly enough: see N Lindsay, "Victoria opposes federal privacy bill" Australian Financial Review (16 June 2000) at 89; S Hayes, "Privacy Bill not up to standard: EU" The Australian (27 June 2000) at 35; K Dearne, "Privacy-free zone" The Australian (27 June 2000) at 53. See also Australia, Senate Legal and Constitutional Legislation Committee, Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000 (October 2000).*

122. *This is the Commission's position so far as surveillance generally is concerned. Where a surveillance device is used by an employer to monitor information on a database concerning an employee, however, the Commission is of the view that the proposed surveillance legislation should apply: see para 2.74-2.76.*

Recommendation 6

The random or overt collection, retrieval and matching of information on computer databases should be excluded from the scope of the proposed Surveillance Act.

Coverage of covert data surveillance

2.73 The proposed surveillance legislation should apply to the covert monitoring of data through the use of a surveillance device. This would include, for example, situations where a computer, or a device placed inside or outside a computer, is used to collect and/or record data, including e-mail, as it is being entered into a computer. It would also include using a computer or other device to "hack" into a database of stored material. These acts involve deliberate attempts to uncover information without the knowledge of the person to whom that information relates. This type of activity is beyond the scope of data protection legislation, as it is obtained indirectly by stealth and need not be personal information. As such, the Commission believes that covert data surveillance should fall within the scope of the proposed legislation.

Recommendation 7

The covert use of a surveillance device to monitor data relating to particular individuals or groups, as it is entered into a technology system or stored on a database, should be regulated under the proposed Surveillance Act.

Data surveillance by employers

2.74 Employers have an interest in ensuring that employees' time is spent productively. To this end, some employers may have a policy of monitoring the number of key strokes their employees enter into a computer, or the number and type of e-mails employees receive. Employers may also wish to monitor documents on databases to

check that employees are performing work adequately and not spending time with personal work. Some of this data surveillance involves data protection issues. The Commission recommended above that the use of a device to retrieve or match information on a database should not be regulated by the proposed surveillance legislation, but should more appropriately be regulated by data protection laws. That is the Commission's position so far as surveillance generally is concerned. Where, however, that type of data surveillance occurs in the context of an employment relationship, the Commission is of the view that it is more of a surveillance than a data protection issue, and consequently the surveillance legislation should apply. The relationship between employers and employees involves special rights and responsibilities which justify additional protective measures in some circumstances.[123] *The Commission believes that data surveillance is one of those circumstances.*

2.75 Employers may wish to conduct data surveillance randomly and overtly, as part of an overall company policy. In order to be considered overt, the surveillance must be conducted only after the requisite notice has been given to all employers.[124] *If data surveillance is carried out overtly, employers must comply with the eight principles governing overt surveillance, one of which is that overt surveillance must be reasonable in the circumstances. Consequently, if the data surveillance is unduly intrusive, it may be considered unreasonable and would potentially be in breach of the proposed legislation.*[125]

2.76 Any surveillance conducted by employers without the requisite notice will be deemed to be covert surveillance. Employers may wish to conduct covert data surveillance, either themselves or through a private investigator, where, for example, the employer suspects fraud or theft and wishes to obtain evidence. As with any covert

123. *See para 2.97-2.98, 2.108-2.113 and ch 7 for the Commission's views on surveillance by employers.*
124. *See para 2.80-2.82 for the notice requirements for overt surveillance conducted by employers.*
125. *See ch 4 for a discussion of overt principles and the reasonableness requirement.*

surveillance, prior authorisation must be sought and obtained before covert data surveillance may proceed. Paragraphs 2.97-2.98 and Chapter 7 detail the authorisation procedure for covert surveillance conducted by employers.

Recommendation 8

Data surveillance of employees conducted by employers, either overtly or covertly, should be regulated by the proposed Surveillance Act.

REGULATION OF OVERT AND COVERT SURVEILLANCE

2.77 As the Commission noted earlier in this chapter, the approach taken in surveillance legislation in other jurisdictions is to limit regulation to private conversations and activity, generally conducted without the knowledge and consent of the subject of the surveillance. The Commission's recommendations differ from this approach by basing regulation, not on the type of activity which is under surveillance, but on the type of surveillance being conducted. The Commission has identified two broad types of surveillance: overt and covert.

Overt surveillance

2.78 Since overt and covert surveillance are to be regulated in very different ways, the Commission considers that the distinction between the two forms of surveillance should be made clear. Overt surveillance is usually conducted randomly for safety or security purposes. Examples include cameras used in banks and at Automatic Teller Machines, and closed circuit television cameras used in public mall areas and car parks. Such surveillance generally occurs openly, the key indicator being knowledge on the part of the subject. The way in which surveillance is regulated under the Commission's proposed new scheme will depend on

whether the subject of the surveillance knows that the surveillance is occurring. Because of the significance for the regulatory scheme of determining when knowledge is present, the Commission considers that it should be clearly and objectively definable. The Commission recommends that knowledge should be assumed, and surveillance therefore treated as overt, where adequate prior notice of the nature of the surveillance is given. Adequate notice should consist of the person or agency conducting surveillance proving the presence of:

- *clearly visible signs which are able to be understood by everyone (including, for example, people from non-English speaking backgrounds and people with a disability);*[126] *or*
- *other warnings of the type of surveillance occurring, such as audio announcements or written notification (where practicable); and*
- *clearly visible and recognisable surveillance equipment which indicates the type of surveillance that is occurring, eg audio, visual or both, etc.*

2.79 Provided these measures are taken, the requirements of notice would be fulfilled even if the subjects of the surveillance did not in fact read the signs or observe the equipment. Where the above requirements are not complied with, the surveillance would be considered to be covert, and would be regulated by the provisions of the legislation dealing with covert surveillance as discussed below.

Recommendation 9

The proposed Surveillance Act should define overt surveillance to be surveillance which occurs in circumstances where adequate notice of the surveillance has been given prior to, or simultaneously with, the occurrence of the surveillance.

Recommendation 10

For the purpose of Recommendation 9, adequate

126. A comparable example would be no smoking signs.

notice is 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.**

Notice required for surveillance by employers[127]

2.80 Where overt surveillance is conducted generally, it will be irrelevant whether or not any individual subject to the surveillance has actual knowledge of its occurrence. The Commission considers that in the employment context, a more stringent approach is appropriate, whereby actual knowledge is required.[128] *The reason for requiring actual knowledge in the employment context is two-fold. First, unlike overt surveillance of a shopping mall or railway station where hundreds of people will be randomly monitored daily, in the employment context those employees who will be affected by overt surveillance can be identified. Accordingly, it is possible to ensure affected employees have actual knowledge of the surveillance. Secondly, where an employer uses surveillance devices, employees are potentially subject to continuous surveillance and consequent privacy invasions for prolonged periods. This contrasts with the temporary invasion involved in most forms of overt surveillance conducted outside the employment context. Spending eight hours a day, five days a week under continuous CCTV surveillance has significantly higher privacy implications than being caught by CCTV for fifteen minutes while one waits for a train.*

127. Refer to para 2.108-2.113 for a detailed discussion of when employment-specific recommendations apply.

128. The Commission notes the view of the Registered Clubs Association of NSW that there should be no requirement to notify each individual employee, Submission at 3.

2.81 Consequently, the Commission recommends that actual knowledge should be ensured by the provision of written notification to each employee prior to the commencement of any surveillance. The current Workplace Video Surveillance Act approach of requiring at least 14 days notice, unless consent to a lesser period is obtained, is considered to be an appropriate time frame. Any employee who commences work following the commencement of overt surveillance must be provided with similar written notice.

2.82 Associated with the requirement that employees be provided with actual knowledge of overt surveillance is our recommendation that the knowledge be fully informed. Notification of the bare fact of surveillance will be insufficient to satisfy the significant privacy implications of overt surveillance by an employer. Accordingly, the Commission recommends that the written notice must provide the details set out in the recommendation below.[129]

Recommendation 11

Surveillance in the employment context should be considered overt if employees are provided with written notification of the intended surveillance at least 14 days (or, if the employer has obtained the consent of the employee to a lesser period of notice, that period) prior to its commencement.

In the case of new employees, where surveillance has already commenced, surveillance in the employment context would be considered overt if they are provided with written notification of the surveillance at the time when an offer of employment is made.

129. These details are based on the Codes of Practice, discussed in ch 4.

Recommendation 12

For the purposes of overt surveillance in the employment context, written notice should contain the following information:

(a) the location of the surveillance;

(b) the nature and capacity of the surveillance devices;

(c) whether the surveillance will be continuous and, if not, the hours of operation;

(d) the purpose of the surveillance; and

(e) the person responsible for the conduct of the surveillance.

Overt surveillance and consent

2.83 The Commission has considered the question of whether, in addition to knowledge, consent should be an element in proving that surveillance is overt. Clearly, where the subject consents freely and expressly to surveillance occurring, that surveillance will be overt since there can be no consent without knowledge of surveillance. However, the Commission has decided against recommending that consent be an essential element in overt surveillance for the following reasons.

2.84 For consent to be real, it should at least involve the two elements of knowledge and choice. In many situations, however, it is not possible to determine whether consent is given freely, and it is therefore often implied from the circumstances. For example, when a person enters a service station to buy petrol, he or she notices a sign indicating that the area is under video surveillance. On one interpretation, that person may be deemed to be consenting to the surveillance by entering the premises knowing that video cameras are operating there. The reality may be, however, that since most if not all petrol stations employ some form of electronic surveillance, there is nowhere else to buy petrol that is not also under surveillance. In this situation, while the person knows the

surveillance is occurring, he or she is not presented with a choice since the only alternative is to submit to the surveillance or run out of petrol. Consequently, any attempt to infer consent from such a situation is largely illusory.

2.85 In addition to conceptual difficulties surrounding consent, the Commission also considers it impractical to require consent before overt surveillance can be conducted. Many forms of overt surveillance target a large number of surveillance subjects and are usually random in nature. Obtaining the express consent of all potential people would be impossible since there is no way of knowing who those people are. Consequently, the Commission is of the view that consent should not be required by those subject to overt surveillance.

Regulation of overt surveillance

2.86 The Commission sets out its recommendations regarding the regulation of overt surveillance in Chapters 3 and 4. Briefly, the proposed legislation should set out basic principles with which people conducting overt surveillance should have to comply. Those principles would, for example, provide that those who undertake overt surveillance must:

- *not contravene reasonable expectations of privacy eg be in toilets or change-rooms;*
- *use the surveillance for lawful and not unlawful purposes;*
- *not exceed the purpose for which the surveillance is intended;*
- *have in place secure systems for the collection, use, storage and destruction of surveillance material eg security procedures for video and audio tapes, proper training and probity checks on staff, etc;*
- *make their surveillance systems and devices available for inspection and monitoring by the Privacy Commissioner; and*
- *ensure that material obtained through surveillance is used only in a fair manner by authorised persons.*

2.87 As these principles are based on best practice measures, many users of overt surveillance would already be complying with them.[130] Breach of the principles in the legislation would give rise to a civil action.[131] For "small" users of overt surveillance, such as corner stores or people using home security systems, compliance with the legislative principles would be sufficient. However, larger users, such as banks, would be required to supplement the legislative principles with codes of practice.[132] The Commission considers that this approach to regulating overt surveillance is flexible and allows for the enforcement of privacy rights without being unduly onerous on those conducting overt surveillance.

Covert surveillance

2.88 Surveillance will be covert under the Commission's recommendations where it is conducted without first notifying the subject. Generally, but not always, covert surveillance tends to be targeted towards a specific individual, group or object, and is undertaken to discover particular information or evidence about the subject of the surveillance. Various laws and guidelines contain definitions of covert surveillance.[133] The Macquarie Dictionary defines covert as covered, sheltered, concealed, secret or disguised. The Commission is of the view that any surveillance conducted in circumstances which fail to satisfy the notice requirements for overt surveillance will be deemed to be covert.

---

130. See ch 3 and 4.

131. See ch 10 regarding complaints and review mechanisms.

132. The Commission refers to these larger users as "relevant surveillance users": see ch 4.

133. For example, guidelines issued by the Commonwealth Privacy Commissioner define covert surveillance as "the secretive, continuous or periodic observation of persons, vehicles, places or objects to obtain information concerning the activities of individuals which is then recorded in material form including notes and photographs: Australia, Privacy Commissioner, Covert Optical Surveillance in Commonwealth Administration – Guidelines (February 1992) at 1.

Recommendation 13

Any surveillance conducted in circumstances that fail to satisfy the notice requirements for overt surveillance should be considered to be covert for the purposes of the proposed Surveillance Act.

Regulation of covert surveillance

2.89 All surveillance legislation examined by the Commission, including the LDA, regulates covert surveillance by prohibiting it unless a warrant is obtained from a judge, or the surveillance falls under an exception in which case a warrant is not needed. The Commission considers that a warrants scheme is the most appropriate way to regulate covert surveillance. Requiring the approval of an independent arbiter before conducting surveillance helps to minimise the serious threat to individual privacy presented by covert surveillance, and ensures that it is conducted only where justified. The Commission considers, however, that the presence of too many ill-defined exceptions can undermine the privacy protection offered by a warrants system. In order to avoid this, the Commission has examined the scope of activity covered by the warrants and exceptions in the LDA and other surveillance legislation, and discovered three main areas where covert surveillance would be legitimately conducted. Those areas are law enforcement, the public interest,[134] and in the course of employment.

2.90 Accordingly, the Commission has devised a three-pronged approach to regulating covert surveillance based on those areas mentioned above, with prior authorisation required for each. Where prior authorisation cannot possibly or practicably be obtained, surveillance may be conducted and retrospectively validated by the appropriate authorising body. Regulating covert surveillance in this

134. While the Commission acknowledges that covert surveillance conducted by, or on behalf of, law enforcement officers and employers has a public interest element, the term "public interest" is used in this context to refer to covert surveillance which can be justified in any circumstance outside law enforcement and employment: see ch 6.

way removes the need for the legislation to contain exceptions, since all surveillance must be authorised either before or after the fact. Since covert surveillance conducted by either law enforcement agencies, in the public interest or by employers, will clearly be for different purposes, the Commission is of the view that three separate but parallel systems of authorisation should operate. The question of which body has the power to authorise surveillance will depend upon either who was conducting the surveillance or the purpose for which it was conducted. Those three systems are explained briefly below, but see Chapters 5, 6 and 7 for more detail.

Covert surveillance by law enforcement officers

2.91 The regime recommended by the Commission to regulate covert surveillance conducted by law enforcement officers is similar to the warrants scheme in the LDA. Generally, a warrant must be obtained from a judge before a law enforcement officer may conduct covert surveillance. Retrospective warrants may be obtained to validate covert surveillance where prior authorisation was not possible, for example, in an emergency or during an undercover operation. The procedure for applying for and obtaining warrants would be largely the same as in the LDA, subject to a few differences. Officers would still have to submit a written affidavit explaining the type of surveillance to be conducted, why it is justified, and what likely use will be made of the material collected.

2.92 The Commission's recommendations depart from the LDA to the extent that only law enforcement officers will be able to apply for a warrant from a judge. Anyone else wishing to conduct covert surveillance must seek authorisation under either the public interest process or the employment system. For the sake of clarity, anyone who is a law enforcement officer must use the warrants system and not the public interest system, even though law enforcement can be said to be upholding a public interest. "Law enforcement officer" should be defined broadly to include commonly regarded law enforcement agencies such as the police, the Independent Commission Against Corruption or the Police Integrity Commission, etc. It should also include any office holder specifically empowered to enforce a particular law, for example, fisheries inspectors, unless those laws specifically exempt the operation of the

proposed surveillance legislation.[135] *The law enforcement warrants system should also include people acting on behalf of law enforcement officers, such as informers.*

Covert surveillance in the public interest

2.93 There will be times when covert surveillance would be justified in situations involving a public interest, other than when conducted by law enforcement officers or in an employment context. Examples include a private inquiry agent investigating insurance fraud or a journalist pursuing a corruption scandal. The Western Australian Act contains a section on surveillance in the public interest. Under the Western Australian Act, a person may conduct audio or visual surveillance (or both) in certain circumstances if it is in the public interest to do so.[136] *Public interest is defined to mean "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".*[137] *Anyone wishing to publish or communicate the information obtained as a result of covert surveillance in the public interest must obtain a publication order from a Judge.*[138]

2.94 The Commission considers that, while the idea of obtaining a publication order before surveillance material can be released is sound, it still allows for too great a breach of privacy since the surveillance may be conducted without any prior authorisation. Consequently, the Commission recommends that authorisation should be obtained before the covert surveillance is conducted, rather than before release of the surveillance material. A more detailed explanation of the reasons why the Commission favours

---

135. See para 2.64.

136. The Western Australian Act has different provisions depending on whether or not the person conducting surveillance in the public interest is a party to the activity being monitored: see Surveillance Devices Act 1998 (WA) s 26-30. See ch 6 for more details of the Western Australian Act. The majority of the Commission rejects the view that different considerations arise where surveillance is conducted by a party: see para 2.99-2.107.

137. Surveillance Devices Act 1998 (WA) s 24.

138. Surveillance Devices Act 1998 (WA) s 31.

prior public interest authorisation is in Chapter 6.

2.95 The Commission is of the view that authorising covert surveillance in the public interest involves different policy questions from hearing a warrant application by a law enforcement officer. Accordingly, the Commission recommends that a separate system of authorisation should apply for covert surveillance in the public interest. That system could be administered either through a court or a tribunal, with the application procedures mirroring as closely as possible the procedures for covert surveillance by law enforcement officers and employers. [139]

2.96 Emergency situations should also be covered, where a prior authorisation is not practicable or possible. In such cases, a retrospective authorisation should be available. An application for a retrospective authorisation should explain why a prior authorisation was not possible. If a person conducts covert surveillance and does not apply for a retrospective authorisation, the surveillance will be considered unlawful and the information obtained may not be released.

Covert surveillance by employers[140]

2.97 Currently, the Workplace Video Surveillance Act requires an employer, or anyone acting on behalf of an employer, who conducts covert video surveillance of employees to obtain prior authorisation from a magistrate. The proposed surveillance legislation would, if implemented, incorporate the operation of the Workplace Video Surveillance Act into its broader scope. The Commission considers that prior authorisation for covert surveillance by, or on behalf of an employer, should be obtained from a Judicial Member of the NSW Industrial Relations Commission or an Industrial Magistrate rather than from a Magistrate. This is because of those persons' specialist knowledge of employment relations. As with covert surveillance conducted by law enforcement agencies or in the public interest, there should be a provisions for surveillance by an employer to be retrospectively validated in circumstances where

139. See ch 6 for more detail.

140. Refer to para 2.108-2.113 for a detailed discussion of when employment-specific recommendations apply.

prior authorisation is not possible or practicable.

2.98 The Commission is of the view that, as far as possible, the provisions relating to surveillance by employers should mirror those conducted by anyone else, except where the nature of the employment relationship justifies differences. Circumstances which justify different provisions for employee surveillance are noted throughout this Report.[141]

Participant monitoring

2.99 The LDA currently permits a party to a conversation to record that conversation, without a warrant and without the knowledge of the other parties, where the recording is reasonably necessary for the protection of the recording party's lawful interests, or where the recording is not made for the purpose of communicating or publishing its contents to others.[142] *This practice, known as "participant monitoring", is one of the most controversial surveillance issues.*[143]

---

141. See para 2.74-2.76, 2.80-2.82, 2.108-2.113, 3.20-3.28, 3.61-3.70, 4.74-4.79 and ch 7.

142. LDA s 5(3). The onus of establishing that the recording was conducted for the protection of lawful interests or was not intended to be released rests with the party seeking to rely on those provisions: Miller v TCN Channel Nine (1988) 36 A Crim R 92 at 97.

143. For a more detailed discussion of participant monitoring see: I Elliot, "Listening Devices and the Participant Monitor: Controlling the Use of Electronic Surveillance in Law Enforcement" (1982) Criminal Law Journal 327; P Ford, "Who's Listening? Recording and Monitoring of Personal and Business Communications" (1998) 48(2) Telecommunications Journal of Australia 75; T Molomby, "Could Monica Lewinsky and Linda Tripp do it here?" (March 1998) Law Society Journal 51; A Henderson and A McDonough, "Call monitoring – legalities and regulation" (1999) 2(8) Telemedia 97.

2.100 It is controversial because the interests that need to be protected or promoted are not easily distinguishable. Where a private conversation is recorded covertly by a third party, there is a clear breach of privacy and confidentiality. The only question is whether, and in what circumstances, that breach can be justified by other interests, such as the public interest in fighting crime. Where a private conversation is recorded by a party to that conversation without the knowledge or consent of the other parties, the situation is less clear.

2.101 Proponents of participant monitoring believe that it is a necessary, accurate, effective and reliable evidence-gathering tool, particularly for undercover law enforcement officers.[144] Participant monitoring is also practised in the commercial and business sectors, and by emergency services, to guard against possible future allegations of illegal or improper conduct. The major argument in favour of participant monitoring is that, as a party to a conversation or activity, a person has an express or implied right to hear the words spoken during that conversation or view the activity. The argument follows that the right to record the conversation or activity flows from the right to observe and be a party to it, and is no more intrusive on privacy than if the person took written notes.[145] In reaching the view that participant monitoring should be permitted without restriction, the ALRC considered that prohibiting or regulating participant monitoring would lead to undesirable

---

144. The NSW Police Special Services Group noted that wiring undercover operatives is often necessary for ensuring their safety during an investigation: NSW Police Service, Special Services Group, Submission at 4. See also Joint Law Enforcement Agencies, Submission at 5; New South Wales, Royal Commission into the New South Wales Police Service, Final Report (May 1997) Vol 2 at 457.

145. See Australian Law Reform Commission, Privacy (Report 22, 1983) Vol 2 at para 1133. The ALRC saw the similarity between note-taking and electronic recording of a conversation as a crucial factor in recommending against the regulation and prohibition of participant monitoring. Two members of the ALRC dissented, taking the view that participant monitoring presented a serious invasion of privacy and ought to be regulated. The ALRC's recommendation reversed the earlier view expressed in its Discussion Paper entitled Privacy and Intrusions (DP 13, 1980) at para 118.

results, and render conduct illegal which should otherwise be acceptable, such as preventing people from recording conversations with their doctors or with the police.[146]

2.102 Those arguing against participant monitoring view it as a fundamental breach of privacy,[147] *since all parties to a conversation or activity should reasonably be able to expect that the conversation or activity will not be monitored, unless all parties expressly consent.*[148] *Some commentators have expressed the concern that the participant monitoring provisions are too vague, are open to misinterpretation and abuse, and are often used as a means of escaping the need to get a warrant.*[149] *Regarding participant monitoring by law enforcement agencies, it has been said that:*

> *[t]he danger here is that any person can be targeted for*

---

146. *It should be noted that the Commission's recommendation that participant monitoring provisions not be included in the proposed surveillance legislation will not necessarily render such conduct "illegal". First, such conversations would only be regulated by the proposed legislation if they were conducted with a surveillance device in circumstances which fulfilled the definition of surveillance recommended by the Commission at para 2.37-2.39. If the conversations amounted to surveillance and were recorded openly, then, under the Commission's recommendations, this would be legal provided the principles regarding overt surveillance were complied with: see ch 3 and 4. Where such monitoring was done covertly, it would be legal provided prior or retrospective authorisation was obtained: see para 2.90.*
147. *The removal of participant monitoring provisions in the Western Australian Act has been said to have enhanced privacy: S Davies, "Privacy and Surveillance: The Surveillance Devices Act 1998" 27(1) Brief (February 2000) at 7.*
148. *Privacy Committee of NSW, Submission at 15.*
149. *Some submissions considered that restricting participant monitoring to situations where a party's "lawful interests" are threatened is not a sufficient check on the power, and that the decision as to whether covert recording is necessary to protect the "lawful interests of the principal party" should more appropriately be made by a court rather than by that party themselves: see NSW Council for Civil Liberties, Submission at 4; Privacy Committee of NSW, Submission at 15; Law Society of NSW, Submission at 3.*

> *unlimited, highly intrusive electronic surveillance without law enforcement officers having first satisfied a judge or other independent person that there are reasonable grounds to believe or suspect that evidence relevant to the commission of an offence may be obtained.*[150]

2.103 Since participant monitoring is often used by law enforcement agencies to record conversations covertly to gain evidence, the provisions have a significant impact on a suspect's right to silence.[151] *The Canadian Supreme Court has held that "warrantless participant surveillance", although conducted lawfully by a police officer under Canadian law, nevertheless breached the constitutional right to be free from arbitrary search and seizure contained in the Canadian Charter of Rights and Freedoms.*[152]

2.104 The Commission considers that allowing a person to conduct surveillance without a warrant merely because they are a party to the activity being monitored presents too great a threat to privacy.[153] *The participant monitoring provisions in the LDA are vague and uncertain. They are couched in broad language which has not been tested by the courts and which raises questions concerning who the "principal party" to a conversation is, and what that party's "lawful interests" are. This uncertainty creates a significant opportunity for people to conduct unjustified covert surveillance by simply becoming a party to an activity, thereby undermining the safeguards contained in the authorisation procedures recommended for covert surveillance.*

2.105 The main objection the Commission has to participant

---

150. S Bronitt, "Electronic Surveillance, Human Rights and Criminal Justice" (1997) 3(2) Australian Journal of Human Rights 183 at 193.

151. Bronitt at 197-205. See ch 9 for a discussion of the use of surveillance evidence and the impact on right to silence.

152. R v Duarte (1990) 53 CCC (3d) 1. Following this decision, the Canadian Criminal Code was amended to remove participant monitoring provisions: s184(2).

153. The Commission's Chairperson, Justice Michael Adams, dissents on the recommendation concerning participant monitoring so far as the use of listening devices is concerned: see Appendix A.

monitoring is that it is based on the flawed assumption that covert surveillance is automatically more acceptable and less of a privacy breach because it is conducted by a party to a conversation rather than a third party. Inviting a person to talk, or impliedly consenting to involve a person in a conversation or activity, is not the same as permitting that person to record the activity. Different questions of knowledge and consent arise. The Commission also rejects the argument that covert recording by a party to a conversation or activity should be allowed, since there is no distinction between electronic recording and taking written notes. Again, different questions and degrees of knowledge and consent are involved. A conversation or activity may be recorded covertly, but it is very difficult to imagine notes being written covertly during a conversation. Notes may be written up later from memory, but this evidence will be less compelling and accurate than a permanent, contemporaneous recording of activity in which the person's gestures and voice, including pauses, intonations and interjections, may be heard and observed out of context. A recording may also be copied and heard by a greater number of people, and will carry more evidentiary weight in court than written notes or oral testimony. Accordingly, the Commission considers that an electronic recording of a conversation or an activity can and should be distinguished from written notes and should be subject to greater control.

2.106 The concept of participant monitoring as included in current legislation also reflects an outdated and narrow approach to technology. It has relevance only to the monitoring or recording of conversations or activity, generally through audio or visual means or by picking up a telephone extension, where the parties to that conversation or activity are identifiable. Participant monitoring has little meaning when applied to computer or internet surveillance where the concept of a "party" is less clear.[154] *It is consequently a device-specific concept, which is at odds with the broad general approach recommended by the Commission in this Report.*

---

154. See P Ford, "Who's Listening? Recording and Monitoring of Personal and Business Communications" (1998) 48(2) Telecommunications Journal of Australia 75.

2.107 In recommending that participant monitoring provisions not be included in the proposed surveillance legislation, the Commission is not suggesting that there should be no controls on a party to a conversation or activity conducting covert monitoring, or that a party should be totally prohibited from doing so. The real question is not whether the person conducting the covert electronic monitoring participates in the conversation or activity, but in what situations should such monitoring be allowable or justifiable and what privacy safeguards should be put in place. For example, when an undercover police officer records a conversation or films an activity covertly in an emergency situation to prevent a serious threat to public safety, this should be allowed under the proposed legislation, not because the police officer was a party to the conversation, but because the circumstances justified covert surveillance in that instance. Accordingly, the Commission recommends that the proposed surveillance legislation should not distinguish between monitoring conducted by parties and non-parties, but should facilitate covert surveillance when it can be justified in any particular situation.

Recommendation 14

The proposed Surveillance Act should not contain participant monitoring provisions with regard to covert surveillance. Covert surveillance should be permitted only when justified and authorised in particular circumstances, regardless of whether the monitoring is conducted by a party or an outsider.

The "employment context"

2.108 With both overt and covert surveillance, specific consideration has been given to the use of surveillance in the employment context. Not only does surveillance in the employment context have serious privacy implications, it raises broader industrial issues grounded in the respective, and often conflicting,

interests of employees and employers.[155] *It is because of the particular privacy issues and the additional industrial dimension that the Commission has identified this field of surveillance to require specific consideration.*

2.109 An important, preliminary matter is to identify when surveillance can be said to occur in the employment context for the purpose of requiring special consideration and regulation. The approach adopted in the Workplace Video Surveillance Act is to regulate the surveillance of an employee by an employer in the workplace. Accordingly, in terms of the Workplace Video Surveillance Act, the employment context is identified by reference to both an employment relationship and a physical location. This approach has the attraction of making it straightforward to identify when the Act will apply. By limiting its application to the workplace, the Act avoids the more difficult question of whether surveillance of an employee by an employer, not on work premises, should ever belong in the employment rather than the general context of surveillance regulation.

2.110 The Commission considers that restricting the employment context to surveillance that occurs in the workplace will exclude situations that should properly be included. Employers may wish to carry out surveillance of employees in a range of situations that, although related to their employment, occur off work premises. For example, an employer may wish to video an employee having a meal at a restaurant during his or her lunch break, suspecting the employee of consuming alcohol. Similarly, an employer could be interested in videoing the activities of an employee who is absent from work because of illness. Such instances of surveillance may have serious implications for the employee, such as forming the basis of dismissal. They are also matters in which an employer may legitimately be interested. In the view of the Commission, it is illogical and inappropriate to exempt this type of surveillance from our consideration of surveillance in the employment context and

---

155. New South Wales, Parliamentary Debates (Hansard) Legislative Council, 26 May 1998 at 5087-5088; New South Wales, Privacy Committee, Invisible Eyes: Report on Video Surveillance in the Workplace (Report 67, 1995) at 11.

any specific provisions that may flow from that consideration.

2.111 Extending the reach of the employment context beyond surveillance occurring on work premises raises the issue of where to draw the line; should any surveillance of an employee by an employer be included? In the Commission's view, surveillance of an employee by an employer, other than on work premises, should only occur in the employment context when it is conducted for an employment-related purpose.[156] *This leaves surveillance of an employee by an employer, not on work premises and not for an employment-related purpose under the general regime. This approach is consonant with the underlying basis of separating the employment context from the general context; namely the industrial dimension.*

Recommendation 15

In the proposed Surveillance Act, employment specific provisions should apply:

(a) when an employer is undertaking surveillance of an employee on work premises; or

(b) when an employer is undertaking surveillance of an employee not on work premises but for an employment-related purpose.

156. For a discussion of when conduct outside work may or may not be related to employment, see Rose v Telstra Corporation (Australian Industrial Relations Commission, U No 20564 of 1998, Ross VP, 4 December 1998, unreported).

Meaning of "employer" and "employee"

2.112 The Workplace Video Surveillance Act defines "employer" and "employee" by reference to a contract of employment or apprenticeship.[157] *This approach excludes volunteer workers and independent contractors. However, as the basis of providing specific consideration to surveillance in the employment context is the industrial dimension, the Commission considers that it is appropriate to limit the concept of an employment context, and therefore any employment specific provisions, to those persons in a formal, employment relationship.*[158]

2.113 Under the Workplace Video Surveillance Act approach, surveillance of an employee by an employer, who is not the employee's employer, will be caught. For example, if the owner of a retail store were to conduct surveillance of a Telstra technician, visiting the retail store in the course of his or her employment, that instance of surveillance would fall within the Workplace Video Surveillance Act. The effect of this is that persons not in a formal, employment relationship are caught by employment-specific provisions. Given that the Commission recommends comprehensive regulation of covert surveillance, the possibility that this type of "employment" surveillance would be left unregulated will be removed. Accordingly, the Commission considers that the current Workplace Video Surveillance Act approach should be tightened and therefore recommends that "employer" and "employee" should be defined in such a way that restricts the employment context to a direct employer-employee relationship.

---

157. *Workplace Video Surveillance Act 1998 (NSW) s 3.*
158. *In the situation of volunteer workers and independent contractors, there has been no intention by the parties to create a legally binding, employment contract. Accordingly, it is inappropriate to impose employment provisions on parties who have chosen not to enter into an employment relationship.*

Recommendation 16

"Employer" and "employee" should be defined in the proposed Surveillance Act by reference to a contract of employment or apprenticeship, to which both are parties.

Conclusion

2.114 In summary, the Commission is recommending surveillance legislation extremely broad in scope, covering the intentional use of any device to monitor a person, place or object with a view to discovering information about the subject of the surveillance. The legislation will regulate surveillance of any activity which falls within its scope, not just activity considered to be private. It will cover surveillance conducted with and without the knowledge of the subject, and regardless of who conducts it. Overt surveillance conducted by anyone will be regulated by eight legislative principles, supplemented by codes of practice for larger users. The principles will cover the proper use of surveillance devices, and the use, storage and disposal of material obtained as a result of overt surveillance. Covert surveillance will be governed by three clear, distinct, yet parallel, schemes of prior authorisation. The applicable scheme will depend on whether the surveillance is conducted by, or on behalf of, a law enforcement officer, an employer, or in the public interest. The terms of each authorisation will dictate the proper use of the surveillance device and the material obtained from that use.

2.115 Deviation from the overt surveillance principles or the provisions of the legislation concerning covert surveillance authorisations will result in a breach of the legislation. Various consequences will follow a breach of the legislation, depending on the nature and extent of the breach. For example, the publication or use of surveillance material may be prevented or restricted, and

criminal sanctions may apply. Breach of the legislation may also give rise to a civil action for damages.[159]

2.116 As noted at the outset of this chapter, the Commission believes this regulatory regime to be the most effective and comprehensive method of achieving the aim of protecting privacy against encroaching surveillance technology, and regulating the breach of privacy where the surveillance can properly be justified.

159. See ch 10 for complaints and review procedures.

3. Overt surveillance: issues

- Introduction
- Ways of “seeing”
- Purposes of overt surveillance
- Problems with using overt surveillance
- The efficacy of overt surveillance
- The future of overt surveillance
- Views contained in submissions
- Regulation

INTRODUCTION

3.1 This chapter reviews the use of surveillance devices, of any type, for the purpose of conducting overt surveillance. This approach differs slightly from that taken in IP 12.[1] *There, our discussion of overt surveillance devices was confined largely to the visual kind, in contrast with aural devices, which were discussed in the context of covert surveillance and the Listening Devices Act 1984 (NSW) ("LDA"). In reality, most surveillance devices can be used either overtly or covertly.*

3.2 The chapter also explains why overt surveillance is likely to become more sophisticated and increasingly prevalent. This, coupled with the convergence of technologies, will make it more difficult for individuals to avoid being subject to some form of surveillance in their daily lives. Simultaneously, the public's understanding of and concern over the possible consequences for their personal privacy is growing. So too are calls for measures to be adopted to safeguard people's privacy expectations. In industries whose activities impinge on personal privacy, such measures have, to date, been largely in the form of self-regulatory codes of practice.

3.3 In this Report, the principal feature that distinguishes overt surveillance from covert surveillance is the giving of notice to the subject of the surveillance.[2] *This is manifested most obviously where the consent of the subject has been sought by and granted to the surveillance user. However, if the issue of actual consent has not arisen, it may be difficult to prove whether the subject of the surveillance received sufficient notification to be aware that surveillance was taking place. For this reason, the Commission recommends*[3] *that so long as certain measures are taken, such as erecting clear signs advising of the surveillance, notice sufficient for such surveillance to be deemed overt will have been given.*

---

1. *New South Wales Law Reform Commission, Surveillance (Issues Paper 12, 1997) at para 4.1.*
2. *Para 2.77-2.79.*
3. *Para 2.78-2.79.*

WAYS OF "SEEING"

3.4 The overt use of surveillance devices can take a number of forms. Examples of what are readily recognised as overt surveillance devices include closed circuit television (CCTV) systems, located in shops, offices, malls, public transport access points and so on, and tracking devices fitted in vehicles to ascertain the progress of employees on their rounds. 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, such as the people in the photographs, or the lecturer, but merely to record an occasion for later enjoyment or as an aid to memory. Similarly, the unconcealed recording of interviews of suspects or witnesses by police are carried out not for the purpose of monitoring but as a visual aid to a written transcript, or as verification that proper procedures were followed.[4] *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.*

3.5 Other surveillance technology may have multiple fields of application, not all of which would be regarded as surveillance. X-ray devices, for example, are used at airports and high-security buildings for weapons and explosives detection, but are more familiar in the context of medical imaging. While we may not think of the latter application as surveillance, it does, strictly, fit our definition of surveillance. Other devices may not appear, initially, to be surveillance devices, yet surveillance is or may be a function. A keycard may give access to a building, or to certain floors within a

4. Criminal Procedure Act 1986 (NSW) s 108.

building, but, unlike an ordinary key, may also identify the keyholder and enable the collection of information regarding the keyholder's movements within the building. Recently it was alleged that the use by some rail workers of free staff travel passes had allowed management to download electronic information from automatic station barriers. This information, recording the time and date of use of the passes, could be used to determine if workers were leaving shifts early.[5]

3.6 The perception of whether a device is employed to conduct overt surveillance may determine whether the device should fall within any possible scheme of regulation. For example, it might be required that signs be displayed at keycard access points, alerting people to the possibility of surveillance. In radiology, ultrasound and other departments where medical imaging equipment is used, however, different considerations would need to apply under any scheme of regulation, notwithstanding the fact that, technically, these are surveillance devices.

PURPOSES OF OVERT SURVEILLANCE

3.7 The Commission is of the view that, despite potential intrusions on personal privacy and other concerns, in principle, surveillance has a proper role to play in today's society. The New South Wales Council for Civil Liberties disagrees with this view,[6] *suggesting that the Commission question not whether to regulate the use of visual surveillance, but rather whether to permit it at all. The Council's position with regard to the use of overt and covert video cameras in public places is that it should be prohibited outright, although it concedes that if such use is to be permitted then sufficient safeguards must be employed.*[7] *In the Commission's view, any likelihood of halting the growing use of surveillance devices, let alone dismantling the existing infrastructure, is wholly unrealistic. Apart from what the Commission sees as the justifiable*

5. *R Wainwright, "Union Claims CityRail Spied on Employees" Sydney Morning Herald (3 November 1999) at 10.*
6. *NSW Council for Civil Liberties, Submission at 1.*
7. *NSW Council for Civil Liberties, Submission at 2.*

reasons for surveillance usage, there is evidence of public support for its continuation.[8]

3.8 The following categories set out what, in the Commission's view, are the justifiable purposes of overt surveillance. However, as the means used to achieve these ends and their degree of intrusiveness vary greatly, the Commission should not be understood to be endorsing all applications of surveillance technology which aim at achieving these objectives.

Protection of people and property

3.9 The most obvious purpose of overt surveillance is the attempt to provide security for persons and property. The chief interests served by surveillance in this context are those of the general public and the agencies charged with responsibility for law enforcement. Such surveillance is carried out by those agencies, as well as private investigators, private companies and individuals. The principal means by which overt surveillance devices provide protection is by acting as a deterrent. Knowledge of the presence of a device which can detect the commission of a theft, assault, vandalism, or some other criminal or anti-social act, and which can assist in identifying the perpetrator, should stop a rational person who is mindful of the consequences from engaging in such an act. The overt nature of these devices is thus intrinsic to their effectiveness. This may explain why such devices are often left to record the scene without anyone simultaneously studying the monitor. A spin-off advantage of their visibility is that in a location such as a shopping

---

8. Some evidence of support from various sections of the public can be gleaned from newspaper reports. "Calls for the urgent introduction of surveillance cameras into Wagga's main street received overwhelming support at an anti-violence meeting in the city last night": Daily Advertiser (Wagga Wagga) (4 April 1997) at 1. "Principals at schools suffering from violent incidents want surveillance cameras installed": Sun-Herald (Sydney) (29 June 1997) at 11. "Cab drivers in Sydney are pressing for trials of a camera in their taxis, offering them protection by photographing their passengers": Sun-Herald (Sydney) (10 May 1998) at 5.

or entertainment district, members of the public may derive reassurance from the presence of such devices. This may bring people in greater numbers to an area that has suffered from a dearth of visitors in the past, and this fact in itself may assist in bolstering safety. If, however, the deterrent effect should fail, then the device nevertheless yields information through recordings, which may be of use in the detection and prosecution of the offender, or for leverage in obtaining a confession so as to obviate the need for prosecution.

3.10 Another possible flow-on advantage of the "overtness" of the security devices is a so-called "diffusion of benefits".[9] This is the phenomenon whereby the use of notified surveillance devices has led to a reduction in crime beyond the expected target area. This is in contrast to the displacement effect.[10] In one example, after CCTV had been installed on five buses, vandalism and misbehaviour were reduced throughout the whole fleet of 80 buses.[11] Another study found that following the installation of CCTV in some of the parking lots on a university campus, vehicle theft was reduced to an equal degree in all the parking lots, even one that was not monitored.[12]

3.11 While CCTV is currently the usual method of carrying out surveillance for such purposes, technological developments may well change this. For example, in the United States, the National Institute of Justice, a branch of the Justice Department, is sponsoring research into several types of concealed weapons detection technology.[13] These remote scanners rely on different technologies[14] to "frisk" subjects electronically for concealed

---

9. Clarke and Weisburd cited in R V Clarke (ed), Situational Crime Prevention: Successful Case Studies (2nd edition, Harrow & Heston, Albany NY, 1997) at 32.

10. See para 3.71.

11. Poyner cited in Clarke at 32.

12. Poyner cited in Clarke at 32.

13. M Hansen, "No Place to Hide" (August 1997) 83 ABA Journal 44 at 46.

14. Passive millimetre wave imaging, for example, relies on variations in the electromagnetic rays emitted by the body and by objects on or around it to produce an image of the objects against a contrasting image of the body. Back-scattered x-ray imaging uses a low-energy x-ray beam to scan the body surface. The reflection of the beam off the

weapons or other objects. Handheld versions of such devices are also being developed,[15] and are likely to be employed initially by police and prison officers, and ultimately in the private sector by, for example, security guards. Glimpsing the future, applications are expected to include a device not dissimilar to the "x-ray specs" familiar to earlier generations of comic book readers.[16]

Protection of the public interest

3.12 While this category and the previous one overlap, here we include the use of overt surveillance devices to monitor situations in which large numbers of people may be affected adversely, although not necessarily from criminal or antisocial behaviour. Again, the interests of the general public in being protected, and of law enforcement agencies in receiving vital support to carry out their work, are intended to predominate. A range of scenarios may be envisaged.

Crowd control

3.13 Crowd control at a major sporting or other large event is one obvious example. CCTV is again likely to be the main mode of device employed to monitor the situation, in conjunction with the presence of police and other security personnel. The presence of known troublemakers might be ascertained through the use of a

---

skin is combined with advanced computer image-processing techniques to create a display of the person and any concealed weapons: Hansen at 47; J Collins "Privacy or Safety: A Choice You Soon May Not Be Able to Make" «205.243.76.8/rcreader/19cov.html».

15. *National Law Enforcement and Corrections Technology Center, "Handheld Acoustic System for Concealed Weapons Detection" «nlectc.org/techproj/nij_p38.html»; Hansen at 47.*
16. *"Longer term [regarding applications for holographic imaging radar], scientists at Pacific Northwest are working on perfecting "x-ray specs". Concealed vest-mounted units that allow images to be displayed on a visor or via specially designed glasses could help security personnel to covertly monitor crowds for weapons": Ingersoll-Rand Company, "Nowhere to Hide" Compressed Air Magazine October/November 1996 «ingersoll-rand.com/compair/octnov96/radar.htm».*

biometric surveillance system, such as "Mandrake",[17] although this would not be an overt usage unless notice were given through signposting or widespread publicity.

National security

3.14 There may be cases when overt surveillance devices are used in the national interest. Devices capable of detecting the presence of weapons and explosives are used at sensitive locations, such as airports and parliament buildings, where walk-through scanning machines and others for monitoring hand luggage are familiar sights. New technologies[18] in this area are advancing at a rapid rate and may come to be used overtly.

Coastal surveillance

3.15 The Australian Customs Service and the defence forces also use surveillance to guard the nation's extensive coastline against entry on land or in Australian waters of illegal immigrants, fishing fleets and drug importers. Radar is employed for this purpose, including the newly developed "Jindalee Over the Horizon Radar" for wide-area surveillance.[19] The Federal Government has announced new measures to detect illegal immigrants, including an increase in the number of electronic surveillance aircraft to extend Coastwatch's aerial surveillance of, particularly, Australia's east coast.[20] These devices could, arguably, be referred to as overt,

---

17. *This face recognition software system, launched by Newham Council in the United Kingdom in October 1998, was designed to identify "target faces" amongst crowds of people: London Borough of Newham Communications Unit, "Newham Council Launches 'Face Recognition' in the UK" «www.newham.gov.uk/press/julythrunov98/ facereg.html»; Visionics Corporation, "Visionics FaceIt is First Face Recognition Software to be Used in a CCTV Control Room Application" «www.faceit.com/Newsroom/PRs/98newham.htm».*
18. *See para 3.11.*
19. *D H Sinnott, "The Development of Over-the-Horizon Radar in Australia" «www.dsto.defence.gov.au/corporate/publicity/brochures/ othr/othr1.html».*
20. *J Marsh, "$124m Plan Targets Illegal Migrant Scam" Sydney Morning Herald (28 June 1999) at 1.*

because most of their subjects, whether actively trying to elude detection or those relying on radar for navigational safety, are likely to have some awareness or, at least, expectation of their deployment.

Road safety

3.16 Cameras monitor busy intersections so that traffic lights and lane directions can be adjusted where applicable to facilitate traffic flow and to help emergency vehicles reach their destinations. Police are also equipped with such overt surveillance devices as breathalysers and speed cameras (the use of which are often notified), used in the furtherance of public safety.

Aiding identification of persons

3.17 Biometric surveillance techniques[21] can assist in recognition and verification of personal identification, and therefore have many applications pertinent to what might be broadly termed "the public interest". Again, there may be some overlap with other functions discussed above. Biometrics can be used to provide "robust authentication" for access to computer systems containing sensitive information pertaining to military, intelligence and other top-level government functions.[22] According to one report,[23] Australia could soon see the introduction of fingerprint identification for ATM use, and voice recognition technology to telephone banking.

---

21. See para 1.16.

22. Biometric Consortium, "Government Applications and Operations" «www.biometrics.org/REPORTS/CTSTG96».

23. G Safe, "Fingerprints to Beat Bank Fraud" The Australian (4 January 2000) at 1.

3.18 Overseas, border control is made possible through systems already installed in North America.[24] The Colombian Legislature has, since 1992, used hand geometry biometrics to verify the identity of members of its two assemblies immediately prior to a vote.[25] The National Crime Information Centre in the United States plans to install automated systems in patrol cars to allow the relaying of fingerprints to the relevant authorities.[26] The United States is also considering the use of biometrics to aid in processing passport and visa applications.[27] A major advantage of this is to prevent individuals from applying for multiple passports under assumed names. One possible method is by adding a record of the applicant's thumbprint and photograph to a database. A verification system would then compare the print to others on the database, to check for matches.[28] The detection of fraud in, for example, applications for social security payments, is potentially the greatest area for the use of biometric surveillance.[29] Spain's TASS

---

24. Biometric Consortium. INSPASS (Immigration and Naturalization Service's Passenger Accelerated Service System) was designed to allow faster admission for frequent travellers to the United States, uses hand geometry to verify identity, and has been installed at, for example, John F Kennedy Airport, New York. CANPASS (the Canadian version of INSPASS) uses fingerprint biometric, and is designed to facilitate transfer of persons and goods between Canada and the United States. PORTPASS is another Immigration and Naturalization Service system, and it monitors people in vehicles at borders through a voice recognition biometric. It is currently in use at the US border with Canada, with planned introduction on the border with Mexico.

25. Biometric Consortium.

26. Biometric Consortium.

27. Biometric Consortium.

28. SJB Services, "Biometric identity system applied to an entire country" (news release) «www.sjb.co.uk/pr/19079601.txt».

29. Nevertheless, "[w]hen electronic fingerprinting was introduced five years ago, it caught the imagination of politicians who saw it as the ultimate high-tech weapon to fight welfare fraud. ... Yet there is little evidence that so-called finger imaging – intended to deter would-be double-dippers using fake identity papers – has had any significant impact in preventing fraud. In fact, a study by the state three years ago found that other welfare changes had made finger imaging

program combines smart card technology with fingerprint biometrics to prevent duplication in the country's social security system and to secure access to personal information relating to pensions, unemployment and health benefits stored on the smart cards.[30] Similar schemes operate in the United States, such as the AFIRM system in Los Angeles.[31] This kind of surveillance would in most cases be carried out overtly, because of the need for the subjects' co-operation in presenting their fingerprints or other identifying traits. Again, such "overtness" can boost the effectiveness of the surveillance. In one example concerning American military retirees living abroad, suspicion that benefits were still being collected on deceased retirees was confirmed by the failure of many to appear in order to enrol their fingerprint in the new identification system.[32]

---

largely superfluous from the outset. But the state has refused to make that $658,000 study public, and now calls it outdated and flawed:" N Bernstein, "Experts Cast Doubt on Worth of New York Plan to Fingerprint for Medicaid" New York Times (30 August 2000) «www.nytimes.com/library/tech/00/08/biztech/articles/30finger.html».

30. *Biometric Consortium. "It is anticipated that all of Spain's citizens will have their own cards by the end of this century.": Unisys, "Spain Selects Unisys as Partner for National Social Security Identification Card Project" (news release) «corp2.unisys.com/AboutUnisys/PressReleases/1996/jan/01175960.html».*
31. *Automated Fingerprint Image Reporting and Match, introduced in 1991, to reduce fraudulent and duplicate welfare benefits. A saving of $5.4 million was reported following the first six months' use, and this is still growing. The system has been extended to other parts of California: Biometric Consortium. New York, New Jersey, Connecticut, Massachusetts and Pennsylvania are among other states that are or will be using similar programs: Committee on Banking and Financial Services, US House of Representatives, "Statement by Jeffrey S Dunn, Chairman, Biometric Consortium" «www.house.gov/banking/52098jd.html».*
32. *Committee on Banking and Financial Services, US House of Representatives, "Statement by Jeffrey S Dunn, Chairman, Biometric Consortium" «www.house.gov/banking/52098jd.html».*

Collection of material for news and entertainment

3.19 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. Those who purchase such publications, impliedly endorse this kind of surveillance, and the interests of the media are served through returns in revenue, the most obvious example in recent times being the unrelenting coverage of the late Princess of Wales.

Workplace surveillance

Occupational health and safety

3.20 It may be considered necessary to monitor a workplace because of some safety concern or hazard particular to that industry.

Recording transactions

3.21 In some instances it may be necessary to undertake surveillance in order to have a record of an event or transaction, to ensure that proper procedures were followed or to protect a legitimate interest. Calls to emergency services are monitored in this way. Certain dealings conducted by telephone may be taped in order to record a client's instructions, such as the use of client/dealer taping systems by stockbroking firms.[33] The Sydney Futures Exchange ("SFE")[34] is open about its use of surveillance technology

---

33. For example, J Heywood, "Were Says Two Men in Dealer Row Have Quit" Sydney Morning Herald (25 August 1998) at 27; J Rouw, "Were Find 'Clean as a Whistle'" Sydney Morning Herald (8 August 1998) at 92.

34. Sydney Futures Exchange Limited, Submission at 1. The SFE also operates, with the knowledge of its members, a computerised trading system, Sydney Overnight Computerised Market (or SYCOM), which is monitored by SFE surveillance staff to ensure no rules have been breached.

to assist in fulfilling its statutory obligation to ensure an orderly futures market.[35] *Aural and optical surveillance are conducted on the trading floor, and telephone conversations from the floor are taped.*[36] *Members are aware of the surveillance, and their clients are given notice of the telephone taping by means of a client agreement form.*[37] *Employers and company shareholders are the main beneficiaries of surveillance in the workplace, but the public also stands to benefit by, for example, lower prices flowing from reduced stock losses, improved efficiency of service, and better safety and security measures.*

Performance monitoring

3.22 Performance monitoring is a form of overt surveillance that arises specifically in the employment context. The phrase "performance monitoring" can be defined as meaning "the random or continuous surveillance of employees for the purpose of monitoring individual work performance". As will be discussed below, this form of surveillance can be undertaken in a range of ways and for a number of purposes. The Commission considers that while certain forms of performance monitoring are justifiable uses of overt surveillance, others should be subject to the authorisation regime. Accordingly, we have identified performance monitoring as a form of overt surveillance requiring particular attention.

3.23 ***Types of performance monitoring.*** *Performance monitoring can take a variety of forms. Commonly used practices are those designed to assess how well an employee is carrying out his or her work duties. For example, an employer can use computer-based devices to record the keystroke rate of a data entry operator or can record the length of time a switchboard operator takes to answer the telephone. In addition to utilising types of monitoring directly*

---

35. *Section 1137(1) of the Corporations Law (Cth) states: "A futures exchange ... shall, to the extent that it is reasonably practicable to do so, take all steps, and do all things, necessary to ensure an orderly and fair market for dealings in futures contracts on a futures market of the futures exchange."*
36. *Sydney Futures Exchange Limited, Submission at 1-2.*
37. *Sydney Futures Exchange Limited, Submission at 2. The client also has the right to listen to any recording in the event of a dispute.*

linked to performance assessment, employers engage in performance monitoring practices such as scanning employee e-mail and Internet use.

3.24 "Investigator"[38] is an example of performance monitoring software currently used by Australian employers.[39] This monitoring tool logs all employee Internet and e-mail use and has the ability to record every keystroke, programme used and file opened or copied. The collected information can be automatically e-mailed to a supervisor or employer in a searchable report.[40]

3.25 ***Purposes of performance monitoring.*** *As with surveillance in general, employers engage in overt performance monitoring for a number of reasons. The traditional reasons for using this form of surveillance are to improve productivity, to ensure work quality and to aid performance evaluation.*

3.26 Many employers consider that performance monitoring is an effective means of improving employee productivity and ensuring the quality of employees' work.[41] Through the use of surveillance, employers can achieve a level of supervision akin to having a human supervisor sitting next to each individual employee for every moment of their working day;[42] surveillance devices can detect every second an employee is absent from his or her computer, details of every Internet site visited can be recorded, the length of every telephone call can be noted. In addition to the basic effect of replicating constant human supervision, the incentive of performance-based bonuses and the threat of sanctions are viewed by many employers as a way of motivating employees to work

---

38. *A software product produced by WinWhatWhere Corporation.*
39. *According to the president of WinWhatWhere, two Australian government departments hold 62 Investigator licences and a further 60 are held by various Australian companies: M Bryan, "Every step you take, every move you make …" Australian Financial Review (4 March 2000) at 27.*
40. *Bryan at 27. See also «http://www.winwhatwhere.com».*
41. *J Flanagan, "Restricting Electronic Monitoring in the Private Workplace" (1994) 43 Duke Law Journal 1256 at 1260.*
42. *New South Wales, Privacy Committee, Invisible Eyes: Report on Video Surveillance in the Workplace (Report 67, 1995) at 31.*

more effectively.[43]

3.27 Performance monitoring can aid performance evaluation by providing a detailed and objective measure of an employee's work.[44] *Rather than relying on second hand reports or periodic observation, a supervisor can see or read what an employee does throughout their entire day.*[45] *This reduces the possibility of bias affecting performance evaluation and provides an accurate record of an employee's performance. Indeed, employers claim that computer monitoring provides the most objective and well-recorded basis possible for making fair evaluative decisions about performance.*[46] *In addition to improving the quality of performance evaluation, the use of non-human performance monitoring is said to have the added advantage of reducing or removing the need for human supervision to carry out that function.*[47]

3.28 As concerns regarding employer liability for employee action have risen, employers are also monitoring employees to guard against liability for matters such as sexual harassment, discrimination and defamation. The use of performance monitoring to protect against employer liability for employee action is primarily an exercise in detecting misconduct. It is particularly prevalent in respect of Internet and e-mail use. Employers' desire to check up on employee activity in cyberspace has been increased by cases such as the libel proceedings brought by Western Provident Association against a British company, Norwich Union, following the appearance of messages on Norwich Union's internal e-mail system falsely suggesting that Western Provident was in financial difficulty. The case was settled, with Norwich Union paying £

43. *Privacy Committee (1995) at 31.*
44. *Flanagan at 1260.*
45. *L Hartman, "The Rights and Wrongs of Workplace Snooping" «www.depaul.edu/ethics/monitor.html».*
46. *A Westin, "Monitoring and New Office Systems" Part II of "Employee Privacy, Monitoring and New Technology" Chapter 6 of Arbitration 1988: Proceedings of the Forty-First Annual Meeting of the National Academy of Arbitration (Bureau of National Affairs, Washington, DC, 1989) at 169.*
47. *Privacy Committee (1995) at 31.*

450,000 and making a public apology.[48] A similar warning to employers was sent by the settlement by the Chevron Corporation of a sexual harassment case brought by four female employees for $2.2 million; the case centred on an e-mail called Why beer is better than women.[49] Such cases may be of significant interest to Australian employers in light of surveys, such as that conducted by Content Technologies, which discovered that two in three workers at large companies are aware that inappropriate e-mail is freely circulating throughout the internal e-mail system.[50]

PROBLEMS WITH USING OVERT SURVEILLANCE

Privacy

Someone is watching

3.29 The threshold problem with surveillance remains the act itself: being watched or otherwise monitored. The potential intrusion on personal privacy through the use of surveillance devices was discussed at paragraph 1.14 and following. It is the most immediate concern with surveillance usage, regardless of whether the devices are employed overtly or covertly. Covert surveillance is potentially more intrusive than surveillance carried out openly for a number of reasons: the surveillance is likely to be targeting a particular individual or group; the context may be more intimate, which may also mean there is less background noise or

---

48. D J Freeman, "Legal issues concerning e-mail" «www.djfreeman.co.uk/pubs/m-email.htm»; McCann FitzGerald "Libel and Internal E-mail Systems: The impact of the Norwich Union case" «www.mccann-fitzgerald.ie/legal_briefing/litigation_arbitration/email_libel.html» .

49. A Carson and D Farrant, "Saving Private E-mail" The Age (4 March 2000) at 3; S Silverstein, "Survey finds more than one-third of employers snoop on workers" Los Angeles Times (23 May 1997) «seattletimes.nwsource.com/extra/browse/html97/altpriv_052397.html ».

50. J Rolfe, "Office email abusers run riot" Daily Telegraph (24 March 2000) at 101. See also S Long, "Think before you click and forward" Australian Financial Review (15 November 2000) at 51.

obstructed vision; the technology employed may be more sophisticated, having greater precision and more capabilities; and, of course, the subject, being ignorant of the surveillance, is likely to engage in unguarded conversation or acts.

3.30 Nevertheless, overt surveillance brings its own particular privacy issues. In its lack of targeting, overt surveillance is analogous to fishing with a fine mesh net. Everything within range is captured, whether relevant to the purpose or not. In most cases, the surveillance is random, and carried out on people who are simply going about their daily business. Those who make a point of being visible in public, for example through exercising their democratic right to attend or address rallies and demonstrations, face a greater likelihood of having their images captured. Without sufficient safeguards, such images could find their way into files, like those kept by the now disbanded New South Wales Police Special Branch.[51] This could have a dissuasive effect on citizens wishing to participate actively in a democratic society.

3.31 Some concern has been expressed[52] in the United States about recent developments in surveillance technology, deployable overtly or covertly, which allow the detection and imaging of concealed weapons and drugs on the person. In response to objections on

---

51. The Special Branch was disbanded in 1997 following criticism by the Police Royal Commission ("the Wood Commission"). Opening the files for inspection by people who were the subject of Special Branch activities, the Premier, Mr Bob Carr, said: "People ought to be able to do what you can in a democracy – stand outside a government building or a courthouse with a protest sign without having their names recorded by people pretending they are Special Branch agents in the FBI": D Murphy, "Special Branch Files Now Marked Open for Inspection" Sydney Morning Herald (10 March 1999) at 6. Examples include a street protest in the early 1980s by "Women Behind Bars", a group advocating rights for female prisoners, which resulted in the compilation of a file on those present: D Murphy, "Special Branch Files Now Marked Open for Inspection" Sydney Morning Herald (10 March 1999) at 6.

52. M Hansen, "No Place to Hide" (August 1997) 83 ABA Journal 44 at 47.

privacy grounds to personal "searches", it has been argued[53] that the scan is less intrusive than a manual "pat-down".[54] The lack of physical contact certainly has this advantage, as well as being safer for police. The fear is, however, that this remote capability will make overt, but unwarranted "searches" possible.[55]

Data protection

3.32 The other major privacy issue centres on the information gathered or generated by surveillance activities, and the proper way of dealing with it, so as to protect reasonable expectations of privacy.

3.33 Examples occasionally come to light of the questionable use of such material.[56] One notorious case was a videotape compilation of segments taken from security cameras at Perth's Burswood Casino and aired by a commercial television station.[57] The tape included footage of zoom shots down women's blouses and up their skirts, as

---

53. Ingersoll-Rand Company, "Nowhere to Hide" Compressed Air Magazine October/November 1996 «ingersoll-rand.com/compair/octnov96/radar.htm».

54. However, concern has been expressed at the degree of intrusiveness made possible by the technology. According to one unnamed critic, cited by Hansen, a radar skin scanner is being developed which is able to produce an anatomically correct image so precise it can reveal whether or not a man has been circumcised: Hansen at 46.

55. In America, constitutional issues have been raised, such as whether using such devices can constitute a search, and, if so, whether the failure to obtain a warrant for their use violates the Fourth Amendment. The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

56. See also para 4.46.

57. An earlier application by the Casino for an injunction to prevent the screening was unsuccessful as it was held to be in the public interest: C Egan, "Casino Video Sees Call for a Code" The Australian (5 July 1994) at 4.

well as sexual scenes.[58] Another tape reportedly in circulation was a compilation of footage from a security camera installed in the ceiling of a lift, and showing people having sexual intercourse.[59] In England, a film entitled "Caught in the Act" showed sexual acts taking place in doorways, muggings, fights and burglaries.[60]

3.34 The issue is more complicated, however, than simply determining what to do with the film from a surveillance camera. Developments in surveillance have overlapped significantly with those in other fields, particularly that of information technology, which, over the past few decades, has brought considerable benefits in the acquisition and communication of information, along with a diminution in personal privacy. There is an analogy to be drawn between surveillance and information technology, with its uneasy relationship to the concept of privacy, especially as it relates to data.

3.35 The term "information technology"(or "IT") was first used in the 1970s to describe a coalescence of computing and telecommunications,[61] nowadays connoting all those technologies, whether electrical, electronic or mechanical, concerned with information, that is its processing, storage, retrieval and communication.[62] The privacy problems associated with IT have generally sprung from its capability to store, collate and transfer vast amounts of information.[63] The focus of surveillance is on obtaining information, generally in a retrievable form.

---

58. C Egan, "Casino Seeks Ban on Secret Footage" The Australian (4 July 1994) at 3.

59. F Walker, "Love in Lift Spy Row" Sun-Herald (11 June 1995) at 5.

60. Q Burrows, "Scowl Because You're on Candid Camera: Privacy and Video Surveillance" (1997) 31 Valparaiso University Law Review 1079 at 1100.

61. C Edwards, N Savage and I Walden (eds), Information Technology and the Law (2nd edition, Macmillan, London, 1990) at 2.

62. Edwards, Savage and Walden at 2; Australian Broadcasting Corporation, "In the Pipeline: Alphabetical Glossary" «www.abc.net.au/pipeline/radio/programs/glos2.htm»; R Hinton, Information Technology and How to Use It: A Handbook of Effective Practice (ICSA Publishing, Cambridge, 1988) at 2.

63. Edwards, Savage and Walden at 3.

3.36 Information, and very often personal information,[64] is the currency common to surveillance and IT. We might previously have distinguished between the technologies of surveillance and information by regarding the former as monitoring the activities of the living, breathing person, as opposed to the information about them, held on some databank. However, the convergence of technologies, that is, the breakdown of barriers between what were largely separate technologies so that they may interact, has changed this. The demarcation between surveillance and other technologies is becoming less clear.[65] Today, surveillance could be regarded as an information technology.

3.37 The same devices can be used in both areas. For example, a cellular telephone, a medium for communication, can also serve as a signalling and bugging device because of radio frequency energy emissions which are capable of being intercepted. Satellites are another form of technology harnessed for both communications and surveillance. Fingerprint and facial recognition, along with other biometric technologies, can establish identity to guard against fraud, but also have a more dynamic surveillance application where indicating a person's whereabouts, for example, within a sports

---

64. Sections 4(1) and 4(2) of the Privacy and Personal Information Protection Act 1998 (NSW) define "personal information" as "information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion" and includes fingerprints and genetic characteristics.

65. For example, the use of a digital camera for roadside traffic enforcement has many advantages over a traditional camera, which requires film to be changed, processed, and kept secure. Images captured by digital cameras can be downloaded to a computer, and, with the use of number plate recognition software, the vehicle's owner can be identified almost immediately: United Kingdom, House of Lords Select Committee on Science and Technology, Digital Images as Evidence (Fifth Report, 1997-98, HL 64) at 1.4. Digital cameras have, incidentally, been installed in the tunnel of Sydney's Eastern Distributor: S Gee, "Secret Cameras: Hidden Speed Checks in Tollway" Daily Telegraph (6 June 2000) at 1, 3.

stadium.[66] *Highway monitoring systems, which can be utilised for such diverse purposes as reducing traffic congestion or deducting tolls from pre-paid accounts, can also monitor an individual's traffic activity, such as:*

> *when and how often a traveller uses the roadway; how he drives, including travel habits such as vehicle speed or lane changes; at what points he makes stops along the way; and whether his vehicle is performing efficiently. As the system acquires this personal information through surveillance, it can store the information in a database for future analysis. In this way [such systems] combine surveillance and information technologies so that the system can be used for real-time monitoring and for later use in compiling an information mosaic.*[67]

3.38 Merging the capabilities of surveillance and information technologies can enhance their effectiveness. For example, the Australian Transaction Reports and Analysis Centre (AUSTRAC) provides support to law enforcement and revenue agencies by "providing an alerts system which notifies the relevant user when a report entering the database matches a specified name, address or account number" and "running automated monitoring so that [its] database can identify patterns of financial activity which may be indicative of money laundering, other serious crime and tax evasion."[68] *Computers can thus be a repository of data on previous transactions, while simultaneously performing a surveillance function by monitoring a person's activity in real time, and then*

---

66. *"If the technology continues to develop as expected it may in the future be possible to match data from the digitised passport photographs that are coming into use with other databases, enabling the rapid identification of individuals who were, for example, attending a football match": United Kingdom, House of Lords Select Committee on Science and Technology, Digital Images as Evidence (Fifth Report, 1997-98, HL 64) at 4.18.*
67. *T B Kearns, "Technology and the Right to Privacy: the Convergence of Surveillance and Information Privacy Concerns" (1999) 7 William and Mary Bill of Rights Journal 975 at 996-97.*
68. *Australia, Australian Transaction Reports and Analysis Centre, Annual Report 1998-99 at 7.*

aggregating this information. The United States Financial Crimes Enforcement Network (FinCEN) can locate an individual by observing activity on his or her credit card as it occurs, and pinpointing the location each time. FinCEN is also capable of conducting surveillance through sophisticated data searches, combing through data held by the network, looking for indicators of suspicious financial activity.[69] A different scenario is hypothesised in the following:

> *You're walking down Elizabeth Street when your phone beeps. It's not a friend reminding you about lunch or your boss setting up a meeting, it's an offer from David Jones [a department store]: "If you come into our store in the next 30 minutes, we'll give you 30 per cent off all Paul Smith suits." How did they know you had a penchant for Paul Smith? They have access to your purchasing history at DJs. How did they know you were walking past the store? Your phone reveals your location and wireless technology allows them to send you special deals when you're nearby.[70]*

3.39 The advantages gained by many sectors of society in merging these technologies makes it likely the trend will continue. Therefore, a major concern with surveillance is akin to that of other information technologies, namely protecting the information, or data, garnered through utilisation of the technology.

3.40 From the foregoing, it is easy to see how the information gathered by means of overt surveillance, and the data processed through other IT applications, can become conjoined. In New South Wales, section 9 of the Privacy and Personal Information Protection Act 1998 requires that personal information cannot be collected except directly from the individual concerned (or from some other authorised person). However, the Act only applies to public sector agencies. As far as the private sector is concerned, information obtained legally by surveillance and other means can sit together on one database, where it can be bought, sold or used in other ways

---

69. Kearns at 998.

70. K Crawford, "Beep on the Street: it's the Internet" Sydney Morning Herald (14 January 2000) at 1-2.

with little restriction.[71]

Public concern over privacy

3.41 Information and privacy have been competing interests throughout the latter half of the twentieth century and beyond. In this relatively short period, concern with the privacy implications of the new technological developments and their uses has waxed and waned. Early privacy activism has, on many fronts, given way to either complacency or surrender.[72] *While these attitudes still exist, there is also considerable evidence of growing awareness of, and concern at, threats to privacy.*

---

71. *The Privacy Amendment (Private Sector) Act 2000 (Cth), commencing late in 2001, will have some impact on this situation as regards large companies.*

72. *Since 1980, there seems to have been "a shift in the perception of privacy and privacy invasion, rather than a diminution of public concern. The effect is an ambivalence that retards consumer and political activism over even the most blatant privacy intrusions. In many countries, fundamental changes have taken place in society's approach to traditional privacy issues.": S G Davies, "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity" in P E Agre and M Rotenberg (eds), Technology and Privacy: The New Landscape (MIT Press, Cambridge, Massachusetts, 1997) at 143-165. In a series entitled "The Surveillance Society", which appeared in The Village Voice during September-October 1998, Mark Boal notes "Surveillance scholarship was hip in the '60s and '70s, but academic interest has dropped noticeably in the past 20 years". He cites one reason for this "apathy" as being dependence by academia on government funding, which is less likely to be forthcoming for surveillance research than for surveillance hardware: M Boal, "Part One: Spycam City" The Village Voice «www.villagevoice.com/features/ 9840/boal/shtml».*

3.42 ***Complacency.*** *According to Simon Davies,[73] director general of Privacy International, a non-government watchdog organisation based in Washington DC, public concern over surveillance has been "neutralised" by such factors as "the illusion of voluntariness", the forging of "partnerships" between surveillance users and their subjects, and the introduction of data protection principles. The experiences Davies refers to are more common overseas, but have increasing applicability in Australia.*

3.43 The "illusion of voluntariness" refers to the inclusion of a voluntary component in surveillance schemes. Davies suggests this may have the effect of neutralising concern on the part of the public who might regard non-volunteers as having brought trouble on themselves.[74] There is a useful analogy in the Australian Tax File Number ("TFN") scheme. The TFN is used as an identifier, and is not required to be quoted in respect of a range of financial transactions. However, if one chooses to exercise the option of not quoting a TFN, financially disadvantageous consequences may follow.[75] Another interesting example occurred recently in the town of Wee Waa, in the State's north-west. Following a brutal assault there, police requested all male residents of the town between the ages of 18 and 45 to submit to voluntary DNA testing by means of

---

73. S G Davies, "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity" in P E Agre and M Rotenberg (eds), Technology and Privacy: The New Landscape (MIT Press, Cambridge, Massachusetts, 1997) at 144.

74. Davies at 159.

75. "The Income Tax Assessment Act 1936 (Cth) does not require a taxpayer to quote a tax file number, but provides for the imposition of the highest prescribed rate of tax where a tax file number is not quoted. Employees may lodge an employment declaration with their employer in which they may quote their TFN. Where an employee has declined to quote their TFN, the employer is required to deduct tax from the employee's salary or wages at the highest prescribed rate. ... Investors may quote their TFNs to the investment body connected to their investment. Where an investor has declined to quote his or her TFN, the relevant investment body is required to deduct tax from the investment income at the highest prescribed rate": Halsbury's Laws of Australia (Butterworths, Sydney, 1996) Volume 25 at [405-31445].

saliva samples.[76] Civil libertarians expressed concern that, although there was no legal compulsion to submit to testing, those who chose not to might be vilified by their community. The question must arise in such cases as to how voluntary the actions of the residents are, given the weight of community pressure to do so.

3.44 Recasting the relationship between surveillance users and surveillance subjects as a "partnership" is another factor contributing to complacency, according to Davies. This reassures the public that their interests are represented. All parties appear to be stakeholders in a common project with mutually beneficial objectives, principally that of reducing crime. The emphasis is on the positives, and detailed analysis of possible disadvantages may be lacking.

3.45 Privacy concerns over surveillance may also have been defused by the introduction of data protection principles, says Davies, although this is more likely to be true in a European context because of a greater focus there on the subject.[77]

---

76. C Ho, "Libertarians Cry Foul at DNA Tests for Rape Investigation" Sydney Morning Herald (10 April 2000) at 8.

77. The first data protection law was enacted in Hesse, Germany, in 1970, followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978). From these evolved two international instruments, the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, and the OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. More recently, the European Union has enacted stronger data protection in its European Data Protection Directive (Directive 95/46/EC), with each EU State required to enact complementary legislation by October 1998, although this process has not been completed. "The key concept in the European model is 'enforceability'. The European Union is concerned that data subjects have rights that are enshrined in explicit rules ... Every EU country will have a Privacy Commissioner or agency that enforces the rules": "Privacy and Human Rights 1999: An International Survey of Privacy Laws and Developments" «www.privacyinternational.org/survey/Overview.html#Heading6» . The full text of the directive can be found at «europa.eu.int/eur-

In December 2000, the Privacy Amendment (Private Sector) Act 2000 (Cth)[78] was passed. Data protection has taken centre stage not only because of its privacy implications, but also because of national interests in promoting trade and electronic commerce.[79] According to Davies, however, these "appear to have satisfied some of the concerns of information users and the public, but have failed to stem the growth of surveillance".[80]

3.46 A local illustration of complacency regarding privacy issues which many can recall was the Australia Card controversy, which flourished for two and a half years, from April 1985. The green and gold identity card's purpose was stated by the then Federal Government to be a means of reducing tax evasion, welfare fraud and illegal immigration.[81] The entire population was to be issued with cards carrying unique identifiers, and this information would be kept on a central register which could be accessed by government agencies such as the Australian Taxation Office ("ATO") and the

---

lex/en/lif/dat/1995/ en_395L0046.html».

78. *The Act incorporates the National Principles for the Fair Handling of Personal Information, developed by the Federal Privacy Commissioner, setting out standards for the collection and use of personal information by business and other private sector organisations.*

79. *Directive 95/46/EC also provides that data should only be transferred to a non-EU country if adequate safeguards are in place: European Union, "Media, Information Society and Data Protection" «europa.eu.int/comm/dg15/en/media/dataprot/news/925.htm».*
For an example of measures being taken by non-EU countries to comply with this "adequacy" provision, see United States, Department of Commerce, "Draft International Safe Harbor Privacy Principles" «www.ita.doc.gov/td/ecom/Principles1199.htm»: "While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from ... [the European Union's comprehensive privacy legislation]. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation."

80. *Davies at 144.*

81. *R Clarke, "The Resistable Rise of the National Personal Data System" «www.anu.edu.au/people/ Roger.Clarke/DV/SLJ.html».*

Department of Social Security. The Australia Card Bill 1986 (Cth) encountered so much opposition in Parliament and from the public, that in September 1987 the Bill was withdrawn.[82] *Subsequently, the Government announced details of proposed amendments to the Tax File Number ("TFN") scheme, used by the ATO since the 1930s. A number of safeguards were to be incorporated, so that the TFN scheme would apply only to taxation administration. The scheme became law in 1988. By 1990, organisations other than the ATO authorised to use the TFN system included the Department of Social Security, the Department of Employment, Education and Training, the Child Support Agency and higher education institutions (in relation to the Higher Education Contribution Scheme). There are now 13 Commonwealth acts which regulate the purpose and use of tax file numbers.*[83] *The expanding role of the TFN has caused little comment.*

3.47 ***Surrender.***

> *In effect, we have traded some of our rights to privacy in public spaces for increased security [through the use of CCTV]. Most of us think this is a price worth paying.*[84]
>
> *Yet citizens may be willing to sacrifice some measure of privacy in order to cut back on fraud [by using biometric technology].*[85]
>
> *You already have zero privacy. Get over it.*[86]

---

82. *R Clarke, "The Resistable Rise of the National Personal Data System" «www.anu.edu.au/people/ Roger.Clarke/DV/SLJ.html».*
83. *Australia, Australian National Audit Office, Management of Tax File Numbers: Australian Taxation Office (Audit Report 37, AGPS, Canberra, 1998-99) at para 1.10 and appendix 1.*
84. *Jack Straw, UK Home Secretary, quoted by P Newton, "'Spy' Cameras Backed" Daily Telegraph (London) (13 May 1999) at 8.*
85. *"Identity Checks Test Big Brother Fears" (editorial) The Australian (4 January 2000) at 10.*
86. *Scott McNealy, chief executive officer of Sun Microsystems, at a product launch in January 1999, responding to concerns that various computer operating systems contain unique identification numbers which make it possible to track individual users: quoted in various sources eg J Markoff "Growing Compatibility Issue: Computers and User Privacy" New York Times (3 March 1999) at A1.*

By surrender, we mean the willingness to give up part of the privacy we would otherwise feel entitled to enjoy. As the quotations above illustrate, the public is sometimes prepared, and sometimes exhorted, to do so in exchange for some claimed benefit. New information technologies and applications are sometimes introduced with an admission that they may carry a small privacy cost, but one either worth paying or of little serious consequence.

3.48 When the announcement was made[87] in late 1999, that a giant database, containing personal details of millions of Australians, was to be constructed by the American data management company Acxiom in a joint venture with Publishing and Broadcasting Limited, there were a number of reactions. The Prime Minister, John Howard told a radio audience:

> *This kind of information is already held by a large number of organisations, and people who have business activities and have some kind of public profile, it's not all that difficult to assemble the information.[88]*

Another commentator[89] claimed that good databases and data-mining[90] techniques should reduce the "clutter" from a customer's life, and if "corporate Australia" used the technology "with propriety, our lives [would] improve". Acxiom's own position is that good data warehouses have become a "strategic imperative" for marketers, providing "highly predictive indicators of future behaviour" by customers.[91]

---

87. *See, for example, I Grayson, "Packer Sets Up Big Brother Data Store" The Australian (30 November 1999) at 33.*
88. *S Mitchell, "Packer Data Shop Sets Off Alarm" The Australian (7 December 1999) at 40.*
89. *M Hollands, "High Price for Abusing Trust" The Australian (7 December 1999) at 34.*
90. *The process of discovering patterns in data for the purpose of improving decision-making, usually in a business context.*
91. *"The enhancement of each customer record with postal, demographic, geodemographic, lifestyle, and psychographic data elements: Appending additional content to each customer record – such as income, age, marital status, home and auto ownership, hobbies and interests, and so forth – helps marketers in many ways.*

3.49 ***The aggregation of data.*** *The Acxiom joint venture also attracted criticism. Nigel Waters, a former Deputy Federal Privacy Commissioner, claimed that "it is precisely the aggregation of previously disparate information that is the main source of concern".*[92] *Some claimed the problem lay with the allegedly questionable ethics involved in the collection of the data,*[93] *while others cited the use of the information as the potential evil.*[94]

3.50 In the United States the acquisition by Doubleclick, the Internet's largest advertising company, of database marketer Abacus Direct, led to protests and an investigation by the Federal Trade Commission.[95] *According to Rosen, this reaction:*

> *shows, people don't want their browsing habits collected in personally identifiable dossiers, because those dossiers can be bought or subpoenaed by employers, insurance companies, divorcing spouses, and others who have the ability to affect our lives in profound ways.*[96]

Such data permits construction of customer profiles and models that predict customer or prospect behaviour": Acxiom, "Data Integration: the Warehouse Foundation" (Acxiom White Paper) «www.acxiom.com.au/whitepapers/wp-11.asp».

92. *N Waters, "Why Privacy Laws Must Have Muscle" Sydney Morning Herald (7 December 1999) at 19.*
93. *Eg C Connolly, "Database Collection is a Valid Question" (letter), The Australian (7 December 1999) at 14.*
94. *Eg M Hollands, "Law Change Urgent: Expert" The Australian (7 December 1999) at 40.*
95. *Consumer Reports Online, "Oh, What a Tangled Web" «www.consumerreports.org/Special/ConsumerInterest/Reports/0005pri1.htm». When a customer visits the web site of a DoubleClick customer, a "cookie" is placed on the visitor's hard drive, allowing DoubleClick to track what he or she is looking at, and build detailed profiles. DoubleClick was able to combine its own anonymous data with the names and purchase histories of 88 million households, held by Abacus Direct, thus helping it to determine the actual identity of the visitor. See also Business Week Online, "Privacy: Outrage on the Web" «www.businessweek.com:/2000/00_07/b3668065.htm?scriptFramed».*
96. *J Rosen, The Unwanted Gaze: The Destruction of Privacy in America (Random House, New York, 2000) at 198.*

3.51 An illustration of the difficulties presented by the aggregation of data was provided recently by the launch of the CrimeNet web site, an online database listing, amongst other things, the names and details of 4000 convicted criminals.[97] *All of the information available on the website was previously in the public domain. Critics argue that as long as this was scattered in court records, newspapers and other sources it was difficult or costly to access,*[98] *minimising any prejudicial effect on a jury which could threaten a fair trial. Within weeks of the site's launch, a murder trial in Victoria was aborted because the judge found it posed an unacceptable risk of having influenced the jury,*[99] *while others called for the site to be closed or expressed concern about the implications for the fair administration of justice.*[100] *One can predict great consternation should information on the website be incorrect.*

3.52 If an individual wished to control the amount of information about himself or herself available to others, he or she could take a number of precautions set out in an editorial in the Economist and described there as sounding "like the paranoid ravings of the Unabomber".[101] *The editorial writer adds, however, that, "[a]nyone*

---

97. *D Reardon, "It's a Steal: $6 Buys a Criminal History" Sydney Morning Herald (2 May 2000) at 8. The site, at «www.crimenet.com.au» was launched on 1 May 2000.*
98. *B Hickman, "Virtual Vigilantes" The Australian (6 May 2000) at 24.*
99. *G Wilkinson, "Net Site Aborts Trial" Herald-Sun (Melbourne) (25 May 2000) at 3.*
100. *Hickman at 24; Wilkinson at 3; R Ackland, "Jury's Out on Web We Weave" Sydney Morning Herald (26 May 2000) at 9.*
101. *"Remember, they are always watching you. Use cash when you can. Do not give your phone number, social-security number or address, unless you absolutely have to. Do not fill in questionnaires or respond to telemarketers. Demand that credit and data-marketing firms produce all information they have on you, correct errors and remove you from marketing lists. Check your medical records often. If you suspect a government agency has a file on you, demand to see it. Block caller ID on your phone, and keep your number unlisted. Never use electronic tollbooths on roads. Never leave your mobile phone on – your movements can be traced. Do not use store credit cards or discount cards. If you must use the Internet, encrypt your e-*

who took these precautions would merely be seeking a level of privacy available to all 20 years ago".

3.53 One of the more extreme consequences which may befall an individual failing to heed the Economist's checklist, is to become a victim of identity theft, or "identity fraud". This crime, which has increased sharply in the United States in recent years, involves the theft of another person's personal identifying information, by means as crude as stealing a wallet or as sophisticated as an organised crime scheme involving the use of computerised databases.[102] The consequences for the victim can be damaging, even apart from any financial loss. The General Accounting Office ("GAO"), the investigative arm of the United States Congress, reports:

> *[T]he "human" costs of identity fraud can be quite substantial. These costs include emotional costs, as well as various financial and/or opportunity costs. For example, the victims may be unable to obtain a job, purchase a car, or qualify for a mortgage.[103]*

3.54 Victims have reported feeling helpless and violated.[104] Apart from the actual harm they suffer, the onus is often on the victim to "clean up the mess",[105] undergoing a sometimes very lengthy and agonising process of clearing up their credit history.[106] The reality is, that for life to return to normal, it is the victim who must prove his or her innocence. The GAO notes "[i]n recent years, concerns have been raised about ... risks associated with computerised

---

mail, reject all 'cookies' and never give your real name when registering at websites. Better still, use somebody else's computer. At work, assume that calls, voice mail, e-mail and computer use are all monitored": "The End of Privacy: Surveillance Society" Economist (1 May 1999) 17 at 11.

102. United States, General Accounting Office ("GAO"), Identity Fraud (Report No GGD-98-100BR, 1998) at 1.

103. GAO at 4.

104. GAO at 49; Privacy Rights Clearinghouse, "Identity Theft: How it Happens, its Impact on Victims, and Legislative Solutions" «www.privacyrights.org/AR/id_theft.htm».

105. Privacy Rights Clearinghouse.

106. GAO at 11.

database services, an industry that is widely used by both public and private sector entities to locate or verify the identity of individuals."[107]

3.55 It is increasingly apparent that if an individual wishes to preserve a level of privacy enjoyed hitherto, he or she will have to work harder. Lacking consistent and comprehensive safeguards to protect their privacy, individuals will be left to take what limited measures are open to them to retain control over their personal information. As we have said elsewhere in this Report,[108] *consent is largely illusory when it comes to being subjected to surveillance. In today's reality, this would mean forgoing many things taken for granted, such as using a credit card or an automatic teller machine, and instead taking more proactive measures. For example, the Australian Direct Marketing Association ("ADMA"), lists procedures consumers must follow in order to "opt out" of receiving unsolicited mail or telephone calls from marketers, who have obtained personal information about the individual without his or her permission.*[109] *To use a metaphor from computer jargon, many features of modern life are configured to default to privacy loss – and that is when they are functioning properly.*

Growing concern

3.56 Information gathering activities are attracting attention because of growing public awareness of privacy issues, although this has been more marked overseas than here in Australia.[110]

---

107. GAO at 4. California is one State which has recently enacted provisions to assist identity theft victims: Penal Code s 530.5, 530.6.

108. Para 2.83-2.85.

109. Australian Direct Marketing Association, "Information and Events – FAQ's" «www.adma.com.au/consumer/FAQs.htm».

110. In September 1999 a Wall Street Journal/NBC News poll found that the loss of personal privacy is the primary concern of Americans approaching the twenty-first century. "When asked what concerns them the most about the next century, 29% of respondents answered the 'loss of personal privacy'. Overpopulation and terrorist acts on US soil followed at 23%, racial tensions at 17%, world war at 16%, and global warming at 14%": Electronic Privacy Information Centre, EPIC Alert (vol 6.15, 23 September 1999) «www.epic.org/alert/EPIC_Alert_6.15.html»; For other US examples,

Even so, the Australian public has demonstrated its interest. For example, the Internet industry within Australia has expressed concern that electronic commerce in Australia is failing to meet growth expectations. The industry cites the general public's worry about the lack of privacy and security associated with conducting such transactions as one of the main reasons for this.[111] The findings of an Australian Bureau of Statistics survey of Internet use by private households[112] tend to support the industry's view.

3.57 In addition to the kinds of personal information held on databases, surveillance can supply details of physical characteristics, habits, activities, whereabouts and associates. The convergence of technologies means that surveillance today is, or has the potential to be, an intrusive information gathering activity.

Social justice

3.58 Street cameras may be fixed so as to capture any person coming within their range of vision, but, in cases where they are

---

see para 3.50 above, and American Civil Liberties Union, "ACLU Calls on Law Enforcement to Support Privacy Laws for Public Video Surveillance" «www.aclu.org/news/1999/n040899b.html». For UK examples, see National Council for Civil Liberties (UK), "Have You Ever Had the Feeling That You're Being Watched?" «users.ox.ac.uk/~liberty/appcctv.html»; UK Public CCTV, Surveillance Regulation Campaign, "Watching Them, Watching Us" «www.spy.org.uk/lobby.htm».

111. *Andersen Legal, "Internet Privacy Survey 2000: a Survey of the Privacy Practices of Australia's Most Popular Web Sites" «www.iia.net.au/index2.html» at para 2.4.*

112. *Australian Bureau of Statistics, "8147.0 Use of the Internet by Householders, Australia (May 2000)" «www.abs.gov.au/ausstats/abs@.nsf/Lookup/NT0000B252». The survey found that, in the year to May 2000, 6% of all adults purchased goods or services for private use through the Internet, despite a finding that 33% of Australian households had Internet access. In the 3 months to May 2000, 8% of all adults used the Internet to pay bills or transfer funds, in contrast with 51% who used the telephone, 67% who used EFTPOS, and 74% who used automatic teller machines.*

being controlled by an operator, critics charge that there is room for abuse, even though in some cases this may be unintentional. One study, emanating from the University of Hull,[113] claims that the prejudices of the camera operator may dictate which persons are targeted. The study found a pattern of targeting black people, youth, and males. For example, cameras would, on average, monitor black people for longer periods than white people. Selection for surveillance was based primarily on the basis of "the operator's negative attitudes towards male youth in general and black male youth in particular."[114] The Associate Director of the American Civil Liberties Union, Barry Steinhardt, claims that "racial profiling and stereotyping is a reality of the American criminal justice system."[115] He quotes a survey which found that during a period of several months in 1995, 73% of cars stopped and searched by police on a highway in Maryland were driven by African-Americans, although they made up only 14% of those using the highway. He concludes that "video surveillance [will be used] to target those [thought] more likely to commit crimes." Biometric technology, in particular, has the potential to be used in a discriminatory way by targeting surveillance subjects, based on preconceived notions of which groups are likely to commit crimes. It must be stressed that the examples given above are drawn from overseas, and are not necessarily transferable to the local context. However, it is also important to be aware of the ease with which surveillance technology could be used in a discriminatory fashion.

3.59 Some critics fear that surveillance will be employed to "engineer" the type of people to frequent a vicinity, and that targeting troublesome and anti-social behaviour will lead

> *to the virtual disenfranchisement from city life of young people with low spending power and of other – generally low-income residents, whose appearances and conduct did not conform to*

---

113. C Norris and G Armstrong, The Maximum Surveillance Society: The Rise of CCTV (Berg, Oxford, 1999) at 150, 196.

114. Norris and Armstrong at 197.

115. American Civil Liberties Union, "ACLU Calls on Law Enforcement to Support Privacy Laws for Public Video Surveillance" «www.aclu.org/news/1999/n040899b.html».

> *the moral codes of well-ordered consumption enforced by shopping centre managers.*[116]

In his submission, Dr Brian Simpson, of Flinders University, comments:

> *To the extent that certain people are more likely to be in public places where CCTV surveillance operates, certain people are going to be watched more than others. Although CCTV surveillance is often presented as "democratic" in that all people are watched equally, the reality is that the opposite is true. CCTV surveillance is anti-democratic inasmuch as it tends to operate in areas where the targets of surveillance have little power. It divides society into the "watched" and the "non-watched".*[117]

3.60 One of the criticisms sometimes made about this kind of surveillance is that it is introduced to combat crime such as assault and theft, but more frequently results in action against more trivial anti-social behaviour. The Hull University report notes that a relatively small number of police deployments and very few arrests resulted from the monitoring of targets, this being in part due, according to the report, to the infrequency with which suspicion of a subject was based on objective fact which would warrant police intervention.[118] *The report concludes:*

> *The gaze of the cameras does not fall equally on all users of the street but on those who are stereotypically predefined as potentially deviant, or through appearance and demeanour are singled out by operators as unrespectable. In this way youth, particularly those already socially and economically marginal, may be subject to even greater levels of authoritative intervention and official stigmatisation, and rather than contributing to social justice through the reduction of victimisation, CCTV may become a tool of injustice through the amplification of differential and discriminatory policing.*[119]

---

116. F Bianchini, cited by Dr B Simpson, Submission at 4.
117. Dr B Simpson, Submission at 5.
118. Norris and Armstrong at 198.
119. Norris and Armstrong at 201.

The Commission is not aware of any study which replicates such results in a local context, or of any evidence to suggest that this has been the experience here.

Performance monitoring

3.61 Monitoring the individual performance of an employee is one of the most controversial uses of overt surveillance.[120] *While it can be of obvious benefit to employers through improving productivity and other such matters, there is a range of objections to performance monitoring, based on the detrimental effects of the practice on employees.*

3.62 Although many employers use surveillance as a means of monitoring performance and thereby enhancing productivity, there is a view that surveillance is in fact counterproductive and harmful to employees.[121] *Research indicates that there is a link between performance monitoring and psychological and physical health problems.*[122] *The problems experienced by employees who have had their performance technologically monitored include increased stress, boredom, high tension, headaches, extreme anxiety, depression, anger, severe fatigue and musculoskeletal problems.*[123] *These health problems can in turn lead to increased absenteeism and employee turnover,*[124] *leading to a decrease in productivity.*

120. *Privacy Committee (1995) at 31 (referring specifically to video surveillance).*
121. *International Labour Office (ILO), "Workers' Privacy Part II: Monitoring and Surveillance in the Workplace" (1993) 12(1) Conditions of Work Digest at 22.*
122. *Flanagan at 1263.*
123. *Flanagan at 1263; Privacy Committee (1995) at 52; ILO (1993) at 22.*
124. *M Levy, "The Electronic Monitoring of Workers: Privacy in the Age of the Electronic Sweatshop" (1995) 14(3) Legal Reference Services Quarterly 5 at 11.*

3.63 We note that clause 6.14 (3) of the ILO Code of Practice, Protection of workers' personal data,[125] states that "[c]ontinuous monitoring should be permitted only if required for health and safety or the protection of property". The Commentary to the Code of Practice identifies the reason for prohibiting continuous monitoring as being that "continuous monitoring has proved to be a cause of constant anxiety which can lead to both physical illness and psychological distress".[126]

3.64 Stress related problems are not the only health concerns connected to performance monitoring. As this form of surveillance can place a particular emphasis on speed and quantity as a means of assessing performance standards, it has the potential to encourage employees to increase their pace of work at the expense of employing sound ergonomic work practices. Accordingly, serious health and safety issues such as Occupational Overuse Syndrome are associated with performance monitoring.[127]

3.65 In addition to the link with health concerns, performance monitoring has been identified as having a more general negative effect on the workplace. The knowledge that employees are being watched, listened to or otherwise monitored can create a negative workplace atmosphere by undermining employee morale[128] and creating division between employees and management.[129] Furthermore, it is apparent that many monitored employees consider that the practice is damaging to their sense of dignity[130] and perceive that they are viewed with suspicion or as being untrustworthy.[131]

---

125. ILO, Geneva, 1997.
126. ILO (1997) at 36.
127. ILO (1993) at 99
128. Flanagan at 1264.
129. T Dixon, "Workplace video surveillance – controls sought" (1995) 2 Privacy Law and Policy Reporter 141 at 142.
130. Westin (1989) at 168.
131. Privacy Committee (1995) at 51.

Submissions

3.66 In the 1997 Issues Paper, IP 12, only covert performance monitoring was expressly raised as an issue for consideration. However, the Commission received several submissions that also addressed the additional issue of overt performance monitoring.

3.67 A number of submissions expressed the view that monitoring employee performance is an inappropriate use of overt surveillance. The Privacy Committee of New South Wales stated that it is opposed to the use of covert and overt visual surveillance for monitoring work performance.[132] The Australian Security Industry Association advised that its CCTV Code of Ethics provides that CCTV systems should not normally be used purely for staff monitoring and surveillance.[133] Similarly, the Retail Traders' Association of New South Wales advised that "Shopwatch", which is an advisory code of practice for the use of video surveillance equipment in retail stores, states that "[t]he use of the CCTV will not relate to the productivity of staff or other similar industrial matters".[134]

3.68 The Service Station Association does not accept that any form of surveillance should be used for an "improper" purpose such as evaluation of normal employee work performance.[135] As the New South Wales Council for Civil Liberties considers that overt visual surveillance should be permitted only in specific circumstances based on concerns for public safety[136] and that in such circumstances, surveillance equipment must not be trained on employees,[137] it is implicit that the Council opposes overt performance monitoring.

3.69 While the New South Wales Nurses' Association considered that there should generally be a prohibition on video monitoring of

132. Privacy Committee of NSW, Submission at 30.
133. Australian Security Industry Association Ltd, Submission at 2.
134. Retail Traders' Association of NSW, Submission at 16.
135. Service Station Association Ltd, Submission at 2.
136. NSW Council for Civil Liberties, Submission at 5.
137. NSW Council for Civil Liberties, Submission at 6.

work performance,[138] *it further submitted that performance monitoring might be acceptable with the consent of the employee.*[139] *The Association noted the difficulty in this regard of ensuring any such consent was valid, given the power imbalance in the employment relationship.*[140]

3.70 A similarly conditional view was expressed by a former Senior Public Defender, who submitted that in the case of overt performance monitoring, limits, such as the aspect of performance being monitored being linked to important areas of the business, should be imposed.[141] *An example of an acceptable instance of overt performance monitoring was given as the time taken to answer a telephone.*[142] *He suggested some form of permit system may be appropriate.*[143]

THE EFFICACY OF OVERT SURVEILLANCE

3.71 The following may sound familiar to an Australian audience:

> *There is an apparent shift in the public mood towards what a cynic might call personal security at all costs, security at any cost. One need only listen to the tirades in Parliament about the need to get tough on the perceived increase in crime. Privacy is being converted into the poor cousin in debates about public security. Privacy interests that are perceived as hindering effective law enforcement or endangering public security, whether they are in truth a hindrance or not, are too often swept aside.*[144]

It is from a paper delivered by the Canadian Privacy Commissioner to an audience in the province of New Brunswick. Occasional calls

---

138. NSW Nurses' Association, Submission at 1.
139. NSW Nurses' Association, Submission at 2.
140. NSW Nurses' Association, Submission at 2.
141. M L Sides, Submission at 20.
142. M L Sides, Submission at 20.
143. M L Sides, Submission at 20.
144. B Phillips, "Privacy in a "Surveillance Society" (1997) 46 University of New Brunswick Law Journal 127 at 135.

for the installation of CCTV suggest that some presume it to be the panacea against crime, and, therefore, worth the cost in both privacy and economic terms. It is, however, by no means clear that this presumption is accurate. It may be, for example, that when CCTV cameras are installed in an area, a so-called "displacement effect" results, with some criminal and anti-social behaviour shifting to locations beyond the range of vision. Furthermore, as Brown notes, the effectiveness of CCTV, like other crime prevention measures, may wear off with time unless it is widely seen to be achieving the desired result.[145]

3.72 In 1999, an independent evaluation of open-street CCTV in Glasgow concluded "open-street CCTV can work in limited ways, but is not a universal panacea. It works in different ways in different situations ... ."[146] *In the year following installation of the cameras, the area under surveillance recorded 3,156 fewer crimes and offences than was the average for the previous two years. However, after statistical refinement for underlying trends, the rate rose slightly to 109%, and was accompanied by a slight fall in detections (from 64% cleared up to 60%).*[147] *The same year another team*[148] *carried out an evaluation of the effect of CCTV on urban violence, by studying accident and emergency department and police assault data in three centres*[149] *in Wales. They concluded that "[c]ity centre CCTV installation had no obvious influence on levels of assaults" recorded in accident and emergency departments.*[150] *As*

145. *B Brown, CCTV in Town Centres: Three Case Studies (Home Office Police Department, Police Research Group Crime Detection and Prevention Series No 68, London, 1995) at 65.*
146. *J Ditton, E Short, S Phillips, C Norris and G Armstrong, The Effect of Closed Circuit Television on Recorded Crime Rates and Public Concern About Crime in Glasgow (Scottish Office Central Research Unit, Edinburgh, 1999) at 61. See also New South Wales Law Reform Commission, Surveillance (Issues Paper 12, 1997) at para 4.13-4.15.*
147. *Ditton at 5 and 29.*
148. *The Violence Research Group, University of Wales College of Medicine, Cardiff.*
149. *Cardiff, Swansea and Rhyl.*
150. *V Sivarajasingam and J P Shepherd, "Effect of closed circuit television on urban violence" (1999) 16 Journal of Accident and*

far as the Commission is aware, no independent and comprehensive study has been carried out in Australia to evaluate the effectiveness of overt surveillance systems.

3.73 The evidentiary value of surveillance material may also be exaggerated. Vicki Bruce, Professor of Psychology at the University of Stirling, states:

> *There are a number of problems with typical CCTV footage which make the task inherently difficult in some circumstances – CCTV images are very variable in quality, and camera and lighting angles may conspire to produce no more than a poorly lit, messy image of the top or back of a person's head. Recent research findings suggest, however, that the process of matching identities across different images may be remarkably error-prone even when image quality is reasonably high.*[151]

THE FUTURE OF OVERT SURVEILLANCE

3.74 Current indications are that the use of overt surveillance is unlikely to diminish in the short term. This is despite growing public awareness of privacy concerns, and the lack of strong evidence to support many of the benefits claimed on behalf of such systems. In addition to the reasons cited earlier for conducting overt

---

Emergency Medicine 255.

151. *Vicki Bruce "Fleeting Images of Shade: Identifying People Caught on Video" (1998) 11(7) The Psychologist 331 at 332. Bruce cites the following example: In 1988 police raided a woman's home, searching for her son, who was a robbery suspect. The woman was shot in the course of the raid. The son was later caught and prosecuted for the robbery entirely on the basis of evidence from a CCTV image showing a young black man. A prosecution witness claimed he could prove that the identities matched by comparing the precise number of pixels (the very small elements that make up a picture) separating key features of the face. The defence's expert witness, however, stated that if his students had made such elementary mistakes, they would fail. Examples were not correcting for the viewpoints when comparing two images, nor considering the resolution with which the face was depicted. The suspect was acquitted.*

surveillance, the reality is that government departments, local authorities and private concerns are under pressure to install such systems as one means of bolstering public confidence regarding personal security. Such pressure may take the form of public opinion, as aired by the media from time to time, often in the wake of particular incidents. Examples from New South Wales include the installation of security cameras to improve safety in trains in response to public perceptions about crime.[152] Principals at "schools suffering from violent incidents"[153] have reportedly called for cameras to be installed. Industry and professional associations, such as those representing taxi drivers[154] and police,[155] together with State magistrates,[156] have argued that their members be subject to video surveillance for their protection.

3.75 In the future, pressure to install overt surveillance systems may have another impetus, the desire to avert litigation. In the United States, a rapidly growing and developing area of tort law[157]

---

152. In May 1998, the Transport Minister, the Hon Carl Scully, announced that all railway stations in Sydney, Newcastle and Wollongong would be included in a $55 million security program to install CCTV and other measures, to be completed by mid-2000: D Humphries, "Cameras, Lights for Rail Stations" Sydney Morning Herald (25 May 1998) at 5.

153. A Patty, "Schools Want Spy Cameras" Sun-Herald (Sydney) (29 June 1997) at 11.

154. A Mitchell, "Look, You're on Candid Camera" Sun-Herald (Sydney) (10 May 1998) at 5.

155. "Police Car Camera Calls" Newcastle Herald (14 January 2000) at 16; L Hannan, "Call for Police Camera Action" Sun-Herald (Sydney) (13 July 1997) at 34.

156. R Morris et al, "Panic Button: Magistrates in Fear of Their Lives" Daily Telegraph (24 August 1999) at 9.

157. M J Rooney, "Liability of a Premises Owner for the Provision of Security: the Massachusetts Experience" (1995) 29 Suffolk University Law Review 51 at 51 and 83. According to the New York weekly, The Village Voice, security cameras "are now an integral part of new construction, along with sprinklers and smoke detectors": "The Surveillance Society (Part One: Spycam City)" The Village Voice «www.villagevoice.com/features/9840/boal.shtml».

involves plaintiffs suing property owners, alleging that the defendants' negligence in failing to provide sufficient security has resulted in their suffering personal injuries, often at the hands of a third party. Even though the criminal act of a third party is an intervening event, the defendant may still be liable if such an act was foreseeable and the defendant did not exercise reasonable care to reduce the risk of its occurrence.[158] *Examples of these so-called "premises liability" cases include ones in which plaintiffs have been attacked in apartment carparks where lighting and locks have been inadequate.*[159] *In a US case, Nebel v Avichal Enterprises Inc,*[160] *a motel patron alleged the defendant was negligent in failing to provide "functional and operational closed circuit surveillance cameras and monitors" in a motel in a New Jersey high crime area.*[161] *Morris v Krauszer's Food Stores Inc*[162] *was a case in which the plaintiff introduced expert testimony that, considering the foreseeability of robbery, the defendant should have increased*

158. *Security Industry Association and International Association of Chiefs of Police ("Security Industry Association"), "Informational Brief for Proposed Guidelines on CCTV Monitoring and Recording of Public Areas for Safety and Security Purposes" «www.siaonline.org/cctvinfobrief.html».*
159. *Pamela B v Hayden (1994) 31 Cal Rptr 2d 147. See also Allison v Rank City Wall Canada Ltd (1984) 6 DLR (4th) 144.*
160. *Nebel v Avichal Enterprises Inc (1989) 704 F Supp 570.*
161. *The court held that, for the plaintiff to prove negligence, it needed to show that security measures, such as a CCTV system, would have been likely to deter the criminal activity which caused the plaintiff's injury: Security Industry Association and International Association of Chiefs of Police, "Legal Issues Related to Silent Video Surveillance" «www.siaonline.org/cctvlegal1.html». Installing a video security system will not be sufficient to avoid liability. It seems necessary that proper policies and procedures be followed and any employees adequately trained (Cohen v Southland Corporation (1984) 203 Cal Rptr 572), and that the system be properly designed, maintained and monitored so as not to create a false sense of security which would encourage visitors, customers etc to take risks they might otherwise not take (Kutbi v Thunderlion Enterprises Inc (1985) 698 P.2d 1044): Security Industry Association (26 October 1999).*
162. *Morris v Krauszer's Food Stores Inc 693 A.2d 510 (NJ App 1997).*

security measures including the installation of video cameras. The jury found for the plaintiff.

3.76 The likely response of Australian courts to these type of claims is, at this stage, uncertain,[163] although one newspaper reported that Australian law firms are already acting for clients seeking compensation for injuries sustained in situations of allegedly inadequate security.[164] In June 2000, Judge Puckeridge of the District Court of New South Wales,[165] found a defendant employer in breach of a duty of care towards the plaintiff employee in failing to provide a safe place of work which would have entailed the adoption of certain security measures. The case did not, however, address the issue of electronic surveillance. We are not aware of any cases in any Australian jurisdiction alleging negligent failure to provide electronic surveillance, but this may come to be regarded as a standard security measure in the future.

3.77 The subject of surveillance has arisen in the context of accidents occasioning personal injury. In Shoeys Pty Ltd v Allan,[166] the plaintiff suffered significant injuries after slipping on some wet vegetable matter on a shop floor. The plaintiff argued that, in order to fulfil its duty of care towards her, one of the obligations of the defendant was to monitor the state of the floor so that it could see when leaves had fallen onto it.[167] Handley JA stated:[168]

---

163. I Newbrun, "'Dangerous' Premises", paper presented at the seminar Occupiers' Liability and Security Obligations (NSW) (LAAMS, Sydney, 21 February 1997) at 33.

164. D Serghis, "Public venues compo warning" Herald Sun (Melbourne) (7 July 1997) at 10. According to one newspaper report, the NSW Police Minister "said shopping centres had an obligation to their customers to provide secure parking": "Videos for Car Parks" Sunday Telegraph (20 April 1997) at 25.

165. Armour v G & E Natoli Real Estate Pty Ltd (NSW, District Court, No 51/99, Puckeridge J, 19 June 2000, unreported) at 11. See also Modbury Triangle Shopping Centre Pty Ltd v Anzil [1999] SASC 335 (carpark lighting at night).

166. Shoeys Pty Ltd v Allan (NSW, Court of Appeal, No 40365/90, 3 May 1991, unreported).

167. Shoeys Pty Ltd v Allan at 5 (Mahoney JA).

> *In my opinion an occupier cannot reasonably be expected to prevent material being dropped in areas being used by the public. Nor can an occupier be expected to remove material the instant it is dropped. What can be expected is that a system will exist for routine inspection and cleaning of busy high risk areas during the times they are in use by the public. (emphasis added)*

3.78 In the context of a relatively small-scale retail operation, electronic surveillance was not an issue.[169] *However, in the earlier case of Brady v Girvan Bros Pty Ltd,*[170] *in which a customer in a large and busy shopping mall was injured after slipping on some jelly, McHugh JA (as he then was) said:*

> *A real risk of injury should be eliminated unless the cost of doing so is disproportionate to the risk. When the inferred size of the common ways, the number of people attending the Mall, and the risks of injury are borne in mind, the employment of a full-time cleaner cannot be regarded as an unreasonable burden on the occupier of a shopping mall as large as Minto Mall. Indeed the installation of video cameras monitoring the common ways is not outside what could be reasonably expected of the occupier. The use of these cameras for surveillance purposes is commonplace in the shops, stores and venues of Sydney. If video cameras can be used to protect the property of occupiers, they can be used to protect the safety of customers. The cost of employing a full-time cleaner or the installing of an electronic surveillance system was not out of proportion to the risk of injury involved at Minto Mall.*[171]

3.79 So-called "spillage" cases, occurring in premises under the defendant occupier's control and where a large volume of people

---

168. *Shoeys Pty Ltd v Allan at 3 (Handley JA).*
169. *"In the present case, it was not, I think, argued that the defendant's duty was to have somebody constantly observing each part of the floor, by means of electronic surveillance or otherwise. No suggestion of this kind was put to the witnesses nor was the cost or practicality of it considered at the trial": Shoeys Pty Ltd v Allan at 7 (Mahoney JA).*
170. *Brady v Girvan Bros Pty Ltd trading as Minto Mall (1986) 7 NSWLR 241.*
171. *Brady v Girvan Bros Pty Ltd at 255.*

pass, have established an occupier's duty to put in place a reasonable inspection and cleaning system.[172] *Thus far, the use of electronic surveillance has received little mention in this regard. However, as the prevalence of its use increases, and the cost of installation decreases, it is possible that at some future time, courts will take the presence of a surveillance system into account when considering measures taken by an occupier to prevent injury to invitees in "spillage", and analogous, cases. Such reasons coupled with those already advanced by surveillance users, means that calls by civil libertarians to reduce the incidence of overt surveillance usage because of privacy concerns, are likely to be met with strong resistance from many quarters.*

VIEWS CONTAINED IN SUBMISSIONS

3.80 Submissions were received from media and other organisations which use surveillance devices, law enforcement agencies, associations representing lawyers, and other concerned parties. Many of the surveillance users stated that they adhered to a code of practice, often industry-based.[173]

---

172. Australian Torts Reporter (CCH, Sydney, 1984) Volume 1 at [10-340].

173. Australian Broadcasting Corporation, Submission at 1 ("Code of Practice"); Australian Press Council, Submission at Annexure B ("Statement of Principles"); Australian Security Industry Association Limited, Submission at 1 ("CCTV Code of Ethics"); Insurance Council of Australia Limited, Submission at 1 ("General Insurance Code of Practice"); Motor Traders' Association of NSW, Submission (copy of submission to Privacy Committee of New South Wales) at 2; Publishing and Broadcasting Limited, Submission at 2 (FACTS (Federation of Australian Commercial Television Stations) "Commercial Television Industry Code of Practice"); Registered Clubs Association of NSW, Submission at 3 (cites the Code of Practice for the Use of Overt Video Surveillance in the Workplace released by the New South Wales Department of Industrial Relations following the deliberations of the Working Party on Video Surveillance which was established in 1996); Retail Traders' Association of NSW, Submission at 11 ("Shopwatch: An Advisory Code of Practice for the Use of Video Surveillance Equipment in

3.81 In the Issues Paper we asked[174] if the use of overt visual surveillance should be regulated. Unambiguous support for the concept of enforceable regulation of overt surveillance came from the New South Wales Council for Civil Liberties,[175] Privacy Committee of New South Wales,[176] Price Waterhouse,[177] the then Senior Public Defender,[178] and Lismore City Council.[179] Support for the contrasting view, that overt surveillance should, at most, be managed by self-regulation (for example, through industry-based codes of practice) was expressed by the Australian Press Council,[180] Australian Security Industry Association Limited,[181] Insurance Council of Australia Limited,[182] New South Wales Department of Training and Education Co-ordination,[183] Publishing and Broadcasting Limited,[184] the Registered Clubs Association of New South Wales,[185] and the Retail Traders' Association of New South Wales.[186] Some others, while favourably disposed towards the concept of regulation, were not clear as to whether this should take the form of legislation or industry code of practice. The submission from the New South Wales Police Service, for example, states the view that there would be "some benefit in the development of a mechanism by which to ensure ... local CCTV initiatives were implemented and managed in a standard manner across the State (emphasis added)."[187] Submissions from Fairfield City Council[188]

Retail Stores"); Service Station Association Ltd, Submission at 1 ("SSA Policy: Surveillance, Audio/Video").

174. New South Wales Law Reform Commission, Surveillance (Issues Paper 12, 1997) at para 4.21.

175. Submission at 3.

176. Submission at 21.

177. Submission at 3.

178. M L Sides, Submission at 5.

179. Submission at 1.

180. Submission at 2.

181. Submission at 1.

182. Submission at 2.

183. Submission at 1.

184. Submission at 4.

185. Submission at 2-4.

186. Submission at 10.

187. Submission at 7. NSW Young Lawyers Criminal Law Committee, Submission at 1; Director of Public Prosecutions, Submission at 2;

and the Department of Corrective Services,[189] while not necessarily expressing opposition to the concept of regulation, were keen to stress that they should be allowed some degree of exemption, because of existing accountability to its local community in the former case, or because of the special needs of the latter.

REGULATION

How overt surveillance is regulated

3.82 As stated at paragraph 1.50 and following, there is very little to fetter the unrestricted use of overt surveillance, other than codes which are adhered to voluntarily and lack sanctions for breach, or a patchwork of common law remedies which are inapplicable in the vast majority of cases. The practical result is that there is no common set of rules for the operation of overt surveillance in New South Wales. In the event that the surveillance has been abused to the detriment of an individual, in most cases that individual will have no redress.

Self-regulation

3.83 A report produced in 1997 by the Commonwealth Interdepartmental Committee on Quasi-regulation stated that:

> *[r]egulation can usefully be considered as a spectrum ranging from self-regulation where there is no government involvement, through various regulatory arrangements with increasing degrees of government influence and involvement,*

NSW Nurses' Association, Submission at 1. The joint submission from the NSW Crime Commission (NSWCC), Independent Commission Against Corruption (ICAC), Police Integrity Commission (PIC) and National Crime Authority (NCA) ("Joint Law Enforcement Agencies") supports the regulation of overt visual surveillance by industry codes of practice or privacy legislation, rather than by the LDA: Submission at 2.

188. *Submission at 1-3.*
189. *Submission at 2-3.*

> *to explicit government regulation (often referred to as "black-letter law").*[190]

In this Report we adopt that Committee's working definition of self-regulation, as being "any regulatory regime which has generally been developed and funded by industry, and is enforced exclusively by industry.[191] *The Commission believes that this is the meaning generally intended by those submissions calling for self-regulation, or regulation by means of voluntary codes of conduct, by users of overt surveillance.*[192] *Falling between the extremes of self-regulation and mandatory government legislation is a broad area which the Interdepartmental Committee calls "quasi-regulation" or "grey-letter law", because of the influence of government on business compliance which falls short of explicit regulation.*[193]

Advantages of self-regulation

3.84 It is self-evident that most industries would, if given the option, prefer to govern themselves than have rules and sanctions imposed by government.[194] *Self-regulation lessens or avoids altogether the need to fulfil bureaucratic requirements, and the consequences of failures in compliance are likely to be relatively light. While this preference is motivated in part by self-interest, there are nevertheless sound reasons why self-regulation can be*

---

190. *Australia, Commonwealth Interdepartmental Committee on Quasi-Regulation, Grey-Letter Law (Canberra, 1997) at ix.*
191. *Commonwealth Interdepartmental Committee on Quasi-Regulation at 6.*
192. *The Committee notes, however, that "self-regulation" has also been used to describe industry schemes which have had some degree of government involvement: Commonwealth Interdepartmental Committee on Quasi-Regulation at 6.*
193. *Commonwealth Interdepartmental Committee on Quasi-Regulation at 7.*
194. *Australia, Taskforce on Industry Self-Regulation, Draft Report (Department of Treasury, Canberra, 2000) at 22. For an example, see Master Builders Association of South Australia, "The Master Builders Association National Code of Practice and the Constitution" «www.mbasa.com.au/ mbasa/c_o_p.htm».*

beneficial to the wider community.

3.85 It may be more efficient for an industry, with its existing expertise, to set the benchmarks, rather than government. The cost to an industry in formulating and operating its own code of conduct is likely to be less than if it were forced to comply with standards mandated from outside. This can benefit taxpayers, as it shifts costs from government to the industry.[195] The "in-house" nature of self-regulatory controls should also make it easier for rules to be modified, and therefore be more responsive, as circumstances change.[196]

Shortcomings of self-regulation

How valuable is the thing being protected?

3.86 Self-regulation may be a feasible alternative to other forms of regulation where it can provide the public with an appropriate and sufficient level of protection for the commodity, value or other objective sought to be safeguarded. This issue was addressed recently by the Australian Broadcasting Authority (ABA), during its inquiry into the commercial radio controversy which came to be known as "cash for comment".[197] In its report, the ABA commented:

> *The right to exclusive use of a section of the radiofrequency spectrum for the purpose of commercial broadcasting is an extremely valuable public asset, and the community has certain expectations of those who are entrusted with the use of such assets ... (T)hose promulgating and seeking to rely on self regulatory codes (as a defence against formal government intervention) are bound to ensure that the codes are living, working and workable guides to behaviour and conduct in the industry. ... (T)he entrusting of significant self-regulatory responsibility to industry indicates that a very high standard*

195. *A J Campbell, "Self-Regulation and the Media" (1999) 51(3) Federal Communications Law Journal 711 at 716.*
196. *Campbell at 716.*
197. *The inquiry was prompted by stories televised by the Australian Broadcasting Corporation's "Media Watch" program during 1999, concerning alleged financial dealings between presenters on various commercial radio stations and outside commercial interests.*

> *of compliance is expected of industry in the fulfilment of its self-regulatory responsibilities.*[198]

3.87 Similarly, it is an important issue as to whether self-regulation of the use of surveillance devices can provide adequate community safeguards for something as valued by individuals as their privacy, and as valuable in the marketplace as personal information. In its Report on surveillance, the Irish Law Reform Commission stated:

> *The fact that a law exists protecting a particular right does much to symbolise the importance to society of that right. It also serves an educative function for society at large. From this perspective, the fact that infringements might be rare is beside the point. What matters is that the right is considered important enough to deserve both the symbolic imprimatur of the law and the provision of practicable means of redress.*[199]

Conflict of interest

3.88 The rights of surveillance users and surveillance subjects will conflict in some ways. While self-regulatory schemes do not preclude protection of the interests of surveillance subjects, they are formulated and operated by surveillance users, whose own interests will, doubtless, be reflected. In the case of conflict arising between the interests on either side, impartiality cannot be assumed when one party makes the rules. A similar point was made by the Senate Select Committee on Information Technologies, in its report on Australian media, entitled "In the Public Interest".[200] *The code of practice of the Federation of Australian Commercial Television Stations ("FACTS")*[201] *states that in broadcasting news and current*

---

198. *Australian Broadcasting Authority ("ABA"), Report of the Commercial Radio Inquiry (Sydney, 2000) at 74.*
199. *Ireland, Law Reform Commission, Report on Privacy: Surveillance and the Interception of Communications (Report 57, 1998) at para 4.19.*
200. *Australia, Senate Select Committee on Information Technologies, In the Public Interest: Monitoring Australia's Media (Senate Printing Unit, Canberra, 2000).*
201. *Television stations operate within a co-regulatory environment, where codes of practice are developed and managed under the supervision of a statutory body operating within a legislative framework. The*

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.*[202]

The Senate Committee's Report stated:

> *[T]he decision as to what will or will not constitute "an identifiable public interest", should not be left to purely sectarian interests. The Committee is of the view that the important balance to be struck between the "private" and "public" interest ought to be weighed up within the framework of a fair, independent and objective statutory regime.*[203]

Lack of consistency and universality

3.89 Where there is significant diversity in an industry or sector, it is unlikely that a voluntary regulatory regime can be adopted universally or consistently. Privacy protection loses force unless all involved in activities which may compromise privacy agree to such participation. This is because it is more and more difficult to fence off personal information.[204] *Information is a commodity which can be bought and sold. Convergence also renders technological barriers increasingly irrelevant.*

Enforceability and accountability

3.90 Some businesses may claim to comply with an industry-wide code of practice. It may be difficult for a member of the public to ascertain the degree of such compliance, and indeed whether the business is even a signatory to the code. If non-compliance is

---

Federation of Australian Commercial Television Stations has developed a code of practice, which has been approved and registered by the Australian Broadcasting Authority: Senate Select Committee on Information Technologies at para 1.22, 3.1 and 3.10.

202. *Federation of Australian Commercial Television Stations, Commercial Television Industry Code of Practice (April 1999) at s 4.3.5.*
203. *Senate Select Committee on Information Technologies at 1.55.*
204. *M E Budnitz "Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Reg is Inadequate" (1998) 49 South Carolina Law Review 847 at 874.*

demonstrated, it must be questioned how sanctions, if any, will be enforced against members, let alone against non-members riding along on their coat-tails. It is difficult to understand why an industry member would choose to bind itself by a set of rules. If a voluntary code is intended to act as reassurance to the public that its rights are being protected, it seems this goal would be better achieved through the enactment of laws providing sanctions and remedies. Commissioner Varney of the United States Federal Trade Commission put it this way:

> *Given the great diversity of companies, a significant number of companies are unlikely to agree on a uniform set of guidelines. Even among those who agree to the guidelines, some may not in fact comply with them. Over time, some who at first complied may cease to do so while not publicly acknowledging that they are no longer in compliance. Without an independent party to monitor and enforce compliance, consumers have no way to judge whether or not a company is actually in compliance with such guidelines. If a statute were to make the guidelines mandatory and provide meaningful remedies, consumers at least would be assured that companies have an incentive to comply.*[205]

Recent examples in other privacy-sensitive areas

Australia

3.91 Prior to 1992, the broadcasting industry was subject to a cumbersome regulatory regime.[206] *In the report of the so-called "cash for comment" inquiry, referred to above at para 3.86, the ABA found there appeared to have been "a systematic failure to ensure the effective operation of self-regulation", as well as a failure by the relevant codes "to provide appropriate community safeguards".*[207]

---

205. Budnitz at 875-76.

206. Australian Broadcasting Authority ("ABA"), Report of the Commercial Radio Inquiry (Sydney, 2000) at 74.

207. ABA at 4. The ABA formed the view "that remedial action is necessary to ensure the commercial radio industry's compliance with the Act and the Codes", and suggested that it should determine three

3.92 A similar conclusion was reached in a report by the Senate Select Committee on Information Technologies evaluating "the appropriateness, effectiveness and privacy implications of the existing self-regulatory framework in relation to the information and communications industries".[208] The Committee found:

> *substantial evidence to question the efficiency and effectiveness of self-regulation and co-regulation in Australia's information and communications industries. Self-regulation in the print media industry appears to be failing the community. In the television and radio industries, co-regulation has attracted widespread criticism. Standards for advertisements are not being adequately enforced.[209]*

---

standards applicable to commercial radio broadcasting licensees (at 4). It warned, however, "that [the ABA's] existing powers lack the flexibility and force to properly respond to serious Code breaches and that it lacks sanctions that have immediate effect" (at 5). It proposed various options to remedy this situation, but noted (at 6) that these would require legislative change.

208. Senate Select Committee on Information Technologies at iii.

209. Senate Select Committee on Information Technologies at para 6.1.

3.93 The Committee formed the view "that robust, investigative journalism and the existence of a statutory framework for regulating the print media are not mutually exclusive",[210] and recommended the establishment of an independent statutory body to deal with complaints and assist in enforcing standards.[211]

3.94 The Privacy Committee of New South Wales was established in 1975.[212] In 1980 it released a paper in which it outlined[213] the Committee's philosophy with regard to privacy protection. This stated that privacy is best protected by:

> *(a) Flexible guidelines, monitored by an informed and concerned public, aided by a vigilant permanent watchdog,*
>
> *(b) specific legislation aimed at particular problems which fail to respond to guidelines.*

This view was said to be based on the Committee's experience of five years, handling 10,000 complaints, completing 53 research reports, and issuing guidelines in a number of areas. By the time the Committee published its 1982 annual report, it had had a change of heart:

> *During 1982, the Committee reassessed its policy which favoured voluntary guidelines as the principal means of protecting privacy, with remedial legislation where such guidelines failed. The Committee believes such a reassessment would be of value in the light of its 7 years of experience, in handling over 15,000 complaints and producing 53 research reports. The Committee believes that the range and extent of privacy invasions in the area of information privacy, where most complaints arise, makes it no longer feasible to leave the bulk of privacy protection to voluntary guidelines. The potential for serious invasion of privacy is large and increasing rapidly. Legislation is now necessary, not merely as*

---

210. Senate Select Committee on Information Technologies at para 2.72.
211. Senate Select Committee on Information Technologies at Chapter 6.
212. It is now known as Privacy NSW, and is the Office of the New South Wales Privacy Commissioner.
213. New South Wales, Privacy Committee, Privacy Protection: Guidelines or Legislation? (Government Printer, Sydney, 1980) at 1.

> *a remedial response to existing violations of privacy rights, but as a general preventative means of protecting privacy rights and laying down privacy protection standards.*[214]

Great Britain

3.95 In England a decade earlier, the Committee on Privacy and Related Matters had delivered its report (chaired by David Calcutt QC) on the measures needed "to give further protection to individual privacy from the activities of the press".[215] *The Committee concluded that the impact of the Press Council on intrusions by the press into privacy had been limited,*[216] *and recommended "that the press should be given one final chance to prove that voluntary self-regulation can be made to work."*[217] *Even so, it recommended replacing the Press Council with a new body, the Press Complaints Commission which "must be seen to be authoritative, independent and impartial".*[218] *Although the Committee reaffirmed the importance of self-regulation,*[219] *it threatened that if the press was "not prepared to put and keep its own house in order, further legislation must follow."*[220] *A second report*[221] *chaired by Calcutt in 1993, gave the following assessment of the Press Complaints Commission:*

> *The Commission, as constituted, is, in essence, a body set up by the industry, financed by the industry, dominated by the industry, operating a code of practice devised by the industry and which is over-favourable to the industry.*[222]

Although the report did recommend the introduction of a statutory regime, this was not adopted by the Government.

---

214. New South Wales, Privacy Committee, Annual Report 1982-1983 at 15.
215 England and Wales, Home Office, Report of the Committee on Privacy and Related Matters (HMSO, London, Cm 1102, 1990) ("Calcutt Report") at para 1.1.
216. England and Wales, Home Office at para 14.37.
217. England and Wales, Home Office at para 14.38.
218. England and Wales, Home Office at para 14.38.
219. England and Wales, Home Office at para 17.14.
220. England and Wales, Home Office at para 17.16.
221. Review of Press Self-Regulation (Dept of National Heritage, Cm 2135, London, HMSO).
222. Review of Press Self-Regulation at para 5.26.

United States

3.96 The American experience does not appear to have been happier, despite a preference for relying on self-regulation. Angela J Campbell concludes that, after analysing past uses of self-regulation in broadcasting, children's advertising, news, alcohol advertising, comic books, movies, and video games, "self-regulation rarely lives up to its claims, although in some cases, it has been useful as a supplement to government regulation."[223] According to another report, self-regulation has "failed abysmally".[224]

3.97 The Federal Trade Commission ("FTC") has monitored online privacy for the past few years. In June 1998 it reported:

> *Effective self-regulation remains desirable because it allows firms to respond quickly to technological changes and employ new technologies to protect consumer privacy. Accordingly, a private-sector response to consumer concerns that incorporates widely-accepted fair information practices and provides for effective enforcement mechanisms could afford consumers adequate privacy protection. To date, however, the Commission has not seen an effective self-regulatory system emerge. As evidenced by the Commission's survey results, and despite the Commission's three-year privacy initiative supporting a self-regulatory response to consumers' privacy concerns, the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness).[225] (emphasis added)*

3.98 Then, in May 2000, the FTC released its third report on the state of online privacy and the efficacy of self-regulation.[226]

---

223. A J Campbell, "Self-Regulation and the Media" (1999) 51(3) Federal Communications Law Journal 711 at 772.

224. "The End of Privacy: the Surveillance Society" Economist (1 May 1999) 17 at 19. "A Federal Trade Commission survey of 1,400 American Internet sites last year [1998] found that only 2% had posted a privacy policy in line with that advocated by the commission ... Studies of members of America's Direct Marketing Association by independent researchers have found that more than half did not abide even by the association's modest guidelines."

225. Federal Trade Commission, "Privacy Online: A Report to Congress" (VI Conclusions) «www.ftc.gov/reports/privacy3/conclu.htm».

226. Federal Trade Commission, "Privacy Online: A Report to Congress"

The Chairman, Robert Pitofsky, addressing a Senate committee, commended industry leaders in developing self-regulatory initiatives, but added that industry efforts had been insufficient. He stated:

> *Because self-regulatory initiatives to date fall far short of broad-based implementation of effective self-regulatory programs, a majority of the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders. While there will continue to be a major role for industry self-reg in the future, a majority of the Commission recommends that Congress enact legislation that, in conjunction with continuing self-regulatory programs, will ensure adequate protection of consumer privacy online.*[227]

3.99 Interestingly, an Australian version was conducted of the 2000 Online Privacy Survey which accompanied the FTC's report, and released in October 2000.[228] *It analysed the stated privacy practices of the 100 most requested web sites in Australia, and found that "a significant amount of work [is] to be done to achieve the level of protection which consumers are beginning to demand."*[229]

(VI Conclusions) «www.ftc.gov/reports/privacy3/conclu.htm».

227. *Federal Trade Commission, "Prepared Statement of the Federal Trade Commission on "Privacy Online: Fair Information Practices in the Electronic Marketplace" «www.ftc.gov/os/2000/05/testimonyprivacy.htm».*
228. *Andersen Legal, "Internet Privacy Survey 2000: a Survey of the Privacy Practices of Australia's Most Popular Web Sites" «www.iia.net.au/index2.html».*
229. *Andersen Legal, "Internet Privacy Survey 2000: a Survey of the Privacy Practices of Australia's Most Popular Web Sites" «www.iia.net.au/index2.html».*

4. Overt surveillance: recommendations

- Finding a balance
- A scheme of regulation
- Elements of proposed legislation
- Principle 1: Overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy
- Principle 2: Overt surveillance must only be undertaken for an acceptable purpose
- Principle 3: Overt surveillance must be conducted in a manner which is appropriate for purpose
- Principle 4: Notice provisions shall identify the surveillance user
- Principle 5: Surveillance users are accountable for their surveillance devices and the consequences of their use
- Principle 6: Surveillance users must ensure all aspects of their surveillance system are secure
- Principle 7: Material obtained through surveillance to be used in a fair manner and only for the purpose obtained
- Principle 8: Material obtained through surveillance to be destroyed within specified period
- The Privacy Commissioner's role
- The employment context

FINDING A BALANCE

Protecting the rights of all parties

4.1 The Commission has, throughout this reference, maintained the view that the practice of overt surveillance involves intertwining legitimate, albeit conflicting, interests. Consequently, any recommendations should reflect this and attempt to find a workable solution. These rights belong, on the one hand, to current or would-be users of overt surveillance devices, seeking justifiable protection of their interests. On the other hand, the general public assumes entitlement to some degree of privacy, irrespective of whether this finds explicit recognition in existing law.[1]

4.2 Although concerned with potential privacy intrusions, the Commission's recommendations are not primarily aimed at reducing the incidence of surveillance use, but rather attempt to steer the best course between the various interests involved. In any event, it appears futile in the short term to attempt proscribing surveillance use to any significant extent.[2] *The appropriate result is one which allows surveillance users to pursue their legitimate interests, while leaving surveillance subjects confident that theirs are protected.*

4.3 One possible course is to leave surveillance users to continue pursuing their interests, assuming little or no adverse impact upon the rights of surveillance subjects. After all, overt surveillance is, by definition, something known to be taking place. It is familiar and widespread, and is largely intended to act as a deterrent to socially harmful behaviour, thus offering a benefit to the public. It seems hardly to have been touched by regulation anywhere in the world. A sizeable industry has grown around its use both here and overseas, and it features prominently in security systems, from the smallest to the largest. Does it, therefore, require regulation? In the Commission's view, the answer is yes, and for a number of reasons.

---

1. *See para 1.4-1.13.*
2. *See para 3.74-3.79.*

Protecting the privacy we have

4.4 Although individuals have a reasonable expectation that their lives will be free from undue monitoring and that they retain significant control over their personal information, it is suggested in some quarters that these desires are misguided or just too difficult to achieve.[3] *There are many and diverse benefits of information and surveillance technology, as outlined in Chapter 3. At the same time, the increasing sophistication of technology capable of being used for surveillance purposes, together with the convergence of this and other types of information technology, raise issues of serious concern. The time is opportune to act, for, as one commentator puts it, there is "a great deal of our privacy left to lose [and] considerable privacy to regain".*[4]

4.5 The full impact on privacy of technologies used in current surveillance and data collection practices will not be apparent until some future time. If, however, no action is taken now to try and preserve privacy, then we may indeed be needlessly surrendering that which we still have, without fully understanding the consequences. Furthermore, a complacent attitude with regard to implementing strong privacy safeguards may have unforeseen consequences for potential victims. A laissez-faire attitude to users of such information technology as data collection and surveillance may bring about a situation in which the onus is placed on individuals who have done nothing wrong, to prove their innocence or correct false impressions when surveillance is misused. To avoid electronic surveillance, an individual would have little alternative but to "opt out" of modern society altogether.

Existing protections inadequate

4.6 In the Commission's view, leaving the area of overt surveillance unregulated ignores the socio-legal context of surveillance use, which has seen electronic surveillance flourish in a society whose laws (such as trespass) are underdeveloped to meet the technological challenge to privacy. The Commission disagrees

---

3. For example, Bruce Phillips, Canadian Privacy Commissioner, asks rhetorically "Is the age now upon us to be the Age of Surrender?": Canada, Privacy Commissioner, Annual Report 1998-1999 at 1.

4. Canada, Privacy Commissioner, Annual Report 1998-1999 at 2.

with the suggestion[5] that existing laws and codes of practice provide sufficient privacy safeguards against technologies which can access huge quantities of personal information, and which render traditional concepts on which many such laws are based (for example, property rights), irrelevant.

4.7 In the previous chapter the use of overt surveillance was likened to that of a fine mesh fishing net. The indiscriminate haul of information that can be obtained through using overt surveillance devices means that, even if the surveillance were undertaken for a legitimate purpose, not all of the information gleaned necessarily relates to that purpose. What should happen to that information is a serious concern.

Accountability

4.8 The Commission further sees a need for statutory regulation of this area in order to provide certainty, consistency and, above all, accountability, elements missing from self-regulatory schemes. Accountability is crucial to providing the necessary incentive to surveillance users to abide by codes of practice. This has benefits for both users and subjects of surveillance. The latter will have the reassurance of rights backed by the force of law. Concomitantly, these rights will be enforceable by means of prescribed sanctions. The former will have set down clear principles of behaviour, to assist them in upholding community expectations regarding privacy. The enactment of statutory provisions mean that no individual participant within an industry or sector can afford to ignore privacy concerns while benefiting from community assumptions that privacy codes of practice apply universally. In other words, those individual surveillance users who do not uphold the mandated standards cannot enjoy a free ride on the coat-tails of those who do, without risking penalty. Furthermore, the Commission believes that those surveillance users who are already voluntarily abiding by codes of practice will not be adversely affected by this recommendation, details of which are set out below.

---

5. For example, in Publishing and Broadcasting Limited, Submission at 2.

Weighing up the interests

4.9 How can the objective of "balancing" the legitimate rights of both the users and the subjects of surveillance be given effect? "Balance" is, in fact, not the apposite term, if this implies a series of parallel rights, or a sort of "give and take". After all, how real is privacy protection, if compromises of the type exemplified by the quotations appearing at para 3.47 are permitted? If, for every claimed countervailing right or benefit, privacy protections are traded off bit by bit, then the partial right to privacy which remains is, arguably, no right to privacy in any meaningful sense. Privacy breaches are, in effect, sanctioned if the price is right. The Commission agrees with the approach, but not the conclusion, of the Chamber of Manufactures of New South Wales, when it states:

> *Employers have never submitted that their interests must be balanced against employees' rights to privacy. Employers have uniformly and consistently emphasised their fundamental right to protect their property, but that within the context of that right there should be protection of employees' privacy.*[6]

4.10 The Commission's view is, to the contrary, that privacy must be secured first, and the entitlement of surveillance users to employ surveillance to protect their interests retained, though made subject to the need to protect privacy interests. The Commission sees no compelling reason to accord greater protection to the property rights of surveillance users than to the privacy of the general public, nor to define or limit the latter by reference to the former. The consequence of doing otherwise would, in effect, allow the degree of privacy from surveillance enjoyed by the public to be decided by, and bestowed at the behest of, a countless number of surveillance users.

4.11 It is, furthermore, important to question the assumptions on which rest arguments favouring the compromising of privacy. Those in favour of, for example, the use of street cameras, accept their efficacy in reducing crime. However, there is no conclusive evidence that street cameras do reduce crime.[7] *The opportunity to introduce*

---

6. Chamber of Manufactures of NSW (Industrial), Submission at 6.

7. para 3.71-3.73.

privacy protections should not be foregone in the face of what may prove to be illusory benefits.

4.12 This is far from saying that surveillance or other potentially intrusive practices ought to be outlawed. There is, however, in the Commission's view, a strong argument for regulating privacy-threatening activities, by making surveillance users accountable for their practices and by giving a right of redress to an individual whose legitimate expectation of personal privacy is violated. Even in areas where most people accept they will have to reveal personal details, there is generally statutory protection of the confidentiality of those details, and outrage if this confidentiality is breached.[8]

A legislative response

4.13 New developments in surveillance technology reveal

8. This was brought to the fore in 2000 by the revelation of plans by the Australian Taxation Office (ATO) to sell personal information supplied by individuals applying for an Australian Business Number (ABN). The ATO had advised applicants for an ABN that the information they supplied would be treated with confidentiality. Instead, the ATO was forced to admit it had been in breach of the Privacy Act 1988 (Cth). The Federal Government announced that, "in response to concerns raised over public access to the register", restrictions would apply to the information publicly available from the Australian Business Register". It was also announced that the A New Tax System (Australian Business Number) Act 1999 (Cth) would be amended to improve privacy protection associated with the ABN: M Kingston, "They Won't Even Let Me Complain" Sydney Morning Herald (3 June 2000) at 4; "Tax Office Admits Privacy Sin" Sydney Morning Herald (6 June 2000) at 3; Australian Privacy Commissioner, "Federal Privacy Commissioner and Taxation Office Continue Discussions Over ABN" (Media release of 5 June 2000) «www.privacy.gov.au/news/00_07.html»; Australia, Treasurer, "Privacy Restrictions on Australian Business Register" (Assistant Treasurer Press Release 29, 20 June 2000) «www.treasurer.gov.au/assistanttreasurer/pressreleases/2000/029.asp»; Australian Privacy Commissioner, "Federal Privacy Commissioner Welcomes Today's Announcement on ABN Privacy Solutions" (Media release of 20 June 2000) «www.privacy.gov.au/ news/00_11.html».

applications whose forms and capabilities are constantly changing. Attempting to regulate each new example of surveillance technology would prove an inefficient and fruitless exercise. Additionally, as we have noted elsewhere in this Report,[9] *the assumptions underpinning current controls on the use of surveillance devices no longer apply. These assumptions include the efficacy of common law protections, such as trespass, as well as hitherto accepted distinctions between "private" and "public". Even the idea that surveillance is a discrete area, which can be demarcated for regulatory purposes, is no longer applicable, if indeed it ever truly was. Attempting to treat surveillance this way risks implementing obsolete solutions, as happened with the Listening Devices Act 1984 (NSW) ("LDA"), or a legislative patchwork, lacking unity. The enactment of legislation which either targets specific types of devices (and thus leaves gaps in coverage of other types), or, alternatively, renders it more complex through maze-like laws and regulations, is an ineffective means of addressing these issues.*

4.14 At the same time, it is desirable that legislative requirements cause minimal disruption to responsible surveillance users, who have set up often costly systems, and are operating them fairly to protect their legitimate interests.

A SCHEME OF REGULATION

4.15 The Issues Paper[10] *sought suggestions for regulating overt surveillance. Responses are canvassed at para 3.80. As alluded to above, the Commission does not consider it desirable to leave overt surveillance unregulated, as it leaves unaddressed the interests of surveillance subjects. At the same time, the diversity of overt surveillance technologies renders it difficult to regulate. The same type of technology can be used in an infinite number of scenarios and on a greatly varying scale. A scheme of regulation for overt surveillance must accommodate the interests of the person in the*

9. *See para 1.46 and para 1.50-1.58 and para 2.20-2.27.*
10. *New South Wales Law Reform Commission, Surveillance (Issues Paper 12, 1997) at ch 4.*

street, a home dweller guarding the front door, media crews gathering material for the evening news, or a firm assisting with security for a major sporting event, to mention just a few examples. It needs to encompass both the global reach of a satellite tracking system and the intimacy of a fingerprint scanner. All forms of surveillance device have the potential to intrude on privacy in an unacceptable way. The Commission proposes, therefore, that legislation governing overt surveillance not be limited in the types of devices to which it applies.

4.16 There is one exception to this, and that is with regard to a small number of devices which fall within the definition of surveillance device and are, indeed, used to conduct surveillance, according to the definitions contained in Chapter 2, but which are not appropriate to regulate in this way. As discussed in the previous chapter[11] medical imaging equipment used for medical purposes is such an example. There may be others. Such devices should be listed in a schedule as being specifically exempted from the operation of the proposed Act.

Self-regulation or legislation?

4.17 The diversity in surveillance technology application requires some flexibility in regulation. As is mentioned elsewhere[12], many surveillance users have implemented voluntary codes of practice to guide their employees or members. These are well-suited to provide flexibility, because they can be adapted to the circumstances of the particular business, industry or other concern. A code can take into account the realities of the environment in which the devices operate. This is a useful feature, to be discussed further below.[13]

4.18 However, in addressing the problems of protecting the privacy rights of the public in the face of inappropriate surveillance, the Commission does not believe that voluntary codes provide the best

11. Para 3.5-3.6.
12. Para 3.80.
13. Para 4.32 and following.

solution.[14] *The Australian Law Reform Commission had this to say on the subject of information privacy:*

> *Would privacy be better served by legislation or by statements of guidelines without the authority of law behind them? Since its establishment, the Privacy Committee of New South Wales has relied heavily on "voluntary guidelines" drawn up, in most cases, in consultation with interest groups, particularly those representing individuals and organisations likely to engage in privacy-invasive activities. These guidelines have generally been based upon principles similar to those recommended in this report. They are purely informal "agreements" with only some of the participants in a limited number of areas of activity. Their impact has therefore been circumscribed. "Gentlemen's agreements" of this sort, especially if reached only with representative industry bodies in particular industries, cannot prevent unacceptable interferences with privacy by those who either are not members of the representative group or who ignore all but the strict letter of the law. A further consequence of an approach that relies solely on guidelines is that it tends to concentrate on particular sectors of activity, particular areas of concern or particular problems that arise. There is the risk of a total lack of protection in areas not covered by up-to-date guidelines. More significantly, a sector by sector approach is likely to proceed on an ad hoc basis, leaving little time for the formulation of overall policies and principles.*[15]

4.19 The misgivings expressed by the ALRC regarding voluntary guidelines resonate in the attempt to formulate policy for regulating overt surveillance. Voluntary codes cannot adequately address such important issues as the need for a consistent regulatory regime for all surveillance devices, and accountability to the public. Those surveillance users who choose not to abide by recommended practices cannot be compelled to do so. This results either in a lack of credibility for the code, or in misguided faith by surveillance

---

14. Discussed at para 3.86 and following.

15. Australia, Law Reform Commission, Privacy (Report 22, 1983) at para 1201. The "voluntary guidelines" approach was repudiated by the Privacy Committee of New South Wales within two years of its promulgation: see para 3.94.

subjects that their interests are being safeguarded, when in fact they may not, which could lead to unguarded complacency.

4.20 In the Commission's view, the public's reasonable expectation of some entitlement to privacy from overt surveillance should be protected by law. At the very least, individuals being recorded without their authorisation should be aware of the fact and of the identity of those responsible and of its purpose. Furthermore, those undertaking the surveillance should be held accountable. These matters can better be addressed through legislation, which applies universally, than through piecemeal voluntary codes or self-regulation lacking real accountability. The practice of overt surveillance should be included within the scope of the proposed Act. Use of overt surveillance, otherwise than in accordance with provisions contained within the proposed Act, would constitute a breach. As discussed earlier,[16] recreational 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.

4.21 Arguments to the effect that it is unfair to place restrictions on an individual's right to employ surveillance devices to protect their property ignore the reality that other legislative controls operate to balance the enjoyment of private property with the amenity of others.[17] Moreover, it is often the case that the place being monitored is legally frequented by the public, and may not even be the property of the surveillance user. It is already the case, and likely to become increasingly so, that public surveillance is carried out by private interests. Recent examples highlighted in the press have included the search for private security personnel prior to the Sydney Olympics,[18] and the phenomenon, new to this country, of "gated suburbs".[19] In 1999,[20] Dr Peter Grabosky, director of research at the

16. *Para 3.4.*
17. *For example, Access to Neighbouring Land Act 2000 (NSW) Pt 2; Environmental Planning and Assessment Act 1979 (NSW) Pt 3; Local Government Act 1993 (NSW) ch 7, s 626.*
18. *L Doherty, "Shortage Sees Firms Get Familiar" Sydney Morning Herald (2 November 1999) at 2.*
19. *D Cameron, "Balmain's Finest Seek Security from the Burglar's*

Australian Institute of Criminology, described the privatisation of crime control and public protection by "crime prevention entrepreneurs" who provide surveillance among their services. All this serves to highlight the diminishing relevance of the public/private dichotomy to a discussion of surveillance regulation.[21]

4.22 Some might argue that legislative measures are heavy-handed, given little hard evidence of abuses by overt surveillance operators. One response to this is that any abuse is impossible to quantify. From time to time examples have come to light.[22] *The potential for abuse of surveillance is, however, undeniable. As Kevin O'Connor, Australia's first Federal Privacy Commissioner, has argued, personal information is a tradeable commodity in today's society, providing the impetus for modern technology to put our privacy and confidentiality at greater risk than ever before.*[23]

4.23 In any event, many industries and public authorities[24] *currently using overt surveillance have already formulated codes for their own use which reflect privacy concerns. In practice, therefore, the Commission does not expect that most surveillance users would need to modify their practices, so long as they are enforcing their own existing voluntary codes. The main change is to render enforceable practices which many surveillance users say they are engaged in already.*

Touch" Sydney Morning Herald (4 November 1999) at 1; C Miranda and S Birch, "Only the Attorney General Feels Safe" Daily Telegraph (5 November 1999) at 18; T Isles, "Private Cops for Lake Shops" Lake Macquarie News (15 December 1999) at 1.

20. *P N Grabosky, "Crime Control and Policing in the 21st Century", paper presented at the 14th Annual Conference of the Australian and New Zealand Society of Criminology (Perth 27-30, September 1999) at 5.*
21. *See also the discussion at para 2.20-2.27.*
22. *Para 3.33.*
23. *K O'Connor, "Why a National Law to Protect the Privacy of Australians?" (1998) 48(2) Telecommunication Journal of Australia 21 at 23.*
24. *See para 3.80*

4.24 The Commission also gave consideration to the suggestion made in some submissions[25] for a system of licensing[26] to pertain to surveillance equipment. Additional cost and compliance measures which would result, both for users, and for government charged with policing such an extensive system, leads the Commission to the view that this is not a viable proposal. The Irish Law Reform Commission commented:

> *The demand for [surveillance] technology by private actors seems set to grow and not diminish. Restricting this market using traditional tools like import controls, a licensing regime for vendors, a licensing regime for users, etc, is unwieldy and likely to be piecemeal and ineffective.[27]*

Furthermore, while licensing might be expected to have some impact on the manner of using surveillance equipment, it would be unlikely to have much effect on the improper distribution of material obtained by surveillance.

Recommendation 17

The use of overt surveillance otherwise than in accordance with the proposed Surveillance Act, should be unlawful. This will entail compliance with the overt surveillance principles (see paragraph 4.38 and following).

25. *Eg Price Waterhouse, Submission at 5; Privacy Committee of NSW, Submission at 22.*
26. *For example, under Swedish legislation a licence is required for surveillance of a place to which the public has access: Ireland, Law Reform Commission ("ILRC"), Report on Privacy: Surveillance and the Interception of Communications (Report 57, 1998) at para 6.56 (Act on Surveillance Cameras 1990 (Sweden) s 4).*
27. *ILRC Report 57 at para 1.69.*

ELEMENTS OF PROPOSED LEGISLATION

The requirement to give notice

4.25 In Chapter 2,[28] we recommended that surveillance be considered overt, if prior or simultaneous notice of the surveillance were given to those likely to be "captured" by the device. Elements which will help satisfy this requirement are listed at paragraph 2.78. Further discussion of the notice provision will be found at para 4.48.

Exceptions to notice requirement

4.26 In some cases, it may not be practicable for notice to be given. However, according to the framework we propose, if no notice is given, then the surveillance is deemed covert. Yet there may be circumstances where, for public interest reasons, this is not a desirable outcome. For example, media 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. This exemption would apply only in cases of genuine media use, for example to illustrate a news story, otherwise consent of the subject should be sought.

4.27 Home use of surveillance devices is another area which the Commission believes should be exempt from notice requirements. The Commission is reluctant to recommend introducing regulation in a domestic situation where the sole motivation is personal security, and does not extend to, for example, spying on neighbours or, for that matter, guests. The guiding principle is, therefore, that notification is not required if the surveillance is of a general non-targeting nature, and conducted purely for reasonable household security. Some people will choose to erect signs on their property, because they hope this will act as a deterrent. The presence of a sign should not, however, have the automatic effect of deeming a visitor

28. Para 2.78-2.79.

to have consented to being monitored, especially in the case where he or she is part of a group specifically targeted, where the surveillance device is concealed, or where the surveillance is conducted for reasons other than security. For example, it will not be permissible to conceal a camera in a teddy bear to spy on a babysitter without having regard to the provisions contained in Chapter 7, dealing with employment relations. In other circumstances, it may be necessary to obtain a warrant in order to conduct household surveillance.

4.28 A third case in which it may be appropriate to waive notice requirements for the operation of overt surveillance devices is in correctional centres, as well as in vehicles used to transport offenders, and the like.[29] Public safety considerations must be given priority in such situations, and, furthermore, it is reasonable to assume that the surveillance targets would not be surprised to find themselves subject to monitoring in these circumstances. Exemptions from notice requirements for this and the other categories mentioned above should be specified in the proposed Act.

4.29 Surveillance users should exercise care in relying on an exemption from giving notice. Failure to give notice in circumstances where no exemption applies will result in the surveillance being deemed covert, and criminal sanctions may apply. In difficult cases users should be able to seek a ruling from the Privacy Commissioner.[30] It should be further noted that exemption from a requirement to give notice does not mean that the surveillance user is exempt from any other compliance measures.

Recommendation 18

In certain cases specified in the proposed Surveillance Act, surveillance will be regarded as overt, notwithstanding the absence of notification to potential surveillance subjects.

29. *Department of Corrective Services, Submission at 2.*
30. *See para 4.73.*

The surveillance user

4.30 Ultimate responsibility for compliance with the scheme of regulation being proposed rests with the surveillance user. This is the individual or organisation with the authority to direct that surveillance be undertaken. This responsibility should not be delegable to an official within the organisation or to a security contractor, nor should it be claimed to reside in the general public or some such group, for whose benefit it is claimed the surveillance is undertaken. Within an organisation, however, some individual must be given authority to operate the surveillance system in accordance with the requirements of the proposed Act, or to hire a contractor to do so.

4.31 There may also be instances in which surveillance schemes are operated jointly by partners. For example, local government may form an alliance with local businesses to operate a surveillance system.[31] The inclusion of the latter may well be necessitated by the high financial cost involved. In such cases, partners should be jointly responsible, so as to ensure complete accountability to the public.[32]

---

31. Eg "Castle Hill police last week took charge of state-of-the-art video equipment required to satisfy updated legislative requirements. The digital video camera will be used to record search warrants, interviewing suspects at crime scenes, location and quantities of drug evidence and also for general surveillance. ... The video equipment was donated by the Hills Chamber of Commerce and Industry which approached local electrical retailers after it became aware of the police's need for the new equipment": G Moses, "Camera Helps Cops Collar Crims" Hills News (17 August 1999) at 1.

32. "Construction of CCTV surveillance systems in public spaces depends crucially on a strategic alliance between the local state and local private capital. Local state involvement is necessary because of municipal responsibility for the areas that make up the public spaces of city centres in which cameras operate. The high financial costs of installing and running a system, however, mean that individual local councils are unable or unwilling to finance CCTV systems unilaterally. ... The construction of a partnership between the local public and private sectors is, however, fraught with

Codes of practice

4.32 Although the Commission believes legislation is essential to underpin the use of overt surveillance, codes of practice have a very useful role to play. Formulating a code would require surveillance users to give consideration to the overt surveillance principles, discussed below, before incorporating them into the day-to-day operation of the system. While it is envisaged that such codes would be mandatory, they would operate essentially as an internal document to guide those managing the system. The failure to draft a code of practice in accordance with the proposed Act would constitute a breach. However, it is important to note that a breach by the surveillance user of its own code of practice is not intended to give rise to any right of action in another party.

4.33 Consistency in surveillance use assists both surveillance users and the general public, by allowing all parties to become accustomed to acceptable practices, and gain a better understanding of their respective rights and responsibilities. A code has the potential to facilitate consistency in practice across a number of surveillance systems operated by the one user (such as a supermarket chain), or across an entire industry (such as retail traders). The latter becomes more likely if industry umbrella organisations, with input from their members, draft industry-wide codes. This may increase consumer confidence in the surveillance practices of the particular industry, leading to benefits in both image and even profits.[33] It would be in the interests of the industry

---

tensions because of the way in which CCTV occupies an ambiguous position, both geographically and conceptually, on the boundary between the private and public domains. From the perspective of local councils there are anxieties about committing public funding to a project which may mainly appear to serve the needs of local private commercial interests and which raises sensitive civil libertarian questions about the invasion of privacy": N R Fyfe and J Bannister, "City Watching: Closed Circuit Television Surveillance in Public Spaces" (1996) 28 Area 37 at 40.

33. *The Internet Industry Association ("IIA"), which describes itself as Australia's national internet and e-commerce representative body, wrote to the Prime Minister in 1998, requesting the introduction of*

to apply pressure to rogue members who pay lip service only to the relevant code, or who choose openly not to subscribe. In this sense, there is a role for self-regulation within industries, with benefits flowing to the public.

4.34 A further advantage is that a code or set of operating principles is a useful tool by which regulators can measure compliance with the Act. If a code is deficient in its embodiment of one or more of the legislated principles, this may signal a failure in practice to comply with those principles.

4.35 Another important consideration in requiring certain surveillance users to formulate codes is that these are then available to any member of the public who is subject to the surveillance. This is consistent with the goals of furthering accountability, by making it possible to identify the surveillance user and the purposes of the surveillance.

4.36 The Commission is mindful of not imposing unnecessary or burdensome obligations on surveillance users. Many of the submissions from surveillance users indicated a desire to use codes, and indeed many already have codes of practice in place which

---

Commonwealth privacy legislation for the private sector: Internet Industry Association, "Letter to the Prime Minister on Privacy Legislation" «www.iia.net.au/news/981012.html». The letter states: "While this request might seem incompatible with our professed and demonstrable commitment to self-regulation, there are ... reasons why we believe it is appropriate for your government to take a stronger position on the issue of privacy. ... [W]e believe the continued uptake of the Internet in Australia depends on strong consumer confidence in the medium, particularly where e-commerce is concerned. ... As with many difficult regulatory issues which the Internet has created, such as the regulation of online content, the IIA considers that industry should have first option to assume responsibility for issues of social concern. Nevertheless, it is not inappropriate for government to provide a safety net, to catch businesses that are not prepared to assume responsibility for themselves. Fortunately, in the area of privacy we believe the interests of citizens coincide with the interests of the market, making this a low risk initiative, but with a strong upside."

could be adapted with little change for the use proposed here. The Office of the Privacy Commissioner can make an important contribution in assisting a surveillance user to draft a suitable code. It could also formulate a list of issues which codes need to address in order to comply with the overt surveillance principles.

Exceptions

4.37 For small surveillance users, such as family-run businesses or people seeking household protection, the need to formulate a code of practice would be cumbersome and of little practical use. Such users should be exempt from meeting this requirement. Only "relevant surveillance users" would be required to formulate and comply with a code of practice. Regulators, in consultation with users and the security industry, should develop criteria to establish who would fall within this category. One possible criterion is the total number of surveillance devices operated by the user, regardless of whether installed on one or more premises. Another criterion might be that businesses operating as part of a franchise be required to draft and adopt a common code. Of course, smaller users would be permitted to adopt a code, and could subscribe to one operating within the same industry. All surveillance users, whether or not required to implement a code of practice, would nevertheless be bound to comply with the overt surveillance principles.

Recommendation 19

"Relevant surveillance users" (defined in the proposed Surveillance Act according to criteria such as the number of devices operated) should be required to formulate and act in accordance with a code of practice consistent with the overt surveillance principles. A relevant surveillance user should make its code available for perusal by any member of the public subjected to its surveillance.

Overt surveillance principles

4.38 In its 1983 Report on Privacy,[34] the Australian Law Reform Commission reviewed a number of formulations of information privacy principles, such as those of the Organisation for Economic Co-operation and Development (OECD). The Report stated:

> *These and other attempts suggest that there are a number of fundamental themes that underlie all statements of information privacy principles. These themes can be made explicit.[35]*

4.39 Similarly, existing industry codes of practice pertaining to surveillance usage identify obvious common areas of concern, such as maintaining privacy in changerooms, and handling and storage of surveillance video tapes. Enunciating a set of principles for overt surveillance would introduce clarity and consistency to the practice, which the Commission believes would serve the public interest, without imposing a burden on surveillance users. In practice, the Commission expects that many existing codes already accord with the principles, or would need only slight amendment to do so.

4.40 The principles proposed by the Commission are set out below. There will be some degree of overlap between them. They are not designed to work in isolation, but to interact so as to allow for adjustment between conflicting interests. For example, while one principle allows overt surveillance to be used for specified purposes, the fact that this condition is satisfied does not preclude the subject from complaining that his or her reasonable privacy expectation was, nevertheless, breached, or that the manner in which the surveillance was conducted was inappropriate. Furthermore, it would not be permissible to derogate from these principles, for example, by means of contractual arrangements. Non-compliance with overt surveillance principles, unlike codes of practice, constitute a breach of the proposed Act.

---

34. Australian Law Reform Commission ("ALRC"), Privacy (Report 22, 1983) Vol 2 at Appendix A.

35. ALRC Report 22 at para 1195. The Privacy Act 1988 (Cth) contains a list of Information Privacy Principles at Section 14.

PRINCIPLE 1: OVERT SURVEILLANCE SHOULD NOT BE USED IN SUCH A WAY THAT IT BREACHES AN INDIVIDUAL'S REASONABLE EXPECTATION OF PRIVACY

4.41 The expression "reasonable expectation of privacy" is used at para 1.13 as an intuitive measure of the acceptability of surveillance conduct. The Irish Law Reform Commission stated the view that privacy is a personal right, "following the personal space of the person".[36] *The Commission agrees, and believes that for this reason the right is not extinguished by entry into either a public space or onto another's private property. While a person's physical location will clearly have a bearing on whether his or her expectation of privacy was reasonable in the circumstances, it would not be just to make this the sole factor. Defining the limits of the right in objective terms such as "public" and "private" or "inside" and "outside" might seem to be expedient, but these are likely to lead to confusion. For example, into which category should the following fall: an open window at ground level, the same window covered by a net curtain, a balcony, a tent in a camping ground, a parked car, or a front yard?*[37]

4.42 ***Other factors***[38] *to consider in determining whether a person had a reasonable expectation of privacy include the nature or customary use of the location (eg a change room, or a room for mothers to breastfeed babies), the type of surveillance device being employed,*[39] *and even the timing of the surveillance.*[40] *Other*

36. *ILRC Report 57 at para 2.11.*
37. *cf Victoria, Department of Justice, Surveillance Devices Bill (Discussion Paper, 1998) at 7.*
38. *See also ILRC Report 57 at para 2.13-2.19.*
39. *Eg it might be reasonable to use visual surveillance devices to monitor a shopping mall, but not aural devices which would pick up conversations.*
40. *"Surveillance, even in a public place, which deliberately seeks out or targets the intimate corners of a person's life or personality, such as at a time of death, injury or grieving, where those affected are vulnerable or are otherwise unable at the time to fend off such surveillance may violate a person's "reasonable expectation" of*

considerations might include the behaviour and intention of the surveillance subject. For example, even in a setting normally regarded as private, if a person behaves in a way that unambiguously draws the attention of onlookers, he or she cannot claim to have had a reasonable expectation of privacy. By extension, people who for one reason or another willingly court publicity, such as some politicians and film stars, may be entitled to a lower expectation of privacy in some contexts than ordinary members of the public. This should not, however, lead to the consequence that people in the public eye thereby forfeit an expectation of privacy. In its adjudication[41] on the Woods case, the Australian Press Council upheld a complaint against the newspaper. It rejected the public interest argument put forward by the newspaper, that the Senator "was a public figure involved in issues of legitimate interest to the public, who after all paid his salary, and his wife was involved in the issues being aired before the public."[42] The Council regarded publication of the photographs as "a breach of its principle relating to 'respect for the privacy and sensibilities of individuals' and [saw] no compelling public interest in the obtaining and publication of pictures of this kind".

4.43 A reasonable expectation of privacy cannot be ousted through the provision of notice of surveillance. The giving of notice is required as a prerequisite for surveillance to be deemed overt, unless falling within one of the exceptions referred to at para 4.26 and following. Thus, surveillance users cannot subvert the privacy protection offered by this principle simply by mounting numerous signs declaring the area to be under surveillance. If this were permitted, then change rooms and the like could be treated no differently to pedestrian malls in terms of privacy protection.

PRINCIPLE 2: OVERT SURVEILLANCE MUST ONLY

privacy": ILRC Report 57 at 2.14.

41. *No 916 (April 1997). See Australian Press Council, Annual Report 1997 at 114-115. A Sydney newspaper published "sneak photographs" of Senator Bob Woods and his wife in private conversation in their backyard at a sensitive time.*
42. *Australian Press Council, Annual Report 1997 at 115.*

BE UNDERTAKEN FOR AN ACCEPTABLE PURPOSE

4.44 The legitimate uses of overt surveillance were discussed earlier.[43] As these can be identified, the Commission believes that overt surveillance should be permissible only for one or more of these specified purposes. They are:

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

4.45 To avoid breaching the proposed Act, surveillance users will need to ensure that their operations can be justified according to one or more of these criteria. An extra condition should apply to public bodies. Their use of surveillance must be in the interests of the general public, which is funding the establishment and maintenance of the system. This is also intended to foster transparency and accountability. For example, the installation of security cameras by a local council must be intended for the benefit of ratepayers at large, not for a few businesses in the monitored area, although it can, of course, serve both interests simultaneously.

4.46 Protection of the person and property are relatively straightforward. Protection of the public interest and protection of a legitimate interest are broader categories, created so as not to exclude overt surveillance for another socially acceptable purpose. Examples are road safety and coastal surveillance.[44] The taping of dealings between a person and that person's client, where notified, is another possible example. Categories 3 and 4 cannot be overly prescriptive, and must be flexible enough to allow for a range of circumstances. Overt surveillance by the media is a case in point, where even "media" is an imprecise term. For example, there have been cases of camera crews trailing police and medical personnel in quest of real-life drama to capture for television. Examples have

43. See para 3.7-3.28.
44. See fuller discussion at para 3.12 and following.

included individuals suffering heart attacks[45] or humiliating themselves while undertaking sobriety tests. Such instances of "real TV" might be regarded as protecting the public interest, or protecting a legitimate commercial interest, or neither of these, depending on the circumstances. Similar issues might arise when filming, for example, a beach scene. This could be for the purpose of illustrating a report on skin cancer, or the images of topless or scantily clad female beachgoers may be sold on the Internet without the consent, let alone payment, of the surveillance subjects.[46] In cases of doubt, recourse may be had to the Privacy Commissioner for a ruling as to whether the purpose is acceptable within the meaning of the proposed Act.[47] However, even if the "acceptable purpose" criterion is satisfied, surveillance users will still need to exercise care with regard to other principles, such as respecting the subject's reasonable expectation of privacy.

PRINCIPLE 3: OVERT SURVEILLANCE MUST BE CONDUCTED IN A MANNER WHICH IS APPROPRIATE FOR PURPOSE

4.47 Earlier[48] we alluded to the revelation of video footage from Burswood Casino, which was evidence of the fact that one or more security camera operators, in the course of carrying out permissible surveillance, used the equipment's capabilities in a quite improper

---

45. Q Burrows, "Scowl Because You're on Candid Camera: Privacy and Video Surveillance" (1997) 31 Valparaiso University Law Review 1079 at 1108.

46. As was reported to be taking place in Miami, according to a report in the Sun-Sentinel (South Florida): D Bunuel, "South Beach Sunbathers Unwittingly Become Fodder for Internet Voyeurs" (25 February 1999) at Mediaeater, "Surveillance Camera Project" «www.mediaeater.com/cameras/news/022598.html». According to a source from the adult publication industry, quoted in the report, "voyeur sites are the biggest thing on the Internet right now", a billion dollar industry with between 45,000 and 200,000 sites up at any time.

47. See para 4.73.

48. Para 3.33.

manner by zooming in on female patrons' apparel. In that case the surveillance was being undertaken for an acceptable purpose, but being conducted in a manner inappropriate to that purpose, and infringing on the subjects' reasonable privacy expectations. This kind of monitoring, incorporating what might be termed a "perve" factor, is sufficiently disturbing when carried out as just described, but also has the potential to be used in a discriminatory fashion. Operators of street safety cameras, for example, have the capability to zoom in on, as well as the liberty to prolong surveillance of, an individual or group. While elderly women, as a statistical group, may be less likely than young males to commit crimes or engage in other unacceptable conduct, the onus must be on surveillance users to avoid targeting particular groups or individuals. Codes of practice or other guidelines should make this explicit. Otherwise, there is a risk that surveillance is conducted according to prejudices, such as those that dictate that members of particular minorities, or even groups of young people in general, are more predisposed than other sectors of society to behave in undesirable ways. Unless relevant to the legitimate purpose for which the camera is operated, such practices may well be excessive or discriminatory. Even if the attention of the camera operator is drawn by no more than idle curiosity, it should still be avoided as a distraction compromising the efficacy of the system.

PRINCIPLE 4: NOTICE PROVISIONS SHALL IDENTIFY THE SURVEILLANCE USER

4.48 If surveillance users are to be held accountable for their conduct, they must be readily identifiable. Part of the process of notifying surveillance subjects that they are under surveillance should involve providing information about the identity of the user. To the extent that subjects give their consent to being watched, the basic information needed to inform a decision must include the identity of the watcher. Even though consent is often meaningless in this context due to the unfeasibility of "choosing" to avoid surveillance in modern urban life, the public still has the right to know who is watching. The identity of the user should include an address at which the user can be contacted, otherwise a front name

can be used to avoid accountability. Furthermore, members of the public and the Privacy Commissioner need to know where inquiries and complaints can be directed.

4.49 It is not envisaged that every notice advising that the area is under surveillance carry all of this additional information. A member of the public should, however, be able to discover this information without undue difficulty. With regard to media organisations, although it was proposed above[49] that they be exempt from the requirement to give notice of carrying out overt surveillance activities, their personnel should be readily identifiable by station logos while doing so.

PRINCIPLE 5: SURVEILLANCE USERS ARE ACCOUNTABLE FOR THEIR SURVEILLANCE DEVICES AND THE CONSEQUENCES OF THEIR USE

4.50 All surveillance users must be accountable for their devices and the activities undertaken with them. They must also be accountable for the records or output of those devices, such as videotapes. In practice, users should be held responsible for everything pertaining to the operation of surveillance devices, including the system's proper operation, the conduct of security staff involved, and the misuse of any information or product generated by the surveillance. Responsibility cannot be delegated to others, such as security contractors.

4.51 Surveillance devices must be available for inspection by the Office of the Privacy Commissioner. This is to monitor for compliance with any prescribed standards, as well as to investigate complaints, such as the positioning of devices. This is discussed below at para 4.68 and following. To facilitate the task of inspection, it is recommended that all public sector surveillance users, as well as all relevant surveillance users (as described above at para 4.37), maintain a register containing details of the number, types and locations of all their overt surveillance devices, together

49. Para 4.26.

with any other details from time to time required by the Privacy Commissioner, such registers being available for inspection by the Privacy Commissioner at any time.

Recommendation 20

All public sector surveillance users, as well as all "relevant surveillance users" operating within the private sector, should maintain a register containing details of the number, types and locations of all their overt surveillance devices, together with any other details from time to time required by the Privacy Commissioner. Such registers should be available for inspection by the Privacy Commissioner at any time.

Public sector

4.52 Because of the public funding involved, the likely wider scale of coverage, and the possibility of information-sharing between them, when surveillance is undertaken by government departments, public authorities and the like, accountability provisions should be more stringent than those required of the private sector. This is not to imply that a lower standard of conduct from the private sector is acceptable, but merely to recognise that an undue burden may be placed on businesses and other private entities forced to comply with too many procedural requirements. Public bodies, such as local councils,[50] which may run surveillance systems in cooperation with private entities, should be under the same obligations regarding accountability as systems that are wholly publicly funded.

50. The State Government has recently developed guidelines for CCTV in public places. The definition of "public place" is from the Local Government Act 1993 (NSW), and refers to public reserves, public bathing reserves, public baths or swimming pools, public roads, public bridges, public wharves or public road-ferries, together with public transport and car parks: «www.lawlink.nsw.gov.au/cpd.nsf/pages/cctv_intro».

Annual reports

4.53 Government departments, statutory authorities, local councils and any other public body should be required to include in their annual reports[51] information about their overt surveillance systems. In addition to statistical information concerning the extent of the system and its associated costs, the report should give an indication of the results believed to have been obtained through the use of such devices. It is acknowledged that this may not be information that can be objectively ascertained. For example, the fact that certain types of crime may have decreased may not necessarily be attributable all or in part to any particular strategy, such as the installation of street cameras. However, for the body in question to be truly accountable to its public, there must be some basis on which to justify both the ongoing surveillance, and its associated cost. A requirement to report may have a desirable flow-on effect, in helping prevent public sector surveillance users from becoming complacent about their existing systems. If surveillance systems are to be effective and credible, they must be properly maintained and their mode of operation reviewed from time to time.[52]

---

51. Annual Reports (Departments) Act 1985 (NSW) Pt 2; Annual Reports (Statutory Bodies) Act 1984 (NSW) Pt 2; Local Government Act 1993 (NSW) s 428.

52. The Sydney Morning Herald reported that, following a stabbing at Sydney's Town Hall railway station in the early hours of New Year's Day, 1999, an audit discovered that a third of the station's surveillance cameras were either not working or were out of focus. In addition to the technical faults, some station staff were blamed for failing to carry out a job specification requiring them to ensure the closed circuit cameras were operating: A Bernoth, "See No Evil: Rail Cameras on Blink" Sydney Morning Herald (13 January 1999) at 1.

PRINCIPLE 6: SURVEILLANCE USERS MUST ENSURE ALL ASPECTS OF THEIR SURVEILLANCE SYSTEM ARE SECURE

4.54 Users must ensure that the surveillance is carried out in such a way that there is no unauthorised access to equipment, recordings, or any other aspect of the process which could compromise the privacy of any of the surveillance subjects. Exemption from the requirement for a code of practice[53] does not release a surveillance user from the need to exercise care in relation to security. Where, however, a code of practice is in place, it needs to address a number of issues.

Staff

Qualifications

4.55 Under the Security Industry Act 1997 (NSW), a person must hold a licence in order to carry out a security activity.[54] A person carries on a "security activity" if, in the course of employment or of conducting a business, the person among other things patrols, protects, watches or guards any property (including cash in transit),[55] or installs, maintains, repairs or services security equipment.[56] "Security equipment" is defined as including "any mechanical, electronic, acoustic or other equipment designed or adapted to provide or enhance security or for the protection or watching of any property."[57] It seems, therefore, that staff hired to monitor security cameras are required to hold a licence under the Act. The Commission believes this should be the case and that the Act be amended to reflect this. Under the Security Industry Act 1997, the Commissioner of Police cannot grant a licence if the applicant is not a fit and proper person,[58] and may refuse a licence

53. *See para 4.37.*
54. *Security Industry Act 1997 (NSW) s 7. For exceptions, see s 6 and Security Industry Regulation 1998 (NSW) cl 5.*
55. *Security Industry Act 1997 (NSW) s 4(b).*
56. *Security Industry Act 1997 (NSW) s 4(c).*
57. *Security Industry Act 1997 (NSW) s 3(1).*
58. *Security Industry Act 1997 (NSW) s 15(1)(a).*

if this is considered contrary to the public interest.[59] *The Commission proposes that staff operating surveillance equipment in control rooms or similar circumstances must be licensed in accordance with the Security Industry Act 1997.*

4.56 In the case of small businesses or other concerns where electronic surveillance is conducted on a smaller scale without the need for a control room and security personnel, the obligation to be licensed is dispensed with. This might arise where a person employed by the surveillance user to perform other duties, such as sales or management, is also given responsibility to operate the surveillance system. The main reason for the distinction regarding licensing requirements is that security personnel are engaged fully in activities such as surveillance and are likely to be conducting surveillance activities through real-time monitoring. This gives them a potentially greater impact on the privacy of surveillance subjects through their ability to control, for example, camera functions and targeting, than the employee occupied in other activities, or where real-time monitoring is not taking place.

Recommendation 21

Staff operating equipment in control rooms (or in similar circumstances) with which to conduct overt surveillance, should be licensed in accordance with the *Security Industry Act 1997* (NSW). The *Security Industry Act 1997* (NSW) should be amended to provide that "security activity" is defined as including the monitoring or operating of a surveillance device or system.

59. Security Industry Act 1997 (NSW) s 15(3).

Training

4.57 All staff involved in the operation of the surveillance equipment, or with access to it or to any tapes, recordings or other data produced by it, must be properly trained in procedural matters, whether or not they are licensed security personnel within the meaning of the Security Industry Act 1997 (NSW). Procedures for the use of surveillance will be set down in the code of practice applicable to that business or other concern. Where, due to an exemption, no code of practice applies, the surveillance user must be responsible for ensuring that such personnel are properly acquainted with the correct procedures and their responsibilities thereto. The Office of the Privacy Commissioner can play a very useful role in formulating easily comprehensible guides for such use, setting out the privacy objectives to be met, and the standard measures to be undertaken, such as protocols for the secure storage of tapes.[60]

4.58 Staff must also be made aware of the possible consequences, including dismissal and even criminal liability, for incorrect or improper behaviour. Of course, these standards of behaviour also apply to surveillance users themselves, or to any person given responsibility for managing surveillance by the surveillance user. Any guides issued by the Privacy Commissioner, such as those just referred to, can also include a summary in plain English of the legal responsibilities and possible consequences for breach arising under the proposed Surveillance Act.

Surveillance material

4.59 In cases of real-time monitoring, only those persons with responsibility for undertaking such monitoring should be in the control room or area. Examination of tapes or other recordings should also, likewise, be restricted to those with the responsibility to do so, whether that be security staff, the proprietor of a business, a homeowner or, in the case of a local council, for example, a committee including councillors and community representatives. Ownership of the images appearing on videotapes is not an issue

60. See para 4.69.

dealt with in this Report. Nevertheless, great care must be taken that such material be dealt with in an appropriate manner. For example, videotape recordings or images obtained from surveillance should not be sold, given to unauthorised persons, used for entertainment purposes, or displayed as "wanted" posters.[61]

4.60 Procedures must be developed whereby videotapes (or other recording media) are designated for use in a particular sequence, and rotated according to that sequence. After the last tape is used, the sequence begins again, so that the old material is replaced with the new recording. Periodically, the tapes will need to be discarded and replaced with new ones to maintain quality. The recordings themselves must be securely stored so as to prevent theft or unauthorised access. They may be accessed only for the proper purposes (see Principle 7 below), and may not be copied or transcribed. All of these matters must be addressed by codes of practice, where these apply.

PRINCIPLE 7: MATERIAL OBTAINED THROUGH SURVEILLANCE TO BE USED IN A FAIR MANNER AND ONLY FOR THE PURPOSE OBTAINED

4.61 Just as overt surveillance may only be carried out for one or more of the permissible purposes under Principle 2, so also any material obtained as a result, such as recordings, may only be put to the same purpose. 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. The Commission does not believe there is a need to widen this exception to include the general public.

4.62 Adherence to the principle means that surveillance users are

61. Eg S Verghis, "Wanted Shots 'Outrageous'" Sydney Morning Herald (22 January 2000) at 15.

responsible for compliance with the following prohibitions in relation to material obtained through surveillance:

- *no unauthorised viewing, listening etc;*
- *no unauthorised copying of all or any part, and where authorised copies are made, these should be strictly limited in numbers;*
- *no unauthorised transfer or conversion to another format of the material obtained by surveillance;*
- *no unauthorised person to be given access;*
- *no amendment, deletion or alteration.*

4.63 "Authorised persons" should be listed in the code of practice by name or position. Where no code applies, only the surveillance user, the person he or she has previously made responsible for operating the surveillance system, or a law enforcement officer, can be so authorised.

PRINCIPLE 8: MATERIAL OBTAINED THROUGH SURVEILLANCE TO BE DESTROYED WITHIN SPECIFIED PERIOD

4.64 Material obtained through surveillance cannot be kept indefinitely, and must be taped over or destroyed within a specified time period. The choice of a maximum time for which recordings may be kept is somewhat arbitrary. Suggestions raised in submissions ranged from 12 hours[62] to 30 days.[63] It is not always clear whether any particular tape might have some evidentiary value. It may, for example, provide a useful lead in tracing the movements of a missing person, whose disappearance is not even reported for some days. The Commission feels that setting the limit at 21 days is a reasonable period for the tapes to be kept available,

62. *NSW Council for Civil Liberties, Submission at 3.*
63. *Dr Brian Simpson, Submission at attachment (Scottish Council for Civil Liberties "Draft Rules for the Use of CCTV in Public Places", draft rule 12).*

so as neither to risk permanent loss of potentially valuable evidence, nor pose an unacceptable risk to privacy. Surveillance material obtained overtly and genuinely for media purposes need not be destroyed within this time limit if the intention is to retain it for file footage.

4.65 Extensions of time should be available where it is reasonably believed that recordings contain useful evidence or can aid in investigations relevant to either civil or criminal proceedings. The Commission proposes that it should be open to any individual to apply to a magistrate for an order to retain a surveillance recording beyond the suggested 21 day period in a place specified by the order. Recordings could then be held by the police or in some other nominated place.

4.66 Surveillance material cannot be copied or converted to another format, thereby avoiding the operation of this principle, without the express consent of the Privacy Commissioner.

THE PRIVACY COMMISSIONER'S ROLE

4.67 The functions of the Privacy Commissioner are largely set out in the Privacy and Personal Information Protection Act 1998 (NSW).[64] *The proposed Surveillance Act gives the Privacy Commissioner new powers and functions to facilitate the objectives of the legislation. Procedures for dealing with complaints and reviews are discussed more fully in Chapter 10.*

Powers

General

4.68 The general functions[65] *of the Privacy Commissioner which are listed in the Privacy and Personal Information Protection Act 1998 (NSW) would well serve the goals of the legislation proposed*

64. *Privacy and Personal Information Protection Act 1998 (NSW) Pt 4.*
65. *"Function" includes a power, authority or duty: Privacy and Personal Information Protection Act 1998 (NSW) s 3.*

here with regard to overt surveillance, and in most cases would require only slight amendment. Some of these functions, which appear at section 36(2), refer specifically to the information protection principles, contained in Part 2 of that Act, but could just as well apply to the overt surveillance principles proposed by the Commission. Examples of such functions include:

> *(a) to promote the adoption of, and monitor compliance with, the information protection principles*
>
> *...*
>
> *(d) to provide assistance to public sector agencies in adopting and complying with the information protection principles and privacy codes of practice; and*
>
> *...*
>
> *(k) to receive, investigate and conciliate complaints about privacy related matters ...*

4.69 In the context of overt surveillance, these functions could be extended to include, for example, assisting both the public and private sectors in drafting codes of practice, and establishing secure surveillance systems. Such assistance might be in the form of printed guidelines or through some form of educational program.

Appointment of inspectors

4.70 As well, the Privacy Commissioner should be given power to appoint inspectors. Under the accountability principle,[66] it is proposed that certain users be required to maintain registers setting out details of their overt surveillance systems, which can then be inspected as deemed necessary by the Office of the Privacy Commissioner. In addition, inspectors should be empowered to enter premises for the purpose of inspecting surveillance devices, where there is a reasonable belief that an offence against the proposed act has been committed. Similar provisions exist in other enactments. Thus, if inspectors appointed under the proposed Surveillance Act were given rights analogous to those of inspectors appointed under the Casino Control Act 1992 (NSW), they could enter business premises to do one or more of the following:

---

66. See Principle 5.

(a) observe the operation of the surveillance system;

(b) ascertain whether the operation of the surveillance system is being properly conducted;

(c) ascertain whether the provisions of the proposed Act are being complied with;

(d) exercise any other function under the proposed Act.[67]

4.71 The Trade Measurement Act 1989 (NSW) grants inspectors the power of entry into a place of business,[68] *in order to examine and test measuring instruments.*[69] *An inspector may require the production of records pertaining to the instrument.*[70] *This power is said to exist "for the purpose of investigating an offence against this Act that the inspector reasonably believes has been committed, or for the purpose of exercising any function of an inspector under [the] Act."*[71] *An inspector can only enter residential premises with the occupier's consent or under the authority of a search warrant.*[72] *In the surveillance context, a similar power might be created to allow for inspection where, for example, a member of the public makes a complaint against a business or neighbour, alleging that a security camera is fixed in such a way as to film inside his or her residence. It would be an offence against the proposed Act to obstruct an inspector in carrying out his or her duties.*

Determining standards

4.72 The Superintendent of Trade Measurement is responsible for providing and maintaining standards of measurement,[73] *with which measuring instruments used for trade*[74] *must comply.*[75]

---

67. Casino Control Act 1992 (NSW) s 108.
68. Trade Measurement Act 1989 (NSW) s 60(1).
69. Trade Measurement Act 1989 (NSW) s 61(a).
70. Trade Measurement Act 1989 (NSW) s 61(b).
71. Trade Measurement Act 1989 (NSW) s 60(1).
72. Trade Measurement Act 1989 (NSW) s 60(2).
73. Trade Measurement Act 1989 (NSW) s 10; Trade Measurement Administration Act 1989 (NSW) s 3(1).
74. Trade Measurement Act 1989 (NSW) s 4.
75. Trade Measurement Act 1989 (NSW) s 7, 11-14.

A similar power would, it is envisaged, reside in the Privacy Commissioner to determine what specifications, standards or restrictions, if any, should apply to devices used for overt surveillance. For example, it may be stipulated in certain circumstances that devices be no more sensitive or have no greater surveillance capacity than is necessary for the stated purpose (in accordance with Principle 3).

Rulings

4.73 In order to provide some measure of certainty and help avoid problems arising at some later date, it would be useful if the Privacy Commissioner were able to give binding rulings on matters of a preliminary or threshold nature. For example, a surveillance user might seek to ascertain whether he or she falls into a category exempted from the requirement to give notice of overt surveillance. Alternatively, a user may desire clarification as to whether the purpose for conducting overt surveillance is an acceptable purpose[76] within the meaning of the proposed Act.

THE EMPLOYMENT CONTEXT

4.74 The Commission considers that overt surveillance of employees by employers should be regulated according to the general framework proposed for overt surveillance, with the exception of the notice requirements outlined in Chapter 2.[77] In formulating the content of the notice requirements, we have had regard to current Codes of Practice, which although not legally binding, serve as guides to good practice. These Codes of Practice may also provide guidance to employers when assessing whether their overt surveillance practices comply with the overt surveillance principles.

---

76. See Principle 2.

77. We note the view of the Chamber of Manufactures of NSW (Industrial) that overt surveillance should be regulated by a voluntary code of practice, Submission at 10. We similarly note the view of the NSW Young Lawyers Criminal Law Committee that overt surveillance is best dealt with between employer and employee, Submission at 9.

Codes of practice

4.75 The most comprehensive guidance regarding overt video surveillance in the workplace is found in the Privacy Committee's Code of Practice for the Use of Overt Video Surveillance in the Workplace (the "Code").[78] *The focus of this Code is on the importance of notification and consultation. Mirroring the Workplace Video Surveillance Act's default definition of overt surveillance, the Code recommends that employees be given written notice of the intended surveillance a reasonable period of time before the cameras are used and that surveillance equipment be clearly visible, with signage. Expanding on the notification requirement, it is recommended that the prior notice should state the location of the proposed surveillance, the specific purpose and the identity of the person responsible for the conduct of the surveillance. In addition to notification, employers should consult their employees before commencing surveillance and cameras should only be installed in areas and operated during hours which were the subject of prior consultation. The Code also places limits on access to and retention of tapes, and empowers the Privacy Committee to conciliate complaints regarding contravention of the Code, make recommendations, cite instances of serious breach in its annual report or issue a special report to parliament regarding exceptional breaches.*

4.76 In March 2000, the Australian Privacy Commissioner issued Guidelines on Workplace E-mail, Web Browsing and Privacy. The purpose of these Guidelines was "to recommend steps that organisations can take to ensure that their staff understand the organisation's position on [use of e-mail and web browsing] through the development of clear policies".[79] *In essence, the Guidelines provide a framework for the conduct of overt surveillance of employee e-mail and internet usage. It is recommended that organisations develop policies that advise employees what information is logged and who has access to the logs and contents of staff e-mail and*

78. «http://www.lawlink.nsw.gov.au/ pc.nsf/pages/videocodeir».
79. Australian Privacy Commissioner, Guidelines on Workplace E-mail, Web Browsing and Privacy (30 March 2000) «http://www.privacy.gov.au/issues/ p7_4.html».

browsing activities. In addition, employees should be advised of any intended monitoring of e-mail and internet usage.

Performance monitoring

4.77 Given the highly controversial nature of performance monitoring and the many forms that the practice can take, the Commission wishes to highlight that substantial consideration must be given to the overt surveillance principles when performance monitoring is in issue.

4.78 Principle 2, which provides that overt surveillance must only be undertaken for an acceptable purpose, is of particular relevance. Whether a particular form of performance monitoring is being undertaken for an acceptable or unacceptable purpose will need to be assessed on a case by case basis. However, an example of what may, in the Commission's view, be an acceptable purpose, is scanning employee e-mails for indications of unauthorised use. This would fall within the "protection of a legitimate interest" category as employers have a legitimate interest in ensuring that employees are not utilising the e-mail system for purposes such as distributing discriminatory or defamatory material.

4.79 Principle 3, which relates to the manner in which surveillance is conducted, will also be of particular relevance to performance monitoring. Again, whether the manner in which performance monitoring is conducted is appropriate for the purpose will depend on the individual circumstances of the case. However, we consider that factors such as the degree of consultation with employees and the frequency of the monitoring[80] may be relevant. To return to the e-mail example, we note that the Australian Privacy Commissioner has stated in the Guidelines on Workplace E-mail, Web Browsing and Privacy that:

> *While it is acknowledged that access to staff e-mails and browsing logs by system administrators may be required in certain circumstances, it is unlikely that pervasive, systematic*

80. Privacy Committee (1995) at 53-54.

and ongoing surveillance of staff e-mail and logs should be necessary.[81]

81. Australian Privacy Commissioner.

5. Covert surveillance by law enforcement officers

- Introduction
- Listening Devices Act 1984 (NSW)
- The proposed Surveillance Act

INTRODUCTION

5.1 Chapter 2 outlines in some detail the proposed framework for the regulation of covert surveillance.[1] *There are two significant features of the recommended approach. First, authorisation must, in every case, be obtained to carry out covert surveillance. Covert surveillance carried out without the requisite authorisation will be unlawful. However, where it has been either impossible or impracticable to obtain prior authorisation, retrospective authorisation may be granted.*

5.2 Secondly, three main contexts in which covert surveillance could legitimately be carried out can be distinguished. These are in the area of law enforcement, in the "public interest"[2] *and in the course of employment. In each of these areas, surveillance will be carried out for different purposes and will be governed by different considerations and parameters. It is therefore expedient to develop three separate, although parallel and consistent, regimes of authorisation to apply to the three identified contexts.*

5.3 This approach represents a departure from the way in which covert surveillance is presently regulated. While all Australian legislation currently in force, including the Listening Devices Act 1984 (NSW) ("LDA"), prohibits covert surveillance unless authorisation by warrant is granted by a judge, provision is then made for exceptions to the requirement to obtain a warrant.[3] *The Commission agrees with the principle that covert surveillance, representing as it does serious incursions into privacy, should be*

1. *See para 2.88-2.98.*
2. *See ch 6 for the way in which "public interest" is defined.*
3. *See Listening Devices Act 1984 (NSW) s 5-10, Part 4; Listening Devices Act 1992 (ACT) s 14; Listening Devices Act 1972 (SA) s 7; Listening Devices Act 1991 (Tas) s 5; Invasion of Privacy Act 1971 (Qld) s 43; Surveillance Devices Act 1999 (Vic) s 11; Surveillance Devices Act 1998 (WA); Surveillance Devices Act 2000 (NT) s 20; Telecommunications (Interception) Act 1979 (Cth) Parts II and V; Australian Federal Police Act 1979 (Cth) s 12F, s 12G; Customs Act 1901 (Cth) s 219B; Australian Security Intelligence Organisation Act 1979 (Cth) s 26.*

conducted only where justified and necessary; and that its justification and necessity should be judged independently, before it is conducted.[4] *However, to then make various exceptions to the general prohibition allows additional encroachment on individuals' privacy and erodes the protection afforded by a system of authorisation.*

5.4 In the area of law enforcement, on which this chapter focuses,[5] *it is arguable that exempting a range of circumstances in which covert surveillance can be conducted without prior authorisation is appropriate: covert surveillance can be a valuable tool in investigating and prosecuting offences and, it can be argued, law enforcement officers should be entrusted with deciding when and how to make use of this tool. However, while acknowledging the compelling reasons to allow the use of covert surveillance by law enforcement officers, its close supervision is still called for in light of the considerable potential for invasion of privacy, and/or damage which may result. A system of authorisation for all covert surveillance by all law enforcement officers, without exception, presents a clear, consistent and legitimate approach to regulation.*

5.5 The provisions contained in the LDA authorising the use of listening devices provide a useful foundation on which to base a scheme of regulating covert surveillance by law enforcement officers in respect of all surveillance devices. Based on the approach in the LDA, law enforcement officers would be required to obtain a warrant in order to carry out covert surveillance. While law enforcement is itself a very substantial public interest, for the sake of clarity, covert surveillance for the purposes of law enforcement should be authorised under the proposed law enforcement system, rather than under the proposed "public interest" system.[6]

4. *In some cases, it will only be possible to obtain retrospective authorisation. This is discussed at para 5.93-5.94.*
5. *Surveillance in the public interest is considered in ch 6; surveillance in employment is considered in ch 7.*
6. *This system is outlined in ch 6.*

Recommendation 22

Law enforcement officers should be required to obtain a warrant in order to carry out covert surveillance. The provisions of the proposed Surveillance Act regulating covert surveillance by law enforcement officers should be based on Part 4 of the *Listening Devices Act 1984* (NSW).

LISTENING DEVICES ACT 1984 (NSW)

5.6 As noted above, the LDA prohibits covert surveillance unless it is carried out in accordance with that Act and has been authorised by warrant. Part 4 of the LDA contains the relevant provisions pertaining to warrants.

5.7 There is no restriction on who may apply for authorisation to use a listening device. In order to succeed on an application for a warrant, "a person" (the applicant) must satisfy an "eligible Judge" of the Supreme Court that there are reasonable grounds to believe that a "prescribed" offence has been, is about to be or is likely to be committed, and that the use of a listening device is necessary to investigate that offence, or obtain evidence of the offender or of the commission of the offence.[7] An "eligible Judge" is one whom the Attorney General has declared, with that judge's consent, to be eligible for the purposes of the LDA.[8] A "prescribed offence" is an indictable offence or is prescribed for the purposes of Part 4, whether indictable or not.[9]

5.8 Pursuant to section 16(2), in determining whether a warrant should be granted, the judge is to have regard to: the nature of the offence; the likely impact on privacy; alternative means of obtaining the evidence or information; the evidentiary value of the evidence;

7. *LDA s 16(1).*
8. *LDA s 3A. The regulations may provide that, in certain prescribed circumstances, the functions of an eligible judge may be exercised by an eligible judicial officer: s 16(7).*
9. *LDA s 15.*

and any previous warrant sought or granted in connection with the offence.

5.9 Section 16(3) provides that, in authorising the installation of a listening device on premises, the Court must authorise and require the retrieval of the listening device and authorise entry onto the premises for that purpose.

5.10 Section 16(4) prescribes that a warrant must specify a number of matters, in default of which the warrant will not be valid.[10] These matters are as follows:

- *the prescribed offence in respect of which the warrant is granted;*
- *where practicable, the name of any person whose private conversation may be recorded or listened to;*
- *the period during which the warrant is in force;*
- *the name of any person who may use the listening device, or who may use it on that person's behalf;*
- *where practicable, the premises on which the device is to be installed, or the place at which it is to be used;*
- *any conditions applying to entry onto premises or use of the listening device; and*
- *the time within which the surveillance user must report to an eligible judge and the Attorney General.*

5.11 An applicant for a warrant must also serve on the Attorney General notice of the particulars required by section 16(4), as well as particulars of: the type of listening device intended to be used; details of any previous warrant sought or granted; any other alternative means of obtaining the information or evidence; and the results of any attempt to use alternative means.[11] The Attorney

---

10. Haynes v Attorney General (NSW) (NSW, Supreme Court, No 012075/95, 9 February 1996, unreported).

11. LDA s 17(1).

General must have an opportunity of being heard in relation to the granting of the warrant.[12]

5.12 A warrant may be issued for a period not exceeding 21 days,[13] *but can be revoked before its expiry.*[14] *Further warrants can be granted in respect of the same offence.*[15]

5.13 Under section 18, in urgent situations, a member of the police force can apply for a warrant by telephone,[16] *providing the eligible judge is satisfied that "the immediate use of a listening device is necessary" and that it is not practicable to grant a warrant in the normal way pursuant to section 16.*[17] *A warrant granted under section 18 cannot be in force for longer than 24 hours.*[18] *In all other respects, the provisions of section 16 (2)-(6) apply to section 18 warrants.*[19]

5.14 A person to whom a warrant was granted, whether pursuant to section 16 or section 18, must satisfy the reporting requirements set out in section 19. Briefly, an eligible judge and the Attorney General must be given particulars in writing concerning the name, if known, of any person subjected to surveillance, the period during which, and the place at which, the device was used, or the premises on which it was installed, the use made of the surveillance material and particulars of any previous use of a listening device in respect of the subject offence.[20]

5.15 After reporting the results of surveillance conducted under warrant, an eligible judge may form the view that, having regard to the evidence or information obtained, or any other relevant matter, the use of the listening device was not justified and was an

---

12. LDA s 17(2).
13. LDA s 16(4)(c).
14. LDA s 16(5).
15. LDA s 16(6).
16. LDA s 18; application can also be by radio or any other communication device: s 18(1).
17. LDA s 18(2)(b), 18(3).
18. LDA s 18(8).
19. LDA s 18(8).
20. LDA s 19(1).

unnecessary interference with privacy. In that case, the eligible judge may make a direction that the subject of the surveillance be informed of the surveillance.[21]

THE PROPOSED SURVEILLANCE ACT

5.16 The Commission makes a number of recommendations below in relation to powers contained in the legislation and conduct authorised by a warrant. It needs to be emphasised that, while a power to make a certain order may be given to an eligible judge by the legislation, unless an order is expressly made and contained in the warrant, the Commission intends by its recommendations that no authorisations should be implied. Only that conduct which the warrant specifically authorises will be lawful.

Who may apply for a warrant

5.17 In Issues Paper 12 ("IP 12"), the Commission asked whether the definition of "applicant" should be amended so as to place restrictions on who may apply for a warrant to conduct covert surveillance.[22] *The Commission noted that allowing "a person" to apply for a warrant gave New South Wales the widest definition of "applicant" of any jurisdiction in Australia.*[23]

---

21. *LDA s 20.*
22. *New South Wales Law Reform Commission, Surveillance (Issues Paper 12, 1997), Issue 9.*
23. *NSWLRC IP 12, at para 5.7. In most jurisdictions outside New South Wales, including overseas, legislation regulating covert surveillance requires that an applicant for a warrant has to be a member of the police force, often above a certain rank. For instance, the Listening Devices Act 1972 (SA) s 6(2) provides for a member of the police force to obtain a warrant, but in Queensland, only a police officer ranked Inspector or above can apply for a warrant: Drugs Misuse Act 1986 (Qld) s 25. In some jurisdictions, the category of applicant is further restricted. For example, in Canada, only the Attorney General, the Solicitor General or a person designated by the Solicitor General may apply: Criminal Code 1985 (Can) s 185.*

5.18 In IP 12, the Commission was of the provisional view that the definition of "applicant" contained in the LDA should not be amended, particularly if regulation of covert surveillance was not limited to surveillance using a listening device. The Commission argued that retaining a wide definition of applicant removes the need to try and incorporate any number of persons/organisations who may seek to obtain such a warrant, and the problems that can arise if individuals/groups are excluded.[24]

5.19 The framework described above, in which three systems of authorisation would apply to the conduct of covert surveillance, was conceived after IP 12. Under this framework, only law enforcement officers would apply for a warrant to carry out law enforcement. The evaluation of whether "a person", meaning anyone at all, should be able to apply for authorisation to conduct covert surveillance no longer arises in this discussion, but arises in relation to the public interest and employment authorisation systems.[25]

5.20 The issue which arises here is who should come within the definition of "law enforcement officer" for the purposes of the proposed Surveillance Act. The Commission is of the view that "law enforcement officer" should not be narrowly construed and should include commonly regarded law enforcement agencies.

5.21 The NSW Police Special Services Group, in response to IP 12, submitted that warrants should be restricted to "qualified agencies" as defined by the Report of the Royal Commission into the New South Wales Police Service ("the Wood Report").[26] *Those agencies include the Australian Federal Police, State and Territory police, the Australian Security Intelligence Organisation,*

Only the Attorney General or the principal prosecuting attorney of a State or an area may apply in the United States: 18 United States Code (US) s 2516. In Germany, applications are limited to officials of the Department of Public Prosecutions: Strafprozessordnung (Criminal Procedure Code) (Germany).

24. *NSWLRC IP 12, at para 5.12.*
25. *See ch 6 and 7 respectively.*
26. *NSW Police Service, Special Services Group, Submission. See NSW, Royal Commission into the New South Wales Police Service, Final Report (May 1997) Volume 2 at 455.*

the Independent Commission Against Corruption, the National Crime Authority, the NSW Crime Commission, Royal Commissions and the Police Integrity Commission. The Commission agrees with this view. It should also include any office holder specifically empowered to enforce a particular law, such as pursuant to the Fisheries Act 1935 (NSW) or the Casino Control Act 1992 (NSW), unless those laws specifically exempt the operation of the proposed Surveillance Act.

Recommendation 23

"Law enforcement officer" should be defined in the proposed Surveillance Act to include 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 and the Police Integrity Commission. It should also include any office holder specifically empowered to enforce a particular law.

Offences for which a warrant may be sought

5.22 In IP 12, the Commission asked whether the existing categories of offences for which warrants can be obtained under the LDA needed revision or expansion and whether any specific offences (including non-indictable offences) should be prescribed.[27]

Submissions and response

5.23 Most submissions expressed the view that the existing offences for which LDA warrants could be sought were adequate and needed no amendment. Price Waterhouse considered the existing categories to be appropriate, suggesting that, in order to justify the invasion of privacy, any amendment would have to be in relation to serious offences only.[28] *Other submissions expressed the view that while*

27. NSWLRC IP 12, Issue 12.

28. Price Waterhouse, Submission at 8. See also Law Society of NSW,

there was no compelling argument for extending the categories of offences, some changes would nevertheless be useful. For example, the Director of Public Prosecutions ("DPP") suggested that there should be a presumptive weighting in favour of granting a warrant where child abuse is alleged.[29] *The Privacy Committee considered that warrants should be limited to serious offences, such as those with a maximum penalty of 7 years or greater.*[30] *The Public Defender submitted that he did not see any compelling argument to expand the existing categories of offences for which a listening device warrant can be obtained. Additionally, he expressed the view that "if the information obtained as a result of a warrant does not amount to proof of an offence falling within the categories which permit the warrant to be given, this should not prevent a prosecution". Likewise, in his view, the LDA should not prevent the use of information obtained about an offence not prescribed under the Act, if that information was obtained incidentally during the lawful use of the warrant in relation to a separate prescribed offence.*[31]

5.24 Some submissions supported a revision of the category of offences, but in divergent respects. The NSW Council for Civil Liberties was of the view that the categories of offences for which warrants may be sought should be narrowed and made more specific.[32] *On the other hand, the Australian Federation of Business and Professional Women considered that the categories should be expanded. The Federation submitted that women often live in fear of offences that might not fall within the scope of "imminent threat of serious violence", and a relaxation of some of the categories would better allow women to protect themselves and prosecute offenders by employing listening devices.*[33]

Submission at 3.

29. *Director of Public Prosecutions, Submission at 5.*
30. *Privacy Committee of NSW, Submission at 24.*
31. *M L Sides, Submission at 10-11. The use of information obtained as a result of surveillance is discussed in ch 9.*
32. NSW *Council for Civil Liberties Inc, Submission at 4.*
33. *The Australian Federation of Business and Professional Women Inc, Submission; NSW Council for Civil Liberties Inc, Submission at 5.*

5.25 ***Law enforcement agencies.*** *Several law enforcement agencies suggested to the Commission that they should be able to apply for a warrant to investigate any offence in the course of their duty. The NSW Police Service, Special Services Group argued that "it is impossible to specifically define now, or into the future, what offences may best be investigated by the employment of surveillance methodologies".[34] The police were of the view that "qualified agencies" should be able to apply for a warrant whenever necessary for the purposes of an authorised investigation, regardless of the offence which is being investigated. The NSW Crime Commission, the Independent Commission Against Corruption, the National Crime Authority and the Police Integrity Commission, in a joint submission, agreed.[35] The police submission also noted the special position of undercover operatives who may be investigating offences not covered under the LDA, or may be in the initial stages of an investigation where sufficient evidence to support a warrant application has not yet been gained. The police argued that it is often necessary to use a listening device to protect the safety of undercover officers in these situations, especially where they are in vehicles and cannot be observed by support personnel.*

Other jurisdictions

5.26 Most Acts in jurisdictions outside New South Wales authorising the use of a listening device allow an application for a warrant for a listening device to be made in respect of an "offence" without specifying particular offences to which the Acts will apply.[36] The most detailed provision specifying categories of offences for which a warrant may be sought is contained in the Telecommunications (Interception) Act 1979 (Cth) ("Interception

---

34. NSW Police Service, Special Services Group, Submission at 4.

35. NSW Crime Commission (NSWCC), Independent Commission Against Corruption (ICAC), Police Integrity Commission (PIC) and National Crime Authority (NCA) ("Joint Law Enforcement Agencies"), Submission.

36. See eg, Invasion of Privacy Act 1971 (Qld); Listening Devices Act 1972 (SA); Surveillance Devices Act 1998 (WA); Surveillance Devices Act 1999 (Vic); Surveillance Devices Act 2000 (NT).

Act").[37]

Conclusion

5.27 The Commission has concluded that the proposed Surveillance Act should neither limit the category of offences, nor attempt to prescribe specific offences, for which a warrant may be obtained. It is often not possible at the time an application is made to know whether the criminal activity under investigation will result in a prosecution for a summary offence or an indictable offence. The distinction between these categories has become increasingly blurred in some legislation.[38] *In addition, there are offences which are serious but not indictable. For example, common assault can be a serious offence, but is not an indictable one. The Commission sees merit in the arguments presented in the submission of the NSW Police Service, Special Services Group, referred to above.*

Recommendation 24

The proposed Surveillance Act should allow an application for a warrant to be made with respect to any offence.

37. *That Act categorises offences into two classes and identifies a variety of offences under each class: Telecommunications (Interception) Act 1979 (Cth) s 5 and 5D.*
38. *The Criminal Procedure Act 1986 (NSW) sets out a number of indictable offences which are to be dealt with summarily unless, in relation to some offences, the prosecuting authority or person charged elects otherwise or, in relation to other offences, the prosecuting authority alone elects otherwise: Schedule 1.*

Who should issue a warrant

5.28 In IP 12, the Commission asked whether the power to grant surveillance warrants should be limited to judges of the Supreme Court.[39]

Submissions and response

5.29 Most submissions addressing this issue considered that the power should be limited to judges of the Supreme Court on the basis that the importance of the decision to issue a warrant justifies restricting the power to judges of the highest authority.[40] *In advocating that the power to grant warrants be limited to Supreme Court judges, the Privacy Committee argued that, since the person who is the subject of the warrant application has no opportunity to defend him or herself against arbitrary privacy infringements, it is appropriate that the matter be considered by a superior court judge.*[41]

5.30 Two submissions expressed the view that the power to grant warrants should not be so limited. The NSW Council for Civil Liberties considered that the power could be extended to District Court judges provided they follow guidelines and report either to a Privacy Commissioner or a Privacy Ombudsman.[42] *The Insurance Council of Australia also indicated that it would not oppose an extension of the power to grant surveillance warrants.*[43]

5.31 A submission from a private investigation and security organisation was of the view that courts should not be involved in issuing warrants at all as this would preclude all but police from using the legislation.[44] *The submission argued that there should be*

---

39. NSWLRC IP 12, Issue 13.

40. Director of Public Prosecutions, Submission at 5; Price Waterhouse, Submission at 8; M L Sides, Submission at 11; NSW Police Service, Special Services Group, Submission at 13; NSW Young Lawyers Criminal Law Committee, Submission; Law Society of NSW, Submission at 3; Joint Law Enforcement Agencies, Submission.

41. Privacy Committee of NSW, Submission at 24.

42. NSW *Council for Civil Liberties Inc, Submission.*

43. Insurance Council of Australia, Submission at 4.

44. Barrington Group, Submission at 2.

a system of licences authorising the covert use of video equipment. According to this submission, to apply for a licence, an organisation should submit a resume of experience to a committee comprising various representatives, including the Privacy Committee. A licence to conduct surveillance should be issued subject to certain strict conditions and the applicant should have to submit to a probity check.

Other jurisdictions

5.32 There is precedent in other jurisdictions for vesting the power to issue warrants in office-holders other than judicial officers. In the United Kingdom, the Interception of Communications Act 1985 (UK) vests the power to issue interception warrants in the Secretary of State. At the Commonwealth level, the Interception Act was amended in 1997 to permit members of the Administrative Appeals Tribunal (AAT) nominated by the Attorney General to issue warrants authorising telephone interceptions.[45]

---

45. Telecommunications (Interception) Act 1979 (Cth) s 6DA inserted by Telecommunications (Interception) and Listening Device Amendment Act 1997 (Cth) s 19. This Act also makes consequent amendments to the Australian Federal Police Act 1979 (Cth) and the Customs Act 1901 (Cth) permitting nominated AAT members to issue listening device warrants in respect of those agencies. These amendments do not affect the provisions already in the Telecommunications (Interception) Act 1979 (Cth) allowing "eligible judges" to issue warrants. The 1997 amendments were partly in response to complaints to the Commonwealth Government by Federal Court judges that issuing warrants was time-consuming: see P Clark, "Judges say no to more phone taps" The Sunday Canberra Times (24 August 1997) at 3; B Lagan, "Judges back phone-tap changes" The Sydney Morning Herald (25 August 1997) at 5; K Hannon, "Phone-tap powers for non-judges" Herald Sun (22 October 1997) at 24.

During the debate of the 1997 amending Bill in the Commonwealth Parliament, the Opposition criticised the move to empower AAT members to issue warrants on the basis that it would jeopardise the integrity of the Telecommunications (Interception) Act 1979 (Cth): Australia, Parliamentary Debates (Hansard) Legislative Assembly, Wednesday 18 June 1997 at 5638-5643 and 5661-5662.

5.33 However, the relevant laws of the Australian States and Territories all provide for warrants to be issued by judicial officers. In the United States, each application for an order authorising or approving the interception of a wire, oral, or electronic communication has to be made in writing to a judge.[46] In Canada, an application for an authorisation to intercept a private communication must be made to a judge.[47] In New Zealand, an application may be made to a judge of the High Court for a warrant for any member of the Police to intercept a private communication by means of a listening device.[48]

Conclusion

5.34 The European Human Rights Commission observed that it is desirable that the power to authorise secret surveillance of suspects in criminal cases be limited to judges because "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust control to a judge".[49] The Commission agrees that the power to issue warrants should be limited to judicial officers. It is important that a decision to authorise such intrusive conduct as the carrying out of covert surveillance be made by an impartial authority, skilled in the appraisal of evidence and the likelihood of obtaining information or evidence by other means, and experienced in the weighing of the community interest to investigate and prosecute offences against the privacy interests of individuals. Judicial officers have the requisite forensic skills and experience, independence and integrity to determine when invasions of privacy are necessary and justified. As well, the respect which judicial officers command in the community would ensure public confidence in a system that vests control over

---

The Government argued that it was not constitutionally possible to force Federal Court judges to exercise administrative power and continue to issue warrants, so alternatives had to be found: Australia, Parliamentary Debates (Hansard) Legislative Assembly, Wednesday 18 June 1997 at 5658-5659.

46. *18 United States Code s 2518.*
47. *Criminal Code 1985 (Can) s 185.*
48. *Crimes Act 1961 (NZ) s 312B.*
49. *Klass v Federal Republic of Germany (1978) 2 EHRR 214 at 235.*

the issuing of warrants for covert surveillance in them. The Commission is, therefore, of the view that the proposed Surveillance Act should limit the power to issue warrants to Supreme and District Court judges and magistrates who have consented to be nominated as "eligible". It is envisaged that the source of "eligible judges" should primarily be judges of superior courts, with District Court judges and magistrates being nominated as "eligible" where the need to do so arises.

5.35 There are two reasons why the Commission is of the view that the power to issue warrants should not be confined to Supreme Court judges. First, it is theoretically possible that the number of Supreme Court judges who have consented to become "eligible" for the purposes of the Act may be insufficient at a particular point in time to decide all applications for warrants. Secondly, requiring an application before the Supreme Court by police officers in a country town may not always be practicable and could jeopardise a planned operation where time is of the essence. Therefore, while as a general rule the authority to issue warrants should be conferred on Supreme Court judges, the proposed Surveillance Act should contain provisions similar to section 3B and 16(7) of the LDA. These sections allow the Attorney General to nominate District Court judges and magistrates to exercise the functions of an "eligible judge". The Commission's recommendation below therefore preserves the existing power to draw not only on Supreme Court judges to be nominated as "eligible" to issue warrants, but on District Court judges and magistrates, should the need arise in particular circumstances.

Recommendation 25

The proposed Surveillance Act should empower the Attorney General to declare Supreme Court judges as "eligible judges" for the purpose of deciding applications for surveillance warrants. The proposed Surveillance Act should also authorise the Attorney General to nominate District Court judges and Magistrates as "eligible judicial officers" who may exercise the functions of an "eligible judge".

Grounds for determining whether a warrant may be granted

5.36 As set out in paragraph 5.8 above, section 16(2) of the LDA prescribes the matters to which the judge must have regard in determining whether a warrant should be granted. In connection with these matters, the High Court has held that in determining the admissibility of evidence obtained by the use of a listening device under the authority of a warrant, a court must determine merely whether the warrant was regularly granted by the eligible judge. It does not inquire into the sufficiency of the material which satisfied the eligible judge of the matters to which he or she must have regard.[50]

5.37 The parameters set out in section 16(2) afford important protection against the issuing of warrants in cases where it was not absolutely essential or appropriate. As well, they provide the judge with a useful check list and guidance in what will often be a difficult exercise of balancing competing claims of apparently equal merit. By the same token, the matters to which the judge must have regard do not impose unreasonable restrictions on the exercise of the judge's discretion. Subject to some reservations the Commission has with section 16(2)(c), the Commission recommends that these guidelines should be used in the proposed Surveillance Act.

5.38 Section 16(2)(c) of the LDA requires the judge to have regard to "alternative means of obtaining the evidence or information sought to be obtained". This suggests that the availability of investigative techniques other than the covert use of surveillance devices may be a ground for refusing an application for a warrant. It is important, however, that the wording be unambiguous in emphasising that law enforcement officers should only resort to covert use of surveillance devices if other investigative techniques are ineffective, inappropriate or unavailable. Covert surveillance should by no means be routinely employed as the initial step in a criminal investigation. The Commission recommends that the purpose of section 16(2)(c) be made unambiguous by more direct and explicit direction as to the matters to which the judge should have regard.

---

50. Murphy v The Queen (1989) 167 CLR 94.

Recommendation 26

In determining whether a warrant should be granted, the eligible judge should have regard to:

- **the nature of the offence in respect of which the warrant is sought;**
- **the extent to which the privacy of any person is likely to be affected;**
- **whether other investigative procedures have been tried but have failed; or other investigative procedures are unlikely to succeed or likely to be too dangerous to adopt in the particular case; or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative techniques;**
- **the evidentiary value of any evidence sought to be obtained; and**
- **any previous warrant sought or granted in connection with the same offence.**

What a warrant should authorise

5.39 It is imperative that a warrant permitting covert surveillance also authorise entry onto premises for the purposes of executing the warrant and installing and retrieving surveillance devices. The proposed legislation should therefore include a section similar to section 16(3) of the LDA. However, a number of issues arise in relation to the parameters of the authority given by a warrant, including:

- *whether there is a need to broaden the meaning of "premises";*[51]
- *whether the proposed legislation should enable an eligible judge to authorise the use of a surveillance device in any*

51. NSWLRC IP 12, Issue 18.

location in relation to a particular person or activity;

- *whether a warrant authorising the installation and retrieval of a surveillance device should state that such entry is not unlawful;*[52]
- *whether the proposed legislation should provide for authority to repair, test, maintain and move the surveillance device after it was installed; and*
- *whether a warrant should authorise the use of electricity to power a surveillance device.*

Defining "premises"

5.40 The current definition of premises in the LDA includes "vessels, vehicles and aircraft".[53] *It makes no provision for containers, which are often used in transporting stolen goods, importing illicit drugs and so forth. The Commission asked in IP 12, whether the definition should be amended to include containers as a type of "premises" which may be authorised by warrant for the installation of a listening device, so that any evidence obtained is not later deemed inadmissible.*[54]

5.41 All but one of the submissions which addressed this issue agreed with the Commission's suggestion that the definition of "premises" in the LDA in which surveillance devices can be located should include containers.[55] *Some submissions favoured a broader definition than the one proposed by the Commission. The NSW Police Special Services Group suggested that the definition of "premises" should also include objects such as suitcases, drums, packages, bags, and other similar equipment. The Police submission also argued that because surveillance devices can be used in so many different environments, it would be extremely*

52. *NSWLRC IP 12, Issue 17.*
53. *Section 15.*
54. *NSWLRC IP 12, Issue 18.*
55. *M L Sides, Submission at 13; Director of Public Prosecutions, Submission at 6; NSW Police Service, Special Services Group, Submission at 7; Price Waterhouse, Submission at 10; NSW Young Lawyers Criminal Law Committee, Submission; Joint Law Enforcement Agencies, Submission; Privacy Committee of NSW, Submission at 26.*

difficult to attempt to define each one. The submission suggested that, in addition to the current definition, the LDA should provide that "premises" includes "other things where a surveillance device may be attached".[56]

5.42 On the other hand, the Law Society of New South Wales expressed the view that the term "containers" is very broad and unclear, and that the need to expand the definition has not been demonstrated.[57]

5.43 The Commission considers that the proposed surveillance legislation should not attempt to define exhaustively the places where it may be possible and necessary to install a surveillance device. The definition of "premises" should be both broad and flexible. There appears to be no public policy reason why the current definition of "vessels, vehicles and aircraft" should not be extended to include any place, thing or object which the eligible judge determines to be appropriates.

Recommendation 27

"Premises" should be defined in the proposed Surveillance Act to include any object, thing or place where the eligible judge, in the exercise of his or her discretion, authorises a device to be installed.

56. *NSW Police Service, Special Services Group, Submission (29 July 1997) at 7.*
57. *Law Society of NSW, Submission at 4.*

Specifying the exact location of a surveillance device

5.44 The DPP and the Joint Law Enforcement Agencies' submission supported the recommendation in the Wood Report that the focus not be on the premises where the surveillance will take place, but on the target of the surveillance or the activity under investigation. They recommended that the warrant should authorise entry to any premises where the relevant person or thing is, or is likely to be.[58] *The Joint Law Enforcement Agencies' submission noted that it is sometimes necessary to enter another premises for the purpose of gaining access to the premises where the device is to be installed, for example, installing a device in a car may necessitate obtaining access to the garage where the car is kept. The submission also stated that sometimes, where data monitoring or tracking devices are concerned, it may be difficult to nominate the location where the device will be used, since the reason it is being used is to determine the location of the suspect person, activity or object.*

5.45 The Commission is of the view, however, that while the definition of premises in the legislation should be broadened, the warrant authorising covert surveillance should remain specific as to the location of the surveillance device. Covert surveillance is an intrusive investigative tool which should be tightly controlled. Enabling a warrant to authorise the use of a device anywhere in relation to a particular person or activity has the potential to affect the privacy of a number of people not connected with the offence under investigation. The Commission accepts that there may be occasions, such as those noted in the submission from the Joint Law Enforcement Agencies, where nominating the exact location of the device is not possible or entry to other premises may need to be gained. In these situations, the onus should be on the applicant to persuade the court that a warrant is still justified in the circumstances. The court would then have the discretion to grant, refuse, or impose conditions on, the warrant.

---

58. Such a provision is used in the Customs Act 1901 (Cth) s 219B(5).

Recommendation 28

The eligible judge should have the discretion to issue a warrant permitting surveillance of a particular person or thing without reference to specific premises if the applicant satisfies the eligible judge that such a warrant is justified in the particular circumstances, subject to any conditions which the eligible judge deems fit to impose.

Authority to enter premises where the device is to be installed and retrieved

5.46 In IP 12, the Commission raised the issue of whether a warrant authorising entry onto premises should state that such entry is not unlawful.[59] *The issue was raised because of the judgment in Coco v The Queen.*[60] *That case examined section 43(2)(c) of the Invasion of Privacy Act 1971 (Qld) which authorises the use of listening devices by police officers.*[61] *The High Court held that there was no clear expression in the legislation of an unmistakable and unambiguous intention to confer a power to authorise conduct that would otherwise amount to a trespass. The High Court concluded that if the statute did not explicitly or implicitly legalise a trespass for the purpose of installing a listening device, then there could be no power in a judge to authorise such an illegality.*

---

59. NSWLRC IP 12, Issue 17.

60. Coco v The Queen (1994) 179 CLR 435.

61. Section 43(1) of that Act makes it an offence to use "a listening device to overhear, record, monitor or listen to a private conversation". Section 43(2)(c) provides that s 43(1) shall not apply: to or in relation to the use of any listening device by – (1) a member of the police force acting in the performance of his duty if he has been authorised in writing to use a listening device by – (a) the Commissioner of Police; (b) an assistant Commissioner of Police; or an officer of Police of or above the rank of Inspector who has been appointed in writing by the Commissioner to authorise the use of listening devices, under and in accordance with an approval in writing given by a judge of the Supreme Court in relation to any particular matter specified in the approval.

5.47 However, the Commission is of the view that the way in which section 16(3) of the LDA is formulated expressly authorises the warrant-holder to enter onto premises, in order to install or retrieve a surveillance device, in such a way as would otherwise amount to a trespass. This provision constitutes clear expression of an unmistakable and unambiguous intention to abrogate the fundamental right of a person to exclude others from his or her property to enable another person to install or retrieve a listening device in or on such property. There appears to be no need to clarify such express authorisation further.

Recommendation 29

The proposed Surveillance Act should contain a provision similar to section 16(3) of the LDA, expressly authorising entry by the warrant-holder onto authorised premises for the purpose of installation and retrieval of the surveillance device, notwithstanding that such entry might otherwise be unlawful.

Entry to other premises

5.48 Related to the issue of authority for lawful entry to the premises where the device is to be installed and retrieved are the issues of access to other premises and the use of force to effect entry. If the definition of "premises" is broadened as recommended, "premises" for the purpose of a surveillance warrant may include personal property. Authority to enter such property, for example a motor vehicle, does not include authority to enter the place where, for example, the motor vehicle is located. The Commission is of the view that access to the place where moveable property is located must also be given by the legislation to allow the warrant-holder to install and retrieve the surveillance device.

Recommendation 30

An eligible judge should have the power to authorise the warrant-holder to enter upon any other premises as may be necessary for the purpose of gaining access to the premises where the surveillance device is to be installed and retrieved, notwithstanding that such entry might otherwise be unlawful.

Authority to enter premises to repair, test, move, maintain and replace the device

5.49 The LDA only authorises entry onto premises for the purpose of installing and retrieving the device.[62] *There is no specific provision authorising entry for the purpose of testing, repairing, maintaining, moving or replacing the device, even though this may on occasion be necessary. The Commission suggested in IP 12, that such powers should become automatic on issuing the warrant, as they may be an integral part of the success or otherwise of an operation.*[63] *The Commission sought submissions on whether the legislation should specifically provide for entry to premises for these ancillary purposes.*[64]

5.50 ***Submissions and response.*** *The NSW Police Special Services Group noted that the devices often break down, necessitating entry onto the premises to carry out repairs.*[65] *This was also noted in the Wood Report.*[66] *Most of the submissions which commented on this issue agreed.*[67] *However, the NSW*

62. *LDA s 16(3).*
63. *NSWLRC IP12, para 5.50.*
64. *NSWLRC IP12 Issue 24.*
65. *NSW Police Service, Special Services Group Submission at 12.*
66. *Wood Report, Vol II at 455.*
67. *M L Sides, Submission at 17; Director of Public Prosecutions, Submission at 8; NSW Police Service, Special Services Group, Submission at 12; Price Waterhouse, Submission at 13; NSW Council for Civil Liberties Inc, Submission at 5; NSW Young Lawyers Criminal Law Committee, Submission; Joint Law Enforcement Agencies, Submission.*

Council for Civil Liberties argued that any entry onto premises for any purpose should be conditional on specific and separate prior judicial authorisation. The Privacy Committee also stated that should entry for such purposes be necessary, it should be the subject of a separate warrant. It submitted that if the power to enter premises to test and maintain the device was ancillary to the warrant permitting installation and retrieval, the applicant "could freely enter the premises any number of times during the period of the warrant". This, in the Privacy Committee's view, is a significant invasion of privacy and one that needs to be considered specifically by a court on a case-by-case basis.[68] *On the other hand, the Law Society of New South Wales suggested that if the legislation provides for such powers, it should also provide for record keeping of the number and detail of entries to premises, and subsequent disclosure to the householder.*[69]

5.51 **Conclusion.** *It is reasonable to expect that surveillance devices will, from time to time, need to be tested and maintained and it is even likely that they will, from time to time, break down. If the devices cannot be maintained, tested, moved or repaired, the entire surveillance operation could be undermined. There is some inconsistency in the legislation allowing entry to premises in order to install a surveillance device, notwithstanding the invasion of privacy that may occur, but not allowing subsequent entry for the purposes of maintaining or repairing a device. Powers of entry to move, repair, maintain or replace a surveillance device sensibly follow from the power to enter to install and retrieve the device. Such authorisation can be granted in other jurisdictions.*[70]

5.52 The Commission has concluded that it is essential that entry onto premises for these ancillary purposes be authorised. The proposed Surveillance Act should provide that warrants may authorise powers of entry for such purposes. If the applicant for a warrant envisages that powers of entry to move, maintain, test or

---

68. Privacy Committee of NSW, Submission at 27-28.

69. Law Society of NSW, Submission at 6.

70. For example, see Surveillance Devices Act 2000 (NT) s 12(2); Drugs Misuse Act 1986 (Qld) s 18 and 27; and Customs Act 1901 (Cth) s 219B(7).

repair the device may be necessary, and the eligible judge is satisfied to that extent, the warrant should specifically authorise such powers. This is important given the court's inability to imply powers into a warrant that are not clear on the face of the document.

Recommendation 31

An eligible judge should have the power to authorise entry to the relevant premises to enable the warrant-holder to repair, test, maintain, move and replace the surveillance device after it was installed, nothwithstanding that such entry might otherwise be unlawful.

Recommendation 32

If the warrant-holder exercises an authority given under the warrant to move a device to premises not specified in the warrant, the warrant-holder must report the move to the eligible judge as soon as reasonably practicable.

The use of reasonable force in the entry to premises

5.53 Circumstances may arise when the use of force may be necessary to gain entry to premises to install the surveillance device, or carry out other authorised functions. An express authority to use reasonable force in the execution of the warrant would protect the warrant-holder from criminal or civil liability for any damage done. A provision giving such authority is contained in a number of Commonwealth and State statutes.[71]

71. *Surveillance Devices Act 1998 (WA) s 20(e)-(g) and 22(2): "[T]he court may by the warrant authorise the entry, by force if necessary, into or onto specified premises …"; Search Warrants Act 1985 (NSW) s 17; Independent Commission Against Corruption Act 1988 (NSW) s 43; Crimes Act 1914 (Cth) s 3G; Customs Act 1901 (Cth)*

5.54 The Commission recommends that the warrant-holder be authorised to use an amount of force that is reasonable under the circumstances to effect entry onto the premises, or into a vehicle, container or other thing or place where a device is to be installed. This authority should be available not only during the initial entry to install but also in subsequent entries to the premises to repair, test, move, maintain or retrieve the surveillance device.

5.55 Some legislation authorising the use of force in the execution of a search warrant impliedly or expressly authorise the use of force against persons, not just against things.[72] *The use of force against persons in the execution of a search warrant may be necessary in certain circumstances when the occupant of the premises to be searched offers resistance to the search. However, covert surveillance operations are, by definition, conducted without the subject's knowledge. Therefore, it is both unnecessary and illogical to authorise the use of force against the person who is to be the subject of the surveillance.*

---

s 203J; Family Law Act 1975 (Cth) s 122A; Road Transport Reform (Dangerous Goods) Act 1995 (Cth) s 26; Proceeds of Crime Act 1987 (Cth) s 36 and 71; Mutual Assistance in Criminal Matters Act 1987 (Cth) s 38J; International War Crimes Tribunals Act 1995 (Cth) s 54; Health Insurance Commission Act 1973 (Cth) s 8ZC; Extradition Act 1988 (Cth) s 31; Defence Force Discipline Act 1982 (Cth) s 101X; Chemical Weapons Act 1994 (Cth) s 76; Air Navigation Act 1920 (Cth) s 19CN; Aboriginal and Torres Strait Islander Heritage Protection Act 1984 (Cth) s 21S; Bounty (Fuel Ethanol) Act 1994 (Cth) s 42; Migration Act 1958 (Cth) s 252.

72. *For example, the Crimes Act 1914 (Cth) s 3G provides that in executing a warrant, "the executing officer, or a person who is a constable and who is assisting in executing the warrant may use force against persons and things [while] a person who is not a constable and who has been authorised to assist in executing the warrant may use such force [only] against things, as is necessary and reasonable in the circumstances".*

Recommendation 33

The eligible judge should have the power to authorise the warrant-holder to employ all reasonable means, not including force against a person, necessary in order to gain entry to premises where the surveillance devices are to be installed, retrieved, repaired, tested, moved, maintained or replaced, as well as other premises where the warrant-holder has been authorised to enter for those purposes, whether or not the means employed would otherwise amount to damage or trespass to property.

Use of electricity to power the device

5.56 In IP 12, the Commission suggested that the authorised use of a surveillance device should also include the use of electricity connected to the premises to power the device.[73] *This was recommended by the Wood Report.*[74] *All submissions on this point agreed with the Commission's suggestion.*[75] *The Privacy Committee submitted that the court should have the authority to approve the use of electricity to power the device, after considering the amount of power involved and any potential damage to property that may occur, and should be able to order the applicant to refund any costs if necessary.*[76]

5.57 Authorising the use of electricity connected to the premises would remove any argument at a later date that the device had been used unlawfully and avoid any suggestion of theft of electricity.[77] *Other forms of power, for example batteries, present the real*

73. *NSWLRC IP 12, para 5.52, Issue 26.*
74. *Wood Report, Vol II at 456.*
75. *M L Sides, Submission at 17; Director of Public Prosecutions, Submission at 8; NSW Police Service, Special Services Group, Submission at 13; Price Waterhouse, Submission at 13; NSW Young Lawyers Criminal Law Committee, Submission; Joint Law Enforcement Agencies, Submission.*
76. *Privacy Committee of NSW, Submission at 28.*
77. *See Electricity Act 1945 (NSW) s 30.*

possibility of not being able effectively to conceal the device or of losing power prior to the expiration of the warrant. The Commission is therefore of the view that, because of the desirability of removing doubt about the lawfulness of the surveillance, and to protect the warrant-holder from civil or criminal liability for the use of electricity, a warrant-holder should be authorised to use electricity connected to the premises to power the surveillance device.

Recommendation 34

The proposed Surveillance Act should empower the eligible judge to authorise the use of electricity connected to the premises to power the surveillance device.

Naming the persons who may use the device

5.58 Section 16(4)(d) of the LDA requires a warrant to specify the name of any person who may use a listening device pursuant to the warrant and the persons who may use the device on behalf of that person.[78] This requirement fails to address situations where:

- *it is necessary to substitute or use extra personnel (currently a new warrant has to be obtained); or*
- *an interpreter is needed to use the device to listen to the conversation and translate, unless this need was foreseen when the warrant was originally obtained.*

5.59 In IP 12, the Commission asked whether legislation should remove the requirement that the warrant name each person involved with the execution of the warrant, or alternatively, whether the warrant should confer the power on an authorised person to

78. Section 20A of the LDA allows the court to grant a warrant that refers to a person by an assumed name or code-name, if the court is satisfied that it is necessary to do so to protect the safety of the person.

delegate that power to others.[79]

Submissions and response

5.60 The views expressed in submissions were divided on this question. Some submissions considered that all people involved in covert surveillance operations should be named in the warrant to guard against abuse and to promote accountability.[80] *The NSW Young Lawyers Criminal Law Committee noted that section 20A of the LDA protects undercover police officers by allowing warrants to be issued to a person in an assumed or code-name if the court considers that to be necessary to protect the safety of that person.*[81] *The Registered Clubs Association considered that specific people should be authorised to carry out surveillance. Those people should be appropriately trained and licensed, undergo security checks and meet high professional and ethical standards.*[82]

5.61 Other submissions were of the view that the requirement should be removed from the legislation. The DPP considered the requirement to be unnecessary and inflexible.[83] *The NSW Police Special Services Group stated that the requirement meant that a warrant may have up to thirty names so as to cover all possible contingencies.*[84] *A number of submissions stated that the preferable option was to follow the Search Warrants Act 1985 (NSW) and nominate a particular person to execute the warrant "with such assistance as he/she considers necessary".*[85] *The Joint Law Enforcement Agencies' submission noted that this approach would allow for officers of the relevant agency, as well as locksmiths, telephone technicians and others to assist in installing and*

---

79. NSWLRC IP 12, Issue 19.

80. M L Sides, Submission at 14; NSW *Council for Civil Liberties Inc, Submission at 4; NSW Young Lawyers Criminal Law Committee, Submission.*

81. NSW Young Lawyers Criminal Law Committee, Submission.

82. Registered Clubs Association of NSW, Submission at 5.

83. Director of Public Prosecutions, Submission at 7.

84. NSW Police Service, Special Services Group, Submission at 8.

85. Director of Public Prosecutions, Submission at 7; See also NSW Police Service, Special Services Group, Submission at 8; Price Waterhouse, Submission at 10; Joint Law Enforcement Agencies, Submission.

monitoring a device. The Privacy Committee was of the view that delegation should be allowed, provided the names of the other people who exercised the warrant are provided to the court within a reasonable time (10 days is suggested) after the date of the surveillance.[86] *The Public Defender also thought that delegation should be allowed, but that the names of the people to whom the power is delegated should be included in the warrant at a later date.*[87] *The Law Society of New South Wales was of the view that the current legislation is unnecessarily cumbersome and does little to advance privacy interests. It suggested that the officer in charge should be named in the warrant, along with other relevant officers, and should be made responsible for any illegal conduct that occurs during the execution of the warrant.*[88]

Other legislation

5.62 Other Acts regulating similar areas are not as stringent as section 16(4)(d) of the LDA. For example, the Search Warrants Act 1985 (NSW) allows a person to execute a search warrant with the aid of such assistance as that person considers necessary.[89] *A warrant issued pursuant to the Australian Security Intelligence Organisation Act 1979 (Cth) authorises "the Organisation", including its officers, employees or agents, to use a listening device.*[90] *Under the Customs Act 1901 (Cth), the warrant confers authority on the chief officer of the Commonwealth law enforcement agency concerned or other officials of the agency appointed by the chief officer.*[91] *As well, the Wood Report recommended that the LDA be amended to provide that only the principal investigator need be named in the warrant and to empower the warrant-holder to seek whatever assistance is necessary.*[92]

Conclusion

5.63 It is not always possible at the time the warrant is sought to positively identify the persons who will be available to install and

---

86. Privacy Committee of NSW, Submission at 26.
87. M L Sides, Submission at 14.
88. Law Society of NSW, Submission at 4.
89. Search Warrants Act 1985 (NSW) s 18.
90. Australian Security Intelligence Organisation Act 1979 (Cth) s 26.
91. Customs Act 1901 (Cth) s 219D.
92. Wood Report, Vol II at 454-5.

monitor a listening device at the relevant time. The Commission is aware that operational requirements of warrant applicants, especially law enforcement agencies, may, and frequently do, change at short notice requiring available officers to undertake other duties. Other factors, such as court commitments of law enforcement officers and sick and recreational leave, also affect the deployment of personnel.

5.64 The Commission recommends that the person primarily responsible for the execution of the surveillance warrant should be named on the warrant before it is issued. Where the identity of people conducting surveillance needs to be protected for safety reasons, assumed or code-names should be able to be used. In situations where it is not possible to foresee the type of assistance that may be needed to execute the warrant effectively, the Commission considers that the surveillance legislation should empower an eligible judge to authorise the warrant-holder to delegate to others the authority conferred by the warrant. As an accountability measure, the Commission agrees with the suggestion of the Privacy Committee that the names of all people involved in the surveillance operation should be provided to the eligible judge as soon as reasonably practicable after the completion of the surveillance.

Recommendation 35

The person primarily responsible for the execution of the warrant should be named in the warrant. The eligible judge should have the power to authorise that person to seek whatever assistance is necessary to execute the warrant.

Recommendation 36

The proposed Surveillance Act should contain a provision similar to section 20A(1) of the LDA permitting the use of assumed names or code names in a warrant.

Recommendation 37

The names of all persons who were involved in executing the warrant should be provided to the eligible judge as soon as reasonably practicable after the completion of the surveillance.

Term of the warrant

5.65 In IP 12, the Commission sought submissions on whether the period for which the warrant can be in force should be extended beyond the 21-day period currently permitted by the LDA.[93]

Submissions and response

5.66 Most submissions on this point were of the view that the warrant period should be extended beyond 21 days.[94] *The Registered Clubs Association noted that the Working Party on Video Surveillance in the Workplace suggested that a warrant for covert video surveillance in the workplace operate for a maximum of 30 days. The Association considered that video surveillance would rarely extend beyond 30 days due to the prohibitive costs.*[95] *In line with this submission, the Public Defender considered that the*

93. *NSWLRC IP 12, Issue 20.*
94. *M L Sides, Submission at 14; Director of Public Prosecutions, Submission; Registered Clubs Association of NSW, Submission at 6; NSW Police Service, Special Services Group, Submission at 8; Price Waterhouse, Submission at 10; NSW Young Lawyers Criminal Law Committee, Submission; Joint Law Enforcement Agencies, Submission.*
95. *Registered Clubs Association of NSW, Submission at 6.*

maximum life of a warrant should be about one month, with the power to apply for an extension of up to 60 days with a supporting affidavit.[96] Other submissions endorsed the recommendation in the Wood Report of a 90 day maximum[97] to address the problems that occur due to operational delays which exist or arise and which are beyond the control of the law enforcement agency.[98] The majority of submissions were of the view that an extension of the warrant period should be judicially approved.[99]

5.67 Contrary views were expressed by the Privacy Committee[100] and the Law Society of New South Wales[101] who considered that 21 days was sufficient time. The Privacy Committee argued that longer time periods may involve "fishing expeditions", and that requiring a fresh warrant means that serious intrusions into privacy must be continuously justified and scrutinised by the court.

Other legislation

5.68 The Northern Territory legislation allows a warrant to be in force for 21 days.[102] Tasmanian legislation allows 60 days;[103] Western Australian, Victorian and South Australian legislation allow 90 days;[104] while Queensland legislation has no statutory maximum. At a Commonwealth level, the Australian Security Intelligence Organisation Act 1979 (Cth)[105] and the Customs Act 1901 (Cth)[106] permit a warrant for a listening device to remain in

---

96. M L Sides, Submission at 14.
97. Wood Report, Vol II at 454.
98. NSW Police Service, Special Services Group, Submission at 8; Joint Law Enforcement Agencies, Submission.
99. M L Sides, Submission at 14; Price Waterhouse, Submission at 10; NSW Council for Civil Liberties Inc, Submission at 4; NSW Young Lawyers Criminal Law Committee, Submission.
100. Privacy Committee of NSW, Submission at 26.
101. Law Society of NSW, Submission at 4.
102. Surveillance Devices Act 2000 (NT) s 13(2).
103. Listening Devices Act 1991 (Tas) s 17(4)(c).
104. Surveillance Devices Act 1998 (WA) s 13(8)(f); Surveillance Devices Act 1999 (Vic) s 17(3)(c); Listening Devices Act 1972 (SA) s 6(7)(c).
105. Australian Security Intelligence Organisation Act 1979 (Cth) s 26(6).
106. Customs Act 1901 (Cth) s 219B(10).

force for 6 months. The Interception Act has a 90 day limit.[107]

Conclusion

5.69 Applying a time limit on the period during which a warrant is in force ensures that the surveillance is carried out within the shortest time possible to prevent any more intrusion on an individual's privacy than is necessary under the circumstances. However, this safeguard has to allow a realistic time frame for the installation and removal of the surveillance device, and for the actual surveillance to take place effectively.

5.70 In many cases, 21 days will be insufficient to effect covert entry, installation of devices, the carrying out of the surveillance to achieve the purpose for which the warrant was issued, and removal of equipment. This is particularly so if there are unforeseen circumstances. The NSW Police Service pointed out in their submission that entry and installation may be delayed if the premises are occupied and the officers involved in the operation have to wait until an appropriate time to covertly install the device.

5.71 To make allowance for such possible procedural delays in complying with the provisions contained in the warrant as soon as it is issued, the Commission recommends that the maximum term of the warrant be extended to 30 days. This extension strikes a reasonable balance between an unrealistically short time-frame on the one hand and unnecessary invasions of privacy on the other. A term longer than this, for example 90 days as recommended by the Wood Report,[108] *weakens the high degree of accountability which covert surveillance requires and which a shorter time frame secures. It also encroaches on justifiable levels of intrusion into the privacy of individuals. A provision allowing the eligible judge to issue further warrants in respect of the same operation would address any need for further time to achieve the object of the surveillance activity. As in the LDA, the proposed Surveillance Act should provide that further warrants, each not exceeding a period of 30*

---

107. Telecommunications (Interception) Act 1979 (Cth) s 49(3).

108. Wood Report, Vol II at 454. See also National Crime Authority, Listening Devices: Aspects of Legislation in Australian States and Territories (Law Reform Discussion Paper 1, 1994) at para 9.1-9.3.

days, would require a fresh application. This will enable the eligible judge to scrutinise whether the extension of the surveillance is appropriate in the circumstances.

Recommendation 38

The period for which a warrant can be in force should be 30 days. Further warrants, each for a maximum period of 30 days, should be able to be applied for in respect of the same offence upon lodgement of a new application.

Contents of the warrant and the application for a warrant

The warrant

5.72 As noted at paragraph 5.10 above, section 16(4) of the LDA prescribes that a warrant must specify a number of matters, in default of which the warrant will not be valid.[109] *Warrants cannot be amended by the Court. Any error in a warrant cannot be amended by the "slip rule",*[110] *nor by the Court's inherent powers, because the warrant is not granted in "proceedings" and is not an order or judgement.*[111]

---

109. For example, a warrant which "authorise[d] the maintenance and retrieval of the listening device" was declared to be void because it did not authorise and require the retrieval of the listening device as provided for in the LDA s 16(3)(a): Bayeh v Taylor (NSW, Supreme Court, No 13497/97, Grove J, 4 February 1998, unreported). In that case, the court held that "authority inheres no obligation to act and a person authorised may or may not choose so to do. By the warrant, there must be no choice, there must be a requirement to retrieve the device": at 18. See K McClymont, "Bayeh warrants were invalid, court rules" Sydney Morning Herald (5 February 1998); S Balogh, "Surveillance judgment compromises police" The Australian (5 February 1998).

110. See Supreme Court Rules 1970 (NSW) Pt 20 r 1 and 10.

111. Haynes v Attorney General (NSW) (NSW, Supreme Court, No 012075/95, 9 February 1996, unreported). In that case, two

5.73 The Commission is of the view that the proposed legislation should specify what the warrant should contain and that these requirements should, like those in the LDA, be mandatory. It is essential that in granting a power of a highly intrusive nature, the scope and limits of that power are specified and that the requirements operate not merely as guidelines. The warrant should specify the nature of the authority to use the surveillance devices, who may use them, for what purpose they are to be used and the circumstances and conditions under which they may be used. The following two recommendations as to what should be specified in the warrant reflect recommendations made elsewhere in this chapter.

Recommendation 39

The warrant should specify:

(a) the offence in respect of which the warrant is granted;

(b) where practicable, the name of any person who is to be the subject of surveillance;

(c) the period (being a period not exceeding 30 days) during which the warrant is in force;

(d) the name of the person primarily responsible for the execution of the warrant;

(e) the premises on which the surveillance device(s) are to be installed or used, except in cases where the eligible judge has determined that it is justified not to specify the premises;

(f) the type(s) of surveillance device(s) to be used;

warrants were issued without the name of the person authorised to use the listening device. The Supreme Court held that the requirement in the LDA s 16(4)(d) that a warrant granted under the LDA shall specify the name of the person who may use a listening device pursuant to the warrant is mandatory and the failure to observe the requirement was fatal to the validity of the warrants. See also Bayeh v Taylor.

(g) any conditions subject to which the premises may be entered, or the surveillance device(s) may be used pursuant to the warrant;

(h) any conditions subject to which any information obtained as a result of the surveillance may be used, released or published; and

(i) the time within which the person authorised to use the surveillance device(s) pursuant to the warrant is required to report to the eligible judge and the Attorney General.

Recommendation 40

Where a warrant authorises the installation of one or more surveillance devices, the eligible judge should have the power to authorise:

(a) the retrieval of the surveillance device;

(b) the repair, testing, movement, maintenance and/or replacement of the surveillance device;

(c) entry onto the premises where the surveillance device is installed, and onto other premises, for the purpose of installation, retrieval, repair, testing, movement and/or replacement of the surveillance device;

(d) the person executing the warrant to employ such means as is necessary and reasonable for the purpose of executing the warrant, not including force against a person;

(e) the warrant-holder to seek whatever assistance is necessary to execute the warrant; and

(f) the use of electricity to power the surveillance device(s).

The eligible judge should also have the power to order retrieval of a surveillance device.

The application for a warrant

5.74 At present, warrant applications are generally in writing, accompanied by an affidavit, although no affidavit is specifically required by the LDA. In IP 12, the Commission suggested that it may be prudent for the form of the affidavit supporting a warrant application to be contained in legislation to ensure a minimum uniformity of application and to provide an understanding of what is required.[112] The Commission sought submissions on this issue.[113]

5.75 ***Submissions and response.*** *Opinion on this issue was divided. Some submissions stated that the form of an affidavit should not be included in surveillance legislation, as it would be too difficult.[114] The NSW Police Special Services Group stated that Supreme Court judges have never requested any further information in support of a warrant application, and so specifying the form of an application in legislation would be unnecessary.[115] The DPP argued that, just as the Interception Act does not specify the exact form of the affidavit required in support of an application for a warrant, neither should the proposed Surveillance Act.[116] The Joint Law Enforcement Agencies were of the view that the form of an affidavit should remain a matter for which individual judges must be satisfied in the circumstances of each case, but a form of*

112. NSWLRC IP 12, at para 5.23.
113. Issue 14.
114. Registered Clubs Association of NSW, Submission at 4; Joint Law Enforcement Agencies, Submission.
115. NSW Police Service, Special Services Group, Submission at 5.
116. Director of Public Prosecutions, Submission at 5.

warrant should be prescribed in the legislation to reduce the risk of technical defects.[117]

5.76 Other submissions considered that legislation should set out the minimum information required in a warrant application.[118] *Price Waterhouse suggested that legislation should contain the same requirements as the Interception Act to promote consistency in warrant applications. The New South Wales Young Lawyers Criminal Law Committee and the Law Society of New South Wales were also of the view that the LDA should mirror the Interception Act, and that applicants should have to detail reasonable grounds for seeking a warrant.*[119]

5.77 **Conclusion.** *Given the court's inability to amend a faulty or insufficient warrant, applicants for a warrant must ensure that sufficient information is provided to fulfil the legislative requirements and that the powers they wish to be authorised by the warrant are expressed in accurate and unequivocal terms.*[120] *The application must contain sufficient information to enable a judge to decide whether or not the granting of the warrant is justified in the circumstances. Given the importance of this decision, and the intrusive powers authorised by a surveillance warrant, the Commission is of the view that the legislation should specify essential information which the applicant for a warrant must furnish to the court. This will also ensure consistency in the standards applied to the determination of applications.*

5.78 The Commission considers that the application for a warrant should generally be in writing and accompanied by an affidavit containing information prescribed by the legislation. In urgent situations, an application may be made by telephone or radio,

---

117. Joint Law Enforcement Agencies, Submission.

118. M L Sides, Submission at 11; Price Waterhouse, Submission at 9; NSW Young Lawyers Criminal Law Committee, Submission; Privacy Committee of NSW, Submission at 25; Law Society of NSW, Submission at 3.

119. NSW Young Lawyers Criminal Law Committee, Submission; Law Society of NSW, Submission at 3.

120. See Coco v The Queen (1994) 179 CLR 47.

in which case, the applicant should also furnish the judge, either orally or in writing as the judge may direct, all the information which a written application is required to contain. Finally, in all applications for a warrant, the court should have the discretion to require information in addition to that which is prescribed by the legislation.

Recommendation 41

Except where the proposed Surveillance Act allows an application to be made by telephone or radio, applications for a covert surveillance warrant should be in writing supported by an affidavit attesting to the following:

- **the name of the person or organisation requesting the warrant and the name of any person acting, or making an application, on behalf of an organisation;**
- **the names of all persons who will be involved in the execution of the warrant, or their codenames and the reasons for the use of codenames, and whether the assistance of other persons in the execution of the warrant is likely to be required;**
- **if known, the identity of the person who will be the subject of the surveillance;**
- **a general description of all surveillance devices intended to be used;**
- **where the surveillance device will be installed and used, or, if it is not possible to nominate an exact location, why this is so;**
- **the length of time (not exceeding 30 days) for which the applicant seeks that the warrant be in force;**
- **details of any previous warrants sought or granted in connection with the same offence; and**
- **evidence in support of the matters to which the legislation requires that the eligible judge, in determining the application, shall have regard.**

Recommendation 42

In the case of applications made by telephone or radio, the applicant should furnish the eligible judge, either orally or in writing as the eligible judge may direct, all the information which a written application is required to contain.

Recommendation 43

The eligible judge should have the discretion to require information in addition to that which is prescribed by the legislation, if it is deemed necessary to determining the application.

Single warrant to authorise the use of more than one device

5.79 The provisions of the LDA regulating warrants refer to "a listening device"[121] or "the listening device".[122] These references to a single device may be interpreted to mean that a warrant may authorise the use of only one device. The Wood Report recommended that the LDA be amended to clarify that more than one listening device may used under the authority of a single warrant, provided that the warrant specifies all the devices intended to be used.[123] While use of the singular form of the term "listening device" in the LDA includes the plural,[124] it nevertheless raises the is-sue of

121. LDA s 16(3).
122. LDA s 16(1), 16(6B) and 16A.
123. Wood Report, Vol II at 455.
124. Interpretation Act 1987 (NSW) s 8(b) and 5: a reference to a word or expression in the singular form includes a reference to the word or expression in the plural form except in so far as there is a contrary legislative intention. See also Blue Metal Industries Ltd v Dilley (1969) 117 CLR 651; Re St George District Builders and Consultants Pty Ltd and the Company Act 1961[1963] NSWR 1265;

whether a surveillance warrant under the proposed Surveillance Act should authorise the use of more than one surveillance device.

5.80 With the range of surveillance devices now available, it is conceivable that law enforcement officers may want to employ different devices during the one operation. Although the privacy considerations for the use of one device may be different from those of another, and factors relating to the way in which a device is used differ from each other, these issues are best dealt with in one application, rather than making each device the subject of separate applications, for a number of reasons.

5.81 First, requiring a separate warrant application for each device to be used in the same operation creates unnecessary administrative costs for the person who has to lodge the application, the eligible judge who must decide the application and the Attorney General who must monitor the implementation of the legislation. Secondly, because a device can be a combination of several devices, a technical argument could arise as to whether an integrated device containing a number of components is a single device or whether separate applications should be made for each component. For example, should the use of a video camera with recording capability be authorised by a single warrant but the use of a video camera with a separate recording device be authorised by two warrants? Attempting to draw such distinctions could give rise to absurd, or at least inconsistent, results. Thirdly, a single application enables the eligible judge to assess the proposed surveillance operation in its entirety, including the different devices proposed to be used and the conditions under which each is to be used.

Taylor v McNamara [1974] 1 NSWLR 164; R v Dickens [1983] 1 NSWLR 403; Baxter v Chief Commissioner of Pay-Roll Tax (1986) 7 NSWLR 122; Public Service Association (NSW) v Public Service Board (NSW) (1986) 14 IR 414; Re Transport Industry (General Carriers) Contract Determination – Appeal by Transport Workers Union of Australia, NSW Branch (1993) 46 IR 154.

5.82 Aside from these practical considerations, focusing on the device in the warrant application, rather than on the surveillance operation as a whole, is contrary to the focus of the proposed Surveillance Act. The proposed legislation is not device-specific in its coverage and definitions. Its focus is emphatically on the activity of surveillance itself.

5.83 The Commission therefore recommends that the use of more than one surveillance device to investigate a particular offence, or in one particular law enforcement operation, should be authorised under a single warrant, provided that the warrant specify all devices to be used.

Recommendation 44

The proposed Surveillance Act should permit one warrant to be issued authorising the use of more than one surveillance device, or a surveillance device which has more that one kind of function, provided that the warrant specify all devices which will be used in the law enforcement operation.

Retrieval of a surveillance device after the expiry of the warrant

5.84 While the LDA section 16(3) provides that a warrant shall authorise and require the retrieval of a listening device, it did not, prior to 1998, contain any provision on retrieval after the expiry of the warrant. The effect of section 16(3) before amendment was that a listening device had to be retrieved before the expiration of a warrant. If this was not done, the validity of the warrant would have been in doubt and the admissibility of evidence obtained through the device would likewise have been in question.

5.85 Even if a further warrant were granted pursuant to section 16(6), the listening device had to be retrieved by the terms of the original warrant and then reinstalled and retrieved by virtue of

the further warrant. Where a listening device which was installed under the terms of a warrant was not retrieved before the expiration of the warrant, and was subsequently used to obtain evidence under the further warrant, evidence obtained by virtue of the subsequent warrant would have been inadmissible.

5.86 In IP 12, the Commission asked whether the proposed surveillance legislation should provide for a restricted warrant authorising and requiring the retrieval of the device, following the expiration of the main warrant.[125]

5.87 In 1998, Parliament passed the Listening Devices Amendment (Warrants) Act 1998 (NSW) amending the LDA by inserting section 16A which provided that if a listening device remained on premises after the warrant expired, it was implied that the warrant required the device's removal as soon as practicable, and was deemed to continue in force for a further 10 days for that purpose. This amendment accorded with the Wood Report recommendation that the LDA should permit retrieval of a device after the expiration of the warrant period[126] *and acknowledged that retrieval may not always be possible or practicable during the life of a single warrant or even consecutive warrants. While the 1998 amendment addressed the practical difficulties in relation to retrieval of a device, it gave rise to problems because it still required retrieval of the device.*

5.88 It may not always be necessary or practicable, or even possible, to retrieve a surveillance device. The Commission is of the view that the eligible judge should have the power to authorise the retrieval of a device but that retrieval of a device should not be automatically required by the legislation nor be implicit in the warrant. However, the Commission is also of the view that if a device is capable of continuing to transmit information after the expiry of the warrant, then the warrant-holder should obtain permission from the eligible judge not to retrieve it.

Recommendation 45

125. NSWLRC IP 12, Issue 25.
126. Wood Report at para 7.99.

The eligible judge should have the power to authorise or order retrieval of a device.

Recommendation 46

If a device is capable of continuing to transmit information after the expiry of the warrant, then the warrant-holder must obtain permission from the eligible judge not to retrieve it.

Emergency warrants

5.89 Circumstances will always arise where a warrant must be obtained as a matter of urgency, and where it is neither practical nor feasible to follow normal procedures in applying for a warrant without risking the failure of a law enforcement operation or the loss of evidence. In particular, a police officer may be stationed in a remote area without ready access to a court where an eligible judge is sitting. In such cases, the opportunity of making an application under section 18 of the LDA has been indispensable. As well, the inclusion of section 18(4), which allows a police officer to cause the telephone or radio complaint to be transmitted to the eligible judge by another member of the police force has been needed. In IP 12, the Commission made no suggestions for change to the provisions of section 18.

Submissions and Response

5.90 Although no issue was raised by the Commission, submissions were received which argued for changes to be made to section 18. The NSW Police Special Services Group suggested that the term of an emergency warrant be extended from 24 hours to 7 days, with a requirement that a written warrant be signed by the judge on the next working day.[127] The Public Defender suggested that a complaint by facsimile to apply for an emergency warrant should be

127. NSW Police Service, Special Services Group, Submission at 16.

allowed.[128]

Conclusion

5.91 The Commission does not agree that the term of the warrant should be extended to 7 days. A section 18 warrant is designed to meet an emergency and allow the police to make a written application through the normal procedure within the 24 hour period if there is further need to use the device beyond that period. The 24 hour period gives the warrant-holder sufficient time to make such application.

5.92 The Commission agrees with the Public Defender that application by facsimile should be possible. Additionally, application by e-mail or other electronic means should be allowed. The Search Warrants Act 1985 (NSW)[129] *defines a telephone, for purposes of telephone warrants, to include radio, facsimile and any other communication device. The Crimes Act 1914 (Cth) allows application by telephone, facsimile, telex and other electronic means.*

Recommendation 47

The proposed Surveillance Act should contain a provision similar to section 18 of the LDA, but should include complaint by facsimile or other electronic means as methods by which an application for a warrant can be made under the proposed section.

Warrants issued retrospectively

5.93 In some situations, there may not even be time to obtain an emergency warrant for covert surveillance. These situations include:

- *where, during covert surveillance of an offence conducted legally pursuant to a warrant, evidence was obtained of a*

128. M L Sides, Submission at 14.
129. Section 12.

separate offence of which officers had no prior suspicion or knowledge and so could not obtain a prior warrant; or

- *where it was not possible or practicable to obtain a warrant before conducting or continuing covert surveillance without prejudicing the investigation or endangering the officers or other parties involved.*

5.94 In these circumstances, the legislation should authorise the obtaining of a retrospective warrant to legitimise the covert surveillance activities and evidence and information gained. Such a warrant should be obtained as soon as possible, preferably within 24 hours, after the surveillance is conducted. Retrospective warrants should be treated as exceptional and issued sparingly.

Recommendation 48

The proposed Surveillance Act should enable warrants to be applied for within 24 hours of the surveillance taking place and issued retrospectively to law enforcement officers where:

- **evidence of an offence is obtained by covert surveillance incidentally during the investigation, pursuant to a warrant, of another offence; or**
- **it was not possible or practicable to obtain a warrant before conducting or continuing covert surveillance of an offence without prejudicing the investigation or endangering the officers or other parties involved.**

6. Covert surveillance in the public interest

- What is the “public interest”?
- The authorisation process

6.1 As stated in Chapter 2, the Commission's approach in this Report is to view individual privacy as the paramount concern in the proposed surveillance legislation. Any intrusions into privacy by way of surveillance must be justified as being of a greater public benefit. One area which may, in certain circumstances, justify intrusions into personal privacy through the use of covert surveillance is the detection and prevention of crime by law enforcement officers. Another is the need to expose illegal or improper practices in the workplace. While both of these areas represent public interests, they raise specific issues requiring the separate consideration given to them in Chapters 5 and 7.

6.2 The Commission's concern in this chapter is specifically with those circumstances which lie outside the use of covert surveillance by law enforcement officers or employers, but which may nevertheless justify invasions into privacy through covert surveillance. It is impossible to predict with any certainty the exact circumstances in which covert surveillance should be permitted to be conducted by people other than law enforcement officers or employers. The only certainty is that, in order to justify the level of privacy intrusion occasioned by covert surveillance, the surveillance must be carried out to uphold or protect a valuable public interest.[1] *Consequently, the Commission refers collectively to those circumstances as covert surveillance in the "public interest".*

6.3 This chapter examines the type of situations which would justify covert surveillance in the public interest, and the people or organisations most likely to be conducting this type of surveillance. It recommends that covert surveillance in the public interest be authorised prior to being conducted, or retrospectively if prior authorisation is not possible or practicable. This chapter also recommends procedures for issuing such authorisations.

WHAT IS THE "PUBLIC INTEREST"?

6.4 Various attempts have been made to isolate factors amounting

1. *That is, an interest so valuable in the circumstances that it displaces the public interest in the protection of individual privacy.*

to public interest and clarify what is meant by the term.[2] It is generally accepted that "public interest" is a fluid and amorphous concept, being most meaningful in the subjective rather than the objective sense.[3] What constitutes the public interest at any time will depend on particular contexts and perspectives.

6.5 The difficulty in precisely defining the concept of public interest is compounded by the fact that few circumstances give rise to just one interest: usually several public interests either blend into one another, or compete and need to be reconciled. Public interest considerations may also become blurred with matters which are merely "of interest to the public".[4] For example, the identity of a public official's partner may be of interest to some people, but it is not a matter of public interest. Expenditure of public funds by that official on his or her partner is, however, an issue in which the public has an interest.

6.6 Some public interests involve broader human rights issues, such as freedom of expression and the protection of personal privacy. Other interests may be more specific. For example, in considering the question of who may have standing to sue in public interest litigation, the Australian Law Reform Commission noted that the public has an interest in "ensuring that government decision-makers are accountable and that their decisions are made

---

2. *For a discussion of various theories as to what amounts to a public interest, see A McHarg, "Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights" (1999) 62 Modern Law Review 671 at 674-678.*
3. *See R v Trade Practices Tribunal; Ex parte Tasmanian Breweries Ltd (1971) 123 CLR 361. See also Australian Law Reform Commission, Open Government (Report 77, 1995) at para 8.13; and a speech by J Mullally, "Privacy: Are the Media a Special Case?" The New Privacy Laws: a symposium on preparing privacy laws for the 21st century (Communications Law Centre Conference, 19 February 1997, Sydney).*
4. *See Johansen v City Mutual Life Assurance Society Ltd (1905) 2 CLR 186; also K Koomen, "Under Surveillance: Fergie, Photographers and Infringements on Freedom" (1993) 17(2) University of Queensland Law Journal at 234.*

in accordance with the law", as well as an interest in "ensuring compliance with legislation that creates public rights and duties".[5]

6.7 In some cases, the public interest may overlap with the rights and interests of private individuals.[6] *A person's interest in preventing unjustified intrusions into his or her personal privacy, or protecting the right to a fair trial, are classic examples of private interests which it is in the public interest to uphold.*

6.8 Public interest is referred to but not defined in legislation across a broad spectrum. Courts and tribunals are required to consider the public interest in assessing whether to allow or prevent particular action, or review a decision to allow or prevent action.[7] *Legislation that gives examples as to the meaning of public interest does so in necessarily broad, non-exhaustive terms. For example, the Whistleblowers Protection Act 1993 (SA) states that public interest information means information that tends to show:*

- *illegal activity;*
- *irregular or unauthorised use, or substantial mismanagement, of public funds or resources;*
- *conduct that causes a substantial risk to public health or safety, or to the environment; or*

---

5. Australian Law Reform Commission, Beyond the door-keeper – standing to sue for public remedies (Report 78, 1996) at 5.

6. Some cases have held that the public interest must amount to more than a private right or individual interest: see Re Eccleston and Department of Family Services and Aboriginal and Islander Affairs (1993) 1 QAR 60. While it may be necessary to make such a distinction in some cases, the Commission contends that undertaking covert surveillance to protect a private right or interest can also involve the public interest: see para 6.11 and 6.23.

7. See eg, Defamation Act 1974 (NSW) s 16; Legal Profession Act 1987 (NSW) s 155A; Independent Commission Against Corruption Act 1988 (NSW) s 12 and s 57G; Freedom of Information Act 1989 (NSW) s 59A; Police Service Act 1990 (NSW) s 156; Protected Disclosures Act 1994 (NSW) s 3; Evidence Act 1995 (NSW) s 130; Privacy and Personal Information Protection Act 1998 (NSW) s 41; Telecommunications (Interception) Act 1979 (Cth) s 6DA.

- *that a public officer is guilty of maladministration in, or in relation to, the performance of official functions.*[8]

6.9 The most relevant definition for the Commission's purpose is that contained in the Surveillance Devices Act 1998 (WA) ("Western Australian Act"), which states that public interest includes:

> *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.*[9]

6.10 Since the Western Australian Act permits covert surveillance to be conducted in the public interest without any form of prior authorisation, a definition of public interest helps to clarify the type of surveillance activity which may lawfully be conducted under that Act. Later in this chapter, the Commission recommends that the proposed surveillance legislation only permit covert surveillance in the public interest following prior authorisation by an appropriate issuing authority.[10] *That issuing authority would assess each application for covert surveillance on a case-by-case basis to determine if a sufficient public interest existed to justify permitting the surveillance. Consequently, a definition of the type in the Western Australian Act would add nothing to the measures recommended by the Commission for the proposed surveillance legislation.*

6.11 While it may not be necessary to define public interest in broad, abstract terms, it would be useful if guidelines supplementing the proposed surveillance legislation were issued to the body responsible for authorising covert surveillance in the public interest. The guidelines could set out the types of circumstances which may give rise to public interest concerns of such significance that they justify intrusions into privacy by way of

---

8. *Whistleblowers Protection Act 1993 (SA) s 4.*
9. *Surveillance Devices Act 1998 (WA) s 24.*
10. *See para 6.33. Provision should also be made for retrospective authorisation in appropriate circumstances: see para 6.43-6.44. The Commission discusses what is meant by the term "appropriate issuing authority" at para 6.35-6.36.*

covert surveillance. Those circumstances may 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.*

These examples cover the types of areas associated with investigations by the media or private inquiry agents, and also include situations where individuals may seek to conduct covert surveillance to protect their private interests or legal rights.

The media and the public interest

6.12 The Commission noted in Chapter 2 that the recommendations in this Report for new surveillance legislation should apply to surveillance conducted by media organisations. Those organisations have long argued that any law which may have the slightest impact on their functions presents a threat to freedom of speech. The Australian Broadcasting Corporation ("ABC") and Publishing and Broadcasting Limited ("PBL") were of the view that, if there is to be any legislative regulation of electronic surveillance, there should be a specific exemption created for the media, or at least a public interest exception to cover surveillance by

media organisations.[11]

The views of the media

6.13 The ABC considered that any regulation of covert surveillance should not curtail the "media's legitimate activities in exposing corrupt, inhumane and other unacceptable practices". The ABC noted that hidden cameras were used only as a last resort after all other avenues had been explored, "appropriate editorial decision making" had occurred, and when it perceived that there was a "legitimate public interest in doing so". The ABC gave examples of when it had used hidden cameras to expose matters of public interest such as conditions in refugee camps, drug sales, consumer fraud and animal abuse. The ABC also noted that privacy concerns were reflected in its Code of Practice, which provides that:

> *[t]he 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 of public duties or about other matters of public interest, intrusions upon privacy may, in some circumstances, be justified.*[12]

6.14 PBL also expressed concern about the impact of the Commission's proposals on the role of the media in providing information to the public.[13] *PBL was opposed to any regulation of video surveillance, stating that it would make the media's job "untenable",*[14] *and that sufficient regulation already exists to protect privacy. In addition to the Listening Devices Act 1984 (NSW) ("LDA"), the Telecommunications (Interception) Act 1979 (Cth) ("Interception Act") and the general laws of trespass, defamation, contempt and nuisance, PBL noted that the Federation of Commercial Television Stations ("FACTS") Code of Practice and the Media Entertainment and Arts Alliance Code of Ethics refer to privacy concerns. The submission stated that FACTS conducted a review of its Code of Practice and received very few public submissions concerned about invasions of privacy. PBL also*

---

11. *Australian Broadcasting Corporation, Submission at 2; Publishing and Broadcasting Limited, Submission at 4.*
12. *Australian Broadcasting Corporation, Submission at 1-2.*
13. *Publishing and Broadcasting Limited, Submission at 2.*
14. *Publishing and Broadcasting Limited, Submission at 4.*

claimed that community reaction provides a safeguard against serious intrusions into privacy: meaning that television ratings and publication circulation figures would drop if the public considered the media had encroached too far into personal privacy, which would in turn discourage further use of those tactics.[15]

6.15 The Australian Press Council ("APC") agreed with the ABC that there appears to be no public interest in laws that regulate public news gathering activities. The APC was of the view that the freedom of the press is a paramount concern in a democratic society, and that the role of the press is to further that freedom by gathering information to inform the community on matters of public interest.[16] *Given that Australia has no constitutional guarantee of freedom of speech, the APC argued that there is a need to be careful when introducing laws that may impinge on free speech. The APC agreed with PBL that personal privacy is sufficiently protected under the current law and is included in the APC's Statement of Principles.*[17] *One of the APC's functions is to investigate and deal with complaints made concerning the press. In exercising this function, the APC has examined and "ruled on the ethical legitimacy of alleged intrusions by invasive means into private property", and believes, based on the small number of complaints it has received in this area, that "such intrusions by the press are not a serious concern in Australia".*

---

15. *Publishing and Broadcasting Limited, Submission at 3.*
16. *Australian Press Council, Submission at 2-3. See also Australian Press Council, "Submission to the Department of Justice, Victoria, on its Discussion Paper, 'Surveillance Devices Bill, July 1998'" «www.presscouncil.org/au/pcsite/fop/surveill.html».*
17. *Two of the principles are of particular relevance. Principle 3 provides that people 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 interest. Rumour and unconfirmed reports, if published at all, should be identified as such". Principle 4 states that news "obtained by dishonest or unfair means, or the publication of which would involve a breach of confidence, should not be published unless there is an over-riding public interest": Australian Press Council, Submission at 2-3.*

The Commission's views

6.16 Freedom of speech is a public interest of fundamental importance, and a free press plays a crucial role in preserving and upholding that public interest. What needs to be recognised, however, 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.[18] The Commission does not consider that recommending the media be included within the scope of the proposed surveillance legislation is an incursion on freedom of speech. 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.

6.17 Freedom of speech, even if it were an issue in this context, is not absolute and must sit with other public interests. Sometimes, circumstances will require that those other interests should take precedence. The law already recognises this by including media activity within the scope of defamation, contempt and trespass laws. The media are also subject to existing surveillance laws, with courts recognising that presenting the public with information should not automatically displace other public interests:

> *The invasion of privacy contrary to the provisions of the Act [the South Australian LDA] is not excused because it was done in the course of "Investigative Journalism" ...[19]*

6.18 There is often a fine line between genuine investigative journalism in the best interests of the public, and serious and

---

18. One commentator has noted that the law has so far failed satisfactorily to reconcile the concepts of privacy and press freedom: see R Wacks, "Reconciling privacy and free speech" (1999) 4(4) Media and Arts Law Review 261 at 262.

19. Miller v TCN Channel Nine (1988) 36 A Crim R 92 at 111 (Finlay J).

unjustifiable breaches of privacy. Bound by their duty to present information to the public, equipped with high quality video and sound devices and subject to the pressure of deadlines and getting a "scoop", the media are not always best placed to decide where that line should be drawn. Without an authorisations process, ratings and circulation figures could determine when intrusions into personal privacy are justified.

6.19 It should also be kept in mind that the authorisation process recommended by the Commission applies only to covert surveillance, due to its highly intrusive nature. As the ABC noted, the use of hidden cameras and other forms of covert surveillance is carried out rarely, and only as a last resort.[20] *Consequently, the recommendations in this chapter would, if implemented, affect only a small part of the media's operations.*

6.20 Finally, the fact that only a small number of complaints has been received by the APC and FACTS concerning breaches of privacy by the media does not necessarily indicate that no problem exists or that the area is sufficiently regulated. While it is praiseworthy that privacy is included in the codes and statements of ethics as an issue to be considered by journalists when investigating stories, the lack of complaints concerning privacy could easily be attributable to the absence of a single, unified and effective complaints system which could provide real redress for people with a grievance. The fact that the codes are not compulsory or binding, and the rulings of the APC are not enforceable in any meaningful way, also works against their effectiveness as privacy control measures.

Private investigators and the public interest

6.21 The private investigation industry is one of the major users of covert surveillance. Using mainly video technology, private investigators conduct covert surveillance in areas ranging from workers' compensation and motor vehicle injury claims, to arson, intellectual property matters, family law, defamation, criminal

20. See para 6.13.

matters, debt collection, repossession and process serving.[21] *Some representatives of the private investigation industry have asserted that covert surveillance is the most effective tool used by the industry to detect internal fraud and major, organised, systematic crime.*[22] *Consequently, while private investigators are hired by individuals or organisations to protect personal or business interests, their role in the detection of offences and other improper behaviour is in the overall public interest.*

6.22 Due to the resource and time pressures experienced by police, private investigators are increasingly undertaking surveillance into matters traditionally investigated by police, particularly regarding fraud.[23] *This highlights the need for greater parity between the procedures for authorising covert surveillance by law enforcement officers and private investigators. Such parity is not being achieved under the present regime. Despite the fact that law enforcement officers receive specialist training in covert surveillance and, unlike private investigators, are publicly accountable,*[24] *the authorisation regime for the type of covert surveillance conducted by law enforcement officers is currently more stringent than that for private investigators. For example, there is no record of an application by a private investigator for a warrant under the LDA, largely because, as noted earlier, private investigators usually use*

---

21. Australian Institute of Private Detectives, Submission at 2.

22. Barrington Group, Submission at 2; Australian Institute of Private Detectives, Submission at 3.

23. See Barrington Group, Submission at 2; D Turner, "Out in the Cold" The Weekend Australian (Saturday, 4 October 1997) at 33; B Kucera, "Outsourcing the Nation's Policing – Business Opportunities for the Private Sector" 35(5) The Agent (Institute of Mercantile Agents Ltd, May 2000) at 6.

24. The accountability of the private investigation industry has been the subject of discussion and debate for many years. In a submission to the Commission, the Australian Centre for Security Research at the University of Western Sydney expressed concern over the current licensing arrangements under the Commercial Agents and Private Inquiry Agents Act 1963 (NSW), and recommended that minimum standards of training, including surveillance training, should be introduced: Australian Centre for Security Research, University of Western Sydney Macarthur, Submission at 3-4.

video rather than audio surveillance. While private investigators are required to obtain an authorisation to undertake covert video surveillance under the Workplace Video Surveillance Act 1998 (NSW), this still leaves much of the non-workplace surveillance conducted by private investigators unregulated. The Commission is of the view that the system for authorising covert surveillance in the public interest under the proposed surveillance legislation should be as similar as possible to that applicable to law enforcement officers.

Private rights and the public interest

6.23 There may be occasions where an individual is justified in conducting covert surveillance to uphold a private legal right or protect a personal interest. As noted earlier, the protection of those private rights and interests may, in some circumstances, be a matter of public interest. For example, a person may have a genuine reason to fear that he or she is being stalked, but may not have sufficient evidence to approach the police. Covert monitoring of the suspect's conversation or activities may be the safest and most effective way to obtain proof of such a threat to pass on to the police. To take another example, a person may have grounds to believe that he or she will be misrepresented in a way that may lead to a wrongful prosecution or severe damage to his or her reputation. An accurate record of conversations with the person suspected may be the best evidence to refute any future allegations. In these examples, there is clearly a private interest in protecting one's personal safety, reputation, livelihood or liberty. There is also a discernible public interest in ensuring that such illegal, dangerous or malicious behaviour is prevented or detected. Accordingly, a person should be able to apply to an issuing authority for authorisation to conduct covert surveillance in the public interest even where the matter essentially involves a private right or interest.[25]

---

25. Generally, prior authorisation should be required. In the circumstances described above, however, it may not be possible or practicable to obtain prior authorisation for reasons such as lack of evidence. In such a situation, authorisation may be obtained

Recommendation 49

The proposed Surveillance Act should permit covert surveillance to be conducted in the public interest only when it is judged to be justified by an appropriate issuing authority. The proposed Surveillance Act should provide that anyone, apart from:

- **an employer in the course of an employment relationship;**
- **a law enforcement officer in the course of his or her duty; or**
- **anyone acting on behalf of an employer or a law enforcement officer in the above circumstances,**

may apply for authorisation to conduct covert surveillance in the public interest. This should include journalists, media organisations, private investigators and any other person.

Recommendation 50

The term "public interest" should be interpreted broadly by the issuing authority, and may include private rights and interests where appropriate.

Recommendation 51

The Privacy Commissioner should develop guidelines to assist the issuing authority to determine the types of circumstances which may give rise to significant public interest concerns (see paragraph 6.11).

THE AUTHORISATION PROCESS

6.24 Given that there are circumstances in which covert

following the surveillance: see para 6.43-6.44.

surveillance may be justified in the broader public interest, outside the areas of law enforcement and employment, the question remains as to how such surveillance should be authorised. As noted earlier, some media organisations suggested to the Commission that there should be a broad public interest exception. The Commission's concern with an open-ended exception requiring no authorisation is that it would be too broad, would be open to abuse and would offer insufficient privacy safeguards.[26]

6.25 Where definitions of public interest have been attempted, they have necessarily been vague and wide-ranging,[27] *and would potentially encompass any type of situation. The Commission is of the view that, because public interest is such a nebulous concept, surveillance legislation which contained a broad exception without requiring approval by an issuing authority would operate so broadly that it would not operate as a proper curb on unwarranted intrusions into personal privacy. The public interest in preventing illegality, protecting legitimate rights and interests or providing the public with information does not and should not automatically take precedence over privacy concerns in every situation. Covert surveillance may sometimes be justified in circumstances which involve the public interest. Covert surveillance will, however, always be a breach of privacy. Introducing a broad public interest exception with no approval process into surveillance legislation would have the effect of condoning covert surveillance in all cases where the person or organisation conducting the surveillance believes there to be a public interest involved, regardless of the privacy ramifications.*

6.26 A public interest exception without any form of authorisation would also place covert surveillance in the public interest at odds with that conducted by law enforcement officers and in an employment context. It would be difficult to justify from a policy perspective why law enforcement officers or employers must obtain

---

26. This view was supported by the Director of Public Prosecutions, Submission at 4; Price Waterhouse, Submission at 8; NSW *Council for Civil Liberties Inc, Submission at 4; Privacy Committee of NSW, Submission at 24; Law Society of NSW, Submission at 3.*

27. See para 6.8-6.9.

prior or retrospective authorisation to conduct covert surveillance to detect serious crime or workplace fraud, yet the same surveillance could be conducted by the media or a private investigator without any type of approval or accountability being required.

6.27 The Commission considers that covert surveillance conducted in the public interest should be required to be authorised under a process similar to that for authorising covert surveillance by law enforcement officers and in the context of employment. Chapter 5 describes the process recommended by the Commission for permitting covert surveillance by law enforcement officers, based largely on the LDA. Chapter 7 sets out the Commission's reasons and recommendations for a separate system of approval for covert surveillance in employment situations. While the procedural requirements for obtaining authorisation for covert surveillance in the public interest should be largely the same as those for the other types of surveillance,[28] a separate type of authorisation would be required due to the different nature and purpose of public interest surveillance.

28. See para 6.37-6.42 for the Commission's recommendations concerning the procedural requirements for public interest authorisations.

The Western Australian Act

6.28 The Western Australian Act contains an exception to the general prohibition on covert surveillance, permitting listening or optical surveillance devices to be used in the public interest.[29] The Western Australian Act provides that a party to a conversation or activity may use a listening or optical surveillance device if there are reasonable grounds for believing it to be in the public interest.[30] Any person, whether or not a party to a conversation or activity, may use a listening or optical surveillance device in an emergency situation where there are reasonable grounds for believing that the matter is so serious and urgent that the use of the device is in the public interest.[31] Where a device is used in an emergency situation, a written report must be made to a judge "without delay", giving details of the type of device used, the duration of use, the name of the person monitored, the circumstances which gave rise to the emergency and the intended use of the information obtained as a result.[32] Before any information obtained from the use of a surveillance device under the public interest provisions may be published or communicated, an order must be obtained from a judge allowing such publication or communication. A judge may make an order allowing publication or communication, including any conditions or restrictions considered necessary, if he or she is satisfied that it will further or protect the public interest.[33]

6.29 Originally, the Western Australian Surveillance Devices Bill did not include the part permitting public interest surveillance. During parliamentary debate on the Bill, however, the Opposition noted the heavy bias towards law enforcement, and claimed that the Bill offered insufficient scope for legitimate surveillance in other circumstances, particularly involving the media and private

29. *Surveillance Devices Act 1998 (WA) Pt 5.*
30. *Surveillance Devices Act 1998 (WA) s 26 and 27.*
31. *Surveillance Devices Act 1998 (WA) s 28 and 29.*
32. *Surveillance Devices Act 1998 (WA) s 30.*
33. *Surveillance Devices Act 1998 (WA) s 31.*

investigators.[34] As a result, the public interest section was included in the legislation.

6.30 The first application for a publication order under the Western Australian Act's public interest provisions was made by a media organisation. The Nine Network's "A Current Affair" program used a hidden camera fitted to a volunteer who offered to buy drugs from an alleged dealer. The police were aware of the surveillance, and the drugs purchased and the film of the exchange were handed to the police following the surveillance. Justice Owen in the Western Australian Supreme Court approved the publication order, considering the screening of the footage to be in the public interest.[35] The executive producer of "A Current Affair" claimed that the provisions made the media's job difficult, since they had to prove to the court that the information was in the public interest rather than deciding for themselves. However, the executive producer also noted that he did not view the Western Australian Act with "trepidation", and that the media would always work within it.[36]

6.31 While the Commission considers that the proposed surveillance legislation should permit covert surveillance in the public interest in certain circumstances, the recommendations in this Report concerning public interest surveillance differ from the Western Australian model in three major respects. First, the Western Australian Act is device-specific in that it only regulates covert surveillance in the public interest through the use of listening or optical surveillance devices. In Chapter 2, the Commission explains why it recommends against a device-specific approach for the proposed surveillance legislation.

---

34. Western Australia, Parliamentary Debates (Hansard) Legislative Assembly, 21 October 1997 at 8345.

35. Re Surveillance Devices Act 1998; Ex parte TCN Channel Nine Pty Ltd [1999] WASC 246 (Owen J).

36. M Videnieks, "How Nine-cam saw and conquered the law" The Australian (30 November 1999) at 6; M Videnieks, "Tripping on the hidden traps" The Australian (16 December 1999) at 3.

6.32 Secondly, the Western Australian Act contains a participant monitoring distinction which allows parties to a conversation or activity to record or monitor it without requiring any authorisation if they consider it to be in the public interest, while non-parties are permitted to record or monitor conversations or activities in the public interest only in an emergency. The Commission recommends, again in Chapter 2, that participant monitoring provisions should not be included in the proposed surveillance legislation.[37] *Participant monitoring is based on the flawed assumption that inviting someone to engage in a conversation or activity impliedly justifies the use of a surveillance device to monitor or record that conversation or activity. The key determinant of whether there is a public interest significant enough to justify setting privacy aside should be the circumstances that give rise to that public interest in each individual case, and not whether the person conducting the covert monitoring was a party to the conversation or activity being monitored.*

6.33 The third area in which the Commission's recommendations differ from the Western Australian Act is the point at which authorisation must be obtained. Under the Western Australian Act, authorisation must be obtained from a judge after the covert surveillance has been conducted but before the results may be published or communicated. This effectively leaves the actual monitoring of the conversation or activity unregulated.[38] *The Commission is of the view that a stronger privacy safeguard is needed, particularly given the breadth of the concept of public interest and the intrusive nature of covert surveillance. The Commission consequently recommends that a person or organisation wanting to conduct covert surveillance in the public interest must obtain approval from an issuing authority before*

---

37. See para 2.99-2.107. The Commission's Chairperson, Justice Michael Adams, dissents on this point with regard to the use of listening devices by a party to a conversation.

38. Simon Davies commented that the privacy safeguards offered by the Western Australian legislation were undercut by the public interest provisions: S Davies, "Privacy and Surveillance: The Surveillance Devices Act 1998" 27(1) Brief (February 2000) at 7.

conducting the surveillance,[39] rather than before publication and release of the information.[40] This would ensure that covert surveillance in the public interest may occur, but only in circumstances where the consequential intrusion into privacy can be justified.

The issuing authority

6.34 Throughout this chapter, reference is made to an appropriate "issuing authority" that may authorise covert surveillance in the public interest. The Commission recommends that authorisations for covert surveillance conducted by, or on behalf of, employers, should be issued by members of the Industrial Relations Commission.[41] For law enforcement officers, the Commission recommends that warrants authorising covert surveillance should be issued by "eligible judges" through the courts system.[42] At the federal level, members of the Administrative Appeals Tribunal have been issuing warrants permitting telephone interceptions since 1997, the warrants having previously been issued by "eligible judges" in the Federal Court.[43]

6.35 Consequently, an issuing authority could be members of a court or a tribunal. Both courts and tribunals are frequently required to determine questions of public interest in matters coming before them. It is the Commission's view that the ultimate decision as to which forum should issue public interest authorisations is

---

39. Unless prior authorisation is not possible or practicable, in which case retrospective authorisation should be sought: see para 6.43-6.44.

40. The authorisation to conduct covert surveillance in the public interest may specify, restrict or place conditions on the use of the information obtained as a result: see para 6.41.

41. See para 7.61-7.62.

42. Since issuing warrants is an administrative rather than a judicial function, judges are not automatically eligible to issue warrants based on their judicial status alone, but must be nominated as eligible by the Attorney General – hence the term "eligible judge": see para 5.32-5.35.

43. See Telecommunications (Interception) and Listening Devices Amendment Act 1997 (Cth).

likely to be more influenced by resources than the issue of whether a court or a tribunal is the most appropriate forum. Since the introduction of a system for authorising covert public interest surveillance is a new concept, there is no way of predicting how many applications would be made under the proposed legislation. If the number of applications happened to be quite low, it may be expedient for public interest authorisations to be issued by the courts, since "eligible judges" are already accustomed to issuing warrants and their workload would not be greatly increased. If, however, the number of applications made presented a strain on the time and resources of the courts, public interest authorisations could be issued by members of a tribunal such as the Administrative Decisions Tribunal ("ADT").[44]

6.36 Since the choice of issuing authority is likely to be a matter of an administrative rather than a legislative policy nature, the Commission refrains from recommending either the court system or the ADT. The Commission does recommend, however, that whichever body is judged to be the appropriate issuing authority, it should be accessible, affordable, expeditious and impartial. The Commission also recommends that the procedures for applying for a public interest authorisation, the factors which must be considered in deciding to issue the authorisation and the contents of the authorisation, should be as similar as possible to those recommended for covert surveillance by law enforcement officers.

---

44. The ADT is comprised of a President (who must be a District Court Judge), Deputy Presidents and non-presidential judicial members (who must be either judicial officers or legal practitioners of at least 7 years standing), and non-judicial members (who are appointed for their expertise in various areas falling within the ADT's jurisdiction): Administrative Decisions Tribunal Act 1997 (NSW) s 17. The ADT may make original decisions, as well as review decisions capable of being reviewed: Administrative Decisions Tribunal Act 1997 (NSW) s 36. The power to make decisions may be conferred on the ADT by any other Act of Parliament: Administrative Decisions Tribunal Act 1997 (NSW) s 37.

Recommendation 52

The appropriate authority for issuing authorisations to conduct covert surveillance in the public interest should be either "eligible judges" or members of a tribunal such as the Administrative Decisions Tribunal. Regardless of which forum is considered to be most appropriate, the authorisation process should be accessible, affordable, expeditious and impartial.

Factors to consider in issuing a public interest authorisation

6.37 Applications for conducting covert surveillance in the public interest should be made in writing, and may be delivered to the issuing authority in person, or transmitted by mail, facsimile or e-mail. Applications should contain as much information as possible concerning the circumstances of the proposed surveillance to enable the issuing authority to determine if the situation gives rise to a public interest which justifies the use of covert surveillance.[45] *The issuing authority should be empowered to request further information, or to refuse an application where insufficient details have been provided.*

6.38 The Commission recommends that, 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 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;*

45. The information should be similar to that required for law enforcement warrants: see para 5.74-5.77.

- *the intended use of any information obtained as a result; and*
- *whether the public interest (or interests) involved justifies the displacement of individual privacy in the circumstances.*

These factors should be listed in the proposed surveillance legislation.

Recommendation 53

The proposed Surveillance Act should require an application for an authorisation to conduct covert surveillance in the public interest to contain information similar to an application for a warrant made by a law enforcement officer (see Recommendation 41).

Recommendation 54

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; and**
- **whether the public interest (or interests) involved justifies the displacement of individual privacy in the circumstances.**

What an authorisation should specify

6.39 The LDA currently prescribes a number of matters that must be contained in a warrant.[46] *Warrants which do not comply with the LDA in this respect are invalid, and cannot be amended by the "slip rule"*[47] *nor by the Court's inherent powers, because the warrant is not granted in "proceedings" and is not an order or judgment.*[48] *So far as warrants for covert surveillance by law enforcement officers is concerned, the Commission recommended that the proposed surveillance legislation should specify what the warrant should contain and that these requirements should, like those in the LDA, be mandatory.*[49]

6.40 The Commission makes the same recommendation in relation to authorisations for public interest surveillance. It is essential that in granting a power of a highly intrusive nature, the scope and limits of that power are specified and that the requirements operate not merely as guidelines.

6.41 The proposed surveillance legislation should enable an authorisation permitting covert surveillance in the public interest to cover the use of more than one device. The legislation should provide for an authorisation to specify:

- *the circumstances in respect of which the authorisation is granted;*
- *where practicable, the name of any person who is to be the subject of surveillance;*
- *the various public interests considered;*

---

46. LDA s 16(4).
47. See Supreme Court Rules 1970 (NSW) Pt 20 r1 and 10.
48. Haynes v Attorney General (NSW, Supreme Court, No 012075/95, 9 February 1996, James J, unreported). See also Bayeh v Taylor (NSW, Supreme Court, No 13497/97, 4 February 1998, Grove J, unreported).
49. See para 5.72-5.73.

- *the period (being a period not exceeding 30 days) during which the authorisation may be in force;*[50]
- *that the surveillance device(s) may be repaired, tested, moved, maintained, replaced and/or retrieved during the duration of the authorisation;*[51]
- *the name(s) of the person(s) who may use the surveillance device(s), or who may repair, test, move, maintain, replace or retrieve the surveillance device(s), pursuant to the authorisation;*
- *if practicable, the premises on which the surveillance device(s) are to be installed or used;*
- *entry onto premises for the purpose of installing, repairing, testing, moving, replacing or retrieving the surveillance device(s), providing that no trespass is committed;*
- *the type(s) and number of surveillance device(s) to be used;*
- *any conditions subject to which the surveillance device(s) may be used pursuant to the authorisation;*
- *any conditions subject to which any information obtained as a result of the use of the surveillance device(s) may be used, released or published;*[52] *and*
- *the time within which the person authorised to use the surveillance device(s) pursuant to the authorisation is required to report to the issuing authority and the Attorney General.*[53]

6.42 In relation to covert surveillance conducted by law

---

50. This is consistent with the Commission's recommendation concerning warrants for law enforcement officers: see para 5.65-5.71.

51. Where retrieval cannot occur, the applicant must seek the further permission of the issuing authority to leave the device in place. This is consistent with the recommendations for law enforcement warrants at para 5.84-5.88.

52. See ch 9 regarding the Commission's recommendations on the use of information obtained as a result of covert surveillance.

53. See ch 8 regarding the Commission's recommendations on the reporting requirements for covert surveillance.

enforcement officers, the Commission recommended that the proposed surveillance legislation should enable a warrant to authorise entry onto premises for the purposes of installing, repairing, testing, moving, replacing or retrieving a surveillance device.[54] *That provision would legitimise entry onto premises that would otherwise amount to a trespass. The Commission considers such a recommendation to be justified in the case of law enforcement officers due to the specific accountability measures with which they must comply.*[55] *People conducting covert surveillance in the public interest are not law enforcement officers and are consequently not subject to the same accountability measures. Accordingly, the Commission considers that it would be improper and excessive for a covert public interest authorisation to authorise any entry onto premises that amounted to a trespass during the course of surveillance.*

Recommendation 55

The proposed Surveillance Act should provide that an authorisation permitting covert surveillance in the public interest may specify:

- **the circumstances in respect of which the authorisation is granted;**
- **where practicable, the name of any person who is to be the subject of surveillance;**
- **the various public interests considered;**
- **the period (being a period not exceeding 30 days) during which the authorisation may be in force;**
- **that the surveillance device(s) may be repaired, tested, moved, maintained, replaced and/or retrieved during the duration of the authorisation;**
- **the name(s) of the person(s) who may use the**

54. *See para 5.46-5.47.*
55. *Police officers, for example, are subject to internal disciplinary procedures and are answerable to the Commissioner for Police, the Police Integrity Commission, Royal Commissions, etc.*

surveillance device(s), or who may repair, test, move, maintain, replace or retrieve the surveillance device(s), pursuant to the authorisation;

- **if practicable, the premises on which the surveillance device(s) are to be installed or used;**
- **that entry onto premises for the purpose of installing, repairing, testing, moving, replacing or retrieving the surveillance device(s) is permitted, provided no trespass is committed;**
- **the type(s) and number of surveillance device(s) to be used;**
- **any conditions subject to which the surveillance device(s) may be used pursuant to the authorisation;**
- **any conditions subject to which any information obtained as a result of the use of the surveillance device(s) may be used, released or published; and**
- **the time within which the person authorised to use the surveillance device(s) pursuant to the authorisation is required to report to the issuing authority and the Attorney General (see recommendation 68).**

An authorisation permitting covert surveillance in the public interest may enable the use of more than one device.

Retrospective authorisation

6.43 Generally, authorisation for covert surveillance in the public interest should be obtained prior to the surveillance occurring. There may be situations, however, where prior authorisation is not possible or practicable. For example, a situation so urgent and serious may arise which justifies the use of covert surveillance in the public interest, but affords no time to obtain prior authorisation from the issuing authority. Another circumstance may be where a person reasonably believes that covert surveillance is necessary to further or protect the public interest, but needs more evidence to

convince the issuing authority that the surveillance is justified. This situation may arise in the example given earlier,[56] where a person wished to keep a record of a conversation because of a reasonable suspicion that he or she may be misrepresented in a way that may result in a wrongful prosecution or serious damage to his or her reputation.

6.44 In these types of situations, there should be a provision in the proposed surveillance legislation permitting authorisation following the surveillance. The Commission recommends that an application should be made to the issuing authority as soon as possible, preferably within 24 hours after the surveillance is completed.[57] In applying for a retrospective authorisation, an applicant must demonstrate why prior approval was not or could not be sought. Due to the intrusive nature of covert surveillance, particularly when conducted without prior approval, retrospective authorisations should be regarded as exceptional.

Recommendation 56

Covert surveillance in the public interest must be authorised by the appropriate body prior to the surveillance being conducted. Where such prior authorisation is not possible or practicable, it may be obtained retrospectively (preferably within 24 hours) following the conclusion of the surveillance.

Public Interest Monitor

6.45 In an attempt to ensure that broad issues of public interest and accountability are adequately canvassed during applications for, and the execution of, covert search and surveillance warrants, the position of Public Interest Monitor ("PIM") was established in Queensland in 1998. The PIM operates under three different pieces

56. See para 6.23.

57. This is consistent with the recommendation concerning retrospective warrants for law enforcement officers: see para 5.93-5.94.

of legislation: the Police Powers and Responsibilities Act 1997 (Qld),[58] the Crime Commission Act 1977 (Qld)[59] and the Criminal Justice Act 1989 (Qld).[60] The office of the PIM is funded from the budget of the Queensland Police Service, but may not be occupied by a person who is, or who is employed by the Police Service, the Director of Public Prosecutions, the Queensland Crime Commission, or the Criminal Justice Commission.[61] The role of the PIM is to:

- *appear at any application made by a law enforcement agency for covert search or surveillance warrants under the above legislation;[62]*
- *test the validity of a warrant application by issuing written questions to the applicant prior to the hearing, cross-examining the applicant during the hearing, and/or making submissions to the court on the appropriateness of granting the warrant;*
- *gather statistical information about the use and effectiveness of warrants;*
- *monitor the retention or destruction of information obtained under a warrant;*
- *provide to the Commissioner of Police, or other authority as appropriate, a report on non-compliance with the legislation; and*
- *report to Queensland Parliament at the end of each financial year on the use of surveillance and search warrants.[63]*

---

58. *Police Powers and Responsibilities Act 1997 (Qld) Pt 10.*
59. *Crime Commission Act 1977 (Qld) Pt 6.*
60. *Criminal Justice Act 1989 (Qld) Pt 3 Division 1A.*
61. *See Police Powers and Responsibilities Act 1997 (Qld) s 79; and Crime Commission Act 1997 (Qld) s 69. The current PIM is Mr Richard Perry, a barrister in private practice.*
62. *It should be noted that the legislation under which the PIM operates in Queensland permits only law enforcement agencies to apply for warrants with respect to serious criminal offences. The PIM does not, therefore, deal with issues of broader public interest as discussed in this chapter.*
63. *See Queensland, Annual Report of the Public Interest Monitor*

6.46 In exercising these functions, the PIM examines, among other things, whether the balance in a particular case lies with the public interest in privacy or the public interest in the detection and prosecution of serious criminal offences.[64]

6.47 The question of whether to include the office of the PIM in surveillance legislation is being looked at and debated in other jurisdictions.[65] *The Commission is of the view that the regime recommended in this Report embodies sufficient accountability measures*[66] *to ensure that public interest concerns are addressed, without the need for a PIM. Courts and tribunals (regardless of which forum is selected to authorise covert public interest surveillance) have been accustomed to identifying and assessing notions of public interest for some time. The Commission considers that the inclusion of a PIM model in the proposed surveillance*

---

delivered pursuant to the Police Powers and Responsibilities Act and the Crime Commission Act (RA Perry and KW Dillon, 1998) ("PIM 1998 Report") at 1-2. The approach taken by the courts has been to require warrant applicants to provide an affidavit to the PIM, within seven days following the removal of the surveillance device, setting out the information necessary for the PIM to make his report: Queensland, Second Annual Report of the Public Interest Monitor delivered pursuant to the Police Powers and Responsibilities Act and the Crime Commission Act (RA Perry and B Springer, 1999) ("PIM 1999 Report") at 1-2.

64. *PIM 1998 Report at 6. See also Heery v Criminal Justice Commission (2000) 110 A Crim R 465 (White J).*

65. *For example, the Listening Devices (Miscellaneous) Amendment Bill 1998 (SA) has been referred to a Parliamentary Legislation Committee to investigate the proposal to include the role of PIM in the legislation. Further, the appropriateness of the PIM model in relation to authorising controlled operations, in particular those conducted by the National Crime Authority, has been considered (and rejected as inappropriate) by a Federal Senate Committee: see Australia, Senate Committee, Street Legal: Senate Committee Report on the involvement of the NCA in controlled operations (December 1999) «www.aph.gov.au/senate/committees/nca_ctte/street_legal/chapter4.htm».*

66. *See ch 8 and 9 for a detailed discussion of the accountability measures recommended by the Commission.*

legislation would not improve the level of scrutiny which the appropriate issuing authority would ordinarily give to each application for a public interest authorisation.[67] *Accordingly, the Commission makes no recommendation on this issue, but raises it for further consideration.*

67. If such a monitoring system were to be considered for New South Wales, it may be more appropriate for the Privacy Commissioner to fulfil that role, rather than establishing a new layer of bureaucracy.

7. Covert surveillance in employment

- The use of surveillance by employers
- The current regulatory framework
- Adequacy of current framework
- Options for reform
- Regulation of covert surveillance

7.1 The covert surveillance of employees by employers has emerged as a growing and controversial industrial issue in recent years. In this chapter, we present an overview of the types of covert surveillance practices used by employers and identify the reasons for which increasing numbers of employers are undertaking surveillance of their employees. We also address the specific objections that are levied against the use of surveillance by employers.

7.2 The increase in the use of surveillance by employers and the issues it raises have not gone unnoticed by the law. Since the Commission released its Issues Paper ("IP 12"), the Workplace Video Surveillance Act 1998 (NSW) ("Workplace Video Surveillance Act") has been enacted and now regulates covert video surveillance of employees in the workplace. This chapter reviews the effect of that Act and provides an overview of the broader regulatory framework. It concludes that the current regulation of covert surveillance in the employment context is inadequate.

7.3 As there is now a statute that directly addresses surveillance in the employment context, we have given significant consideration to whether the deficiencies in the current regulatory regime should be remedied by amending the Workplace Video Surveillance Act or whether the issue is more appropriately addressed within the new framework recommended by the Commission. We have concluded that covert surveillance in the employment context should be addressed as an aspect of the Commission's proposed legislation. A system of covert surveillance authorisations, permitting employers to undertake covert surveillance of their employees, is proposed in this chapter.

THE USE OF SURVEILLANCE BY EMPLOYERS

Purpose of surveillance

7.4 Various surveillance devices are commonly used for a number of purposes. These are discussed in more detail below. By way of a general overview, these purposes can be summarised as follows:

> *to ensure productivity and competitiveness; to allow for quality control and customer service; to comply with laws and regulations; to assist in training and supervision; to ensure a safe and secure workplace; and to protect employer property and assets.*[1]

Types of surveillance[2]

Video

7.5 The video camera is one of the most commonly used surveillance devices in the workplace.[3] *As the cost of video surveillance equipment has fallen, this form of surveillance has become affordable to all but the smallest businesses*[4] *and, indeed, is now a standard feature of security systems in premises which have a high risk of theft or damage.*[5] *At the time of the release of the Privacy Committee's Report, Invisible Eyes, it appeared that, compared to other industrialised nations, Australia spent substantially more money per capita on video surveillance equipment.*[6]

7.6 Video surveillance is used primarily as security against theft, vandalism or unauthorised intrusion.[7] *As a form of security, a video surveillance system can be significantly cheaper than a professional security guard.*[8] *According to the Retail Traders' Association of New South Wales, "employers have a fundamental right to protect their*

---

1. *International Labour Organisation, "Workers' Privacy Part II: Monitoring and Surveillance in the Workplace" (1993) 12(1) Conditions of Work Digest ("ILO (1993)") at 17.*
2. *We note that all of the types of surveillance discussed below can be undertaken covertly and/or overtly.*
3. *Privacy Committee of New South Wales, Invisible Eyes: Report on Video Surveillance in the Workplace (Report 67, 1995) at 13.*
4. *Privacy Committee (1995) at 16. However, the Commission notes that the Chamber of Manufactures of NSW (Industrial) considers that the cost of video surveillance makes its usage practicable only for larger employers: Submission at 5-6.*
5. *Privacy Committee (1995) at 24.*
6. *Privacy Committee (1995) at 1.*
7. *Privacy Committee (1995) at 24.*
8. *Privacy Committee (1995) at 25.*

property at all times and hence should be able to make use of visual surveillance equipment to achieve this".[9]
A further use of video surveillance is to monitor employee-related matters such as breaches of occupational health and safety procedures, and general performance.[10]

Telephone

7.7 Telephone-based surveillance is another traditional and still commonly used form of surveillance.[11] *In the workplace, telephone-based surveillance takes two forms: telephone call accounting and service observation. Telephone call accounting is a form of surveillance that records the time, length and destination of telephone calls. The primary purpose of telephone call accounting is as a business tool to allocate costs,*[12] *but it is also used by employers as a means of monitoring the number of personal calls made by employees.*[13] *Service observation is a more intrusive form of telephonic surveillance as it entails listening in on telephone conversations between employees and customers or other third parties. It is commonly used by telemarketing companies, airlines and in other areas where telephone operators work.*[14] *Service observation can be used to check if employees are adhering to*

9. *Retail Traders' Association of NSW, Submission at 10.*
10. *Privacy Committee (1995) at 31 and 35.*
11. *It should be noted that the covert interception of telephone calls during their passage across a telecommunications system is governed by the Telecommunications (Interception) Act 1979 (Cth): see para 1.40.*
12. *H Metz, "They've Got Their Eyes on You" (1994) Student Lawyer 22 at 24.*
13. *D Braue, "Every Breath You Take" The Bulletin (25 January 2000) at 64; J Flanagan, "Restricting Electronic Monitoring in the Private Workplace" [1994] 43 Duke Law Journal 1256 at 1259.*
14. *M Greenbaum, "Introduction" Part I of "Employee Privacy, Monitoring and New Technology" Chapter 6 of Arbitration 1988: Proceedings of the Forty-First Annual Meeting of the National Academy of Arbitration (Bureau of National Affairs, Washington, DC, 1989) at 164.*

customer service policies,[15] to monitor the number of calls handled and time taken per call,[16] and as a training device.[17]

Computer

7.8 Computer-based monitoring is an increasingly common form of surveillance in the workplace.[18] As the number of employees using computers has increased, so too has the prevalence of computer-based monitoring. A standard form of computer-based surveillance is monitoring the performance of employees, such as data entry operators, who spend the majority of their work time on a computer.[19] The devices used are capable of tracking the number of keystrokes per minute, error rate, time taken to complete each task and time spent away from the computer.[20] The information obtained can be used by supervisors for a number of reasons including to monitor speed and accuracy, to determine pay rates and to discipline for failure to perform at the required standard.[21]

7.9 In addition to performance or productivity monitoring, computer-based monitoring can involve an employer having the ability to access all the files on an employee's computer.[22] Some technology even enables an employer to watch an employee's screen as he or she works.[23] Associated with access to the contents of an employee's hard drive is the technological potential for employers to

---

15. *Flanagan at 1260.*
16. *Greebaum at 164.*
17. *C Puplick, Privacy Commissioner of NSW, "The total workplace: A human rights perspective" Address to Employment and Industrial Law Specialists Conference (26 August 1999) «http://www.lawlink.nsw.gov.au/adb.nsf/pages/workplace».*
18. *A Westin, "Privacy in the Workplace: How Well Does American Law Reflect American Values" [1996] 72 Chicago-Kent Law Review 271 at 277.*
19. *K Jenero and L Mapes-Riordan, "Electronic Monitoring of Employees and the Elusive 'Right to Privacy'" (1992) 18(1) Employee Relations Law Journal 71 at 73; Metz at 24.*
20. *Metz at 24; Greenbaum at 164.*
21. *Greebaum at 164.*
22. *Metz at 24; L Kearley, "Computer-Based Surveillance" (1997) 2(8) Privacy Files 5 at 5.*
23. *Metz at 24; Kearley at 5.*

monitor an employee's e-mail and internet usage.[24] The key reasons cited by employers for monitoring internet and e-mail usage are diminished productivity,[25] potential legal liability[26] and information theft.[27]

Tracking devices

7.10 The final commonly used form of surveillance in the workplace is tracking devices. These can take the form of ID cards with imbedded microchips,[28] swipe cards[29] or devices attached to vehicles. The central purpose of tracking devices is to identify the physical location or movements of employees.

Objections to covert surveillance

7.11 As outlined above, covert surveillance of employees can be a highly effective business tool and can be used for a range of positive purposes, such as ensuring a safe workplace. However, these benefits must be balanced against the detrimental effects on employees.

7.12 As in the case of surveillance generally, surveillance in the employment context has serious privacy implications. Although the surveillance may be intended to capture only work-related matters, even narrowly focussed surveillance has the potential to intercept personal information or activity.[30] For example, covert video surveillance designed as a security measure may capture images of an employee engaged in a private activity such as scratching a body

---

24. Refer to ch 2 for a fuller discussion of e-mail and internet monitoring.

25. NetComm, an Australian modem maker, estimates that the internet is responsible for $1 billion a year in lost productivity: M Bryan, "Every step you take, every move you make" Australian Financial Review (4 March 2000) at 27.

26. See performance monitoring discussion in ch 3.

27. Bryan at 27.

28. Kearly at 5.

29. M Ford, Surveillance and Privacy at Work (Institute of Employment Rights, London, 1998) at 11.

30. Flanagan at 1262.

part.[31] *Even where only work-related matters are caught by surveillance, there are still broad issues of workers' autonomy and dignity, matters inherent in the concept of privacy.*

7.13 In addition to the impact of workplace surveillance upon an employee's privacy, the privacy implications extend to third parties with whom employees may communicate or who may be physically present at a location that is under surveillance. For example, listening-in on telephone calls or reading e-mails has implications for the privacy of the non-employee participant.[32] *Similarly, CCTV cameras installed, for example, in a service station to ensure employee safety will inevitably capture images of customers.*

7.14 A final objection to the use of surveillance by employers is based on its potentially discriminatory impact. This impact becomes clear when consideration is given to labour market segregation; for example, as women and ethnic minorities tend to predominate in monitored jobs, they are monitored at a disproportionately high rate.[33] *A further way in which surveillance can have a discriminatory impact is through its capacity to target certain individuals or groups, such as union members.*[34]

THE CURRENT REGULATORY FRAMEWORK

7.15 General legislation regulating surveillance, such as the Listening Devices Act 1984 (NSW) ("LDA"), is equally applicable in the employment context. In this chapter, consideration is given to those means of regulation specific to the employment context.

---

31. Privacy Committee (1995) at 41.

32. A Westin, "Monitoring and New Office Systems" Part II of "Employee Privacy, Monitoring and New Technology" Chapter 6 of Arbitration 1988: Proceedings of the Forty-First Annual Meeting of the National Academy of Arbitration (Bureau of National Affairs, Washington, DC, 1989) at 168.

33. ILO (1993) at 12.

34. For example, swipe cards that can identify individual employees can be used to monitor which employees attend a union meeting, if the meeting is held in a part of the building that requires swipe card access.

The Workplace Video Surveillance Act 1998 (NSW)

7.16 The Workplace Video Surveillance Act commenced operation on 1 February 1999. The object of the Act is to regulate the covert video surveillance of employees in the workplace by their employers. It applies to both public and private sector employers.[35] *At the time the Workplace Video Surveillance Act was enacted, video surveillance in the workplace was completely unregulated. However, a number of industrial disputes regarding employee surveillance had highlighted the need for regulation of what had become a prominent industrial issue.*[36] *In coming to the approach adopted in the Act, the Government aimed to strike an appropriate balance between the competing interests of employers and employees.*[37] *The Workplace Video Surveillance Act approach follows extensive consideration of the issue of video surveillance in the workplace by the Privacy Committee of New South Wales*[38] *and the Working Party on Video Surveillance in the Workplace.*[39]

Threshold elements

7.17 The Workplace Video Surveillance Act only applies to surveillance that is:

- *covert;*
- *carried out by video;*
- *of an employee;*
- *by an employer; and*
- *undertaken in the workplace.*

---

35. *Special provision is made for prisons, casinos, police and the courts: Workplace Video Surveillance Act 1998 (NSW) s 7(2).*
36. *New South Wales, Parliamentary Debates (Hansard) Legislative Council, 26 May 1998 at 5087.*
37. *New South Wales, Parliamentary Debates (Hansard) Legislative Council, 26 May 1998 at 5088.*
38. *Privacy Committee (1995).*
39. *Working Party on Video Surveillance in the Workplace, Report to the Hon J W Shaw QC MLC Attorney General and Minister for Industrial Relations (NSW Department of Industrial Relations, Sydney, December 1996).*

7.18 Any surveillance that does not meet the above criteria is untouched by the Act. Accordingly, overt surveillance of an employee by an employer is unregulated. So too is covert surveillance of an employee's telephone or computer.

Meaning of "covert surveillance"

7.19 Under the Workplace Video Surveillance Act, surveillance is presumed to be covert and will only escape being classified as covert if:

- *an employee has been notified in writing of the intended video surveillance at least 14 days in advance;*
- *the cameras or other parts of equipment are clearly visible; and*
- *signs notifying people that they may be under surveillance are clearly visible.*[40]

7.20 It should be noted that the above criteria are cumulative and, accordingly, all three elements must be satisfied before surveillance will escape the reach of the Act.

Undertaking covert video surveillance

7.21 The Workplace Video Surveillance Act establishes strict criteria for the use of covert video surveillance in the workplace. Covert video surveillance is only permitted if:

- *it is carried out solely for the purpose of establishing whether or not an employee is involved in any unlawful activity in the workplace; and*
- *it is authorised by a covert surveillance authority, issued by a Magistrate.*[41]

7.22 Accordingly, employers can only undertake covert surveillance if they believe an employee is involved in an unlawful activity in the workplace. The use of surveillance for other purposes, such as monitoring performance, is expressly prohibited.[42] *Surveillance is*

---

40. Workplace Video Surveillance Act 1998 (NSW) s 4(1).
41. Workplace Video Surveillance Act 1998 (NSW) s 7(1).
42. Workplace Video Surveillance Act 1998 (NSW) s 9(3)(a).

also prohibited in a change room, toilet facility, shower or other bathing facility.[43]

7.23 An application for a covert surveillance authority must provide detailed information such as the grounds for suspecting that a particular employee is involved in unlawful activity and whether other investigative procedures have been undertaken to detect the unlawful activity.[44] *In order to issue an authority, a Magistrate must be satisfied that the application shows that reasonable grounds exist to justify its issue.*[45] *The Magistrate is also expressly required to consider the privacy implications of the proposed surveillance.*[46] *Should an employer wish to undertake surveillance in a recreation or meal room, the Magistrate must consider the employees' heightened expectations of privacy.*[47]

Offences

7.24 An employer who undertakes covert video surveillance otherwise than for the permitted purpose and without the requisite authority commits an offence, for which significant monetary penalties apply.[48]

7.25 It is also an offence to use a recording obtained by surveillance, which was authorised by a covert surveillance authority, for an "irrelevant purpose".[49] *A purpose will be irrelevant if it is not related to the detection of unlawful activity, to other associated matters such as taking disciplinary action or legal proceedings or to taking any other action authorised by the Workplace Video Surveillance Act. This offence reinforces the prohibition regarding performance monitoring as it prevents an employer using a recording as the basis for performance-related dismissal or other similar matters.*

---

43. *Workplace Video Surveillance Act 1998 (NSW) s 9(3)(b).*
44. *Workplace Video Surveillance Act 1998 (NSW) s 10(2).*
45. *Workplace Video Surveillance Act 1998 (NSW) s 13(1).*
46. *Workplace Video Surveillance Act 1998 (NSW) s 14.*
47. *Workplace Video Surveillance Act 1998 (NSW) s 13(2).*
48. *Workplace Video Surveillance Act 1998 (NSW) s 7(1) (subject to the limited exceptions in s 7(2) and 7(3)).*
49. *Workplace Video Surveillance Act 1998 (NSW) s 8.*

Industrial relations legislation

7.26 The primary industrial relations statute in New South Wales is the Industrial Relations Act 1996 (NSW) ("IRA"), with its federal counterpart being the Workplace Relations Act 1996 (Cth) ("WRA"). Neither of these Acts expressly regulates surveillance or privacy in the employment context. However, they do provide the potential for covert surveillance of employees by employers to be regulated indirectly.

An industrial matter

7.27 The surveillance of employees in the workplace is listed as an example of an "industrial matter" in section 6(2)(j) of the IRA. Accordingly, surveillance can be the subject of negotiations regarding employment conditions, addressed in awards and enterprise agreements. As an industrial matter, surveillance may form the basis of an industrial dispute, which can be arbitrated by the NSW Industrial Relations Commission.

7.28 Under the WRA, only "allowable award matters" can be included in an industrial dispute, which can be addressed by the Australian Industrial Relations Commission by way of arbitration or an award.[50] Surveillance is not listed as an allowable award matter. However, section 89A(7) does permit an "exceptional matter" to be included in an industrial dispute. While this creates the possibility that surveillance could be the subject of an industrial dispute, stringent criteria must be met before a matter will qualify as "exceptional".

7.29 Despite not being an allowable award matter at a federal level, surveillance can, of course, be a negotiated condition of a certified agreement or an Australian Workplace Agreement under the WRA.

Unfair dismissal

7.30 Under the WRA and the IRA, employees are able to apply for relief in respect of a dismissal that was harsh, unjust or

50. Workplace Relations Act 1996 (Cth) s 89A.

unreasonable.[51] Relief is potentially available where the dismissal is based on evidence collected using surveillance. However, at both state and federal level, relief for unfair dismissal is only available to a limited range of persons.[52]

7.31 Determination of an unfair dismissal claim is a discretionary exercise and each case is considered in light of its own particular circumstances.[53] However, both the IRA[54] and WRA[55] set out a number of matters that the NSW Industrial Relations Commission or the Australian Industrial Relations Commission must take into account in determining a claim. Those matters likely to be relevant to a claim for unfair dismissal where the dismissal was based on evidence collected using surveillance are those pertaining to procedural fairness:

- *whether a reason for the dismissal was given to the applicant;*
- *if a reason was given, whether it had a basis in fact;*
- *whether the applicant was given an opportunity to make out a defence or give an explanation for his or her behaviour; and*
- *whether a warning of unsatisfactory performance was given before the dismissal.*

7.32 An example of where procedural unfairness may taint a surveillance-based dismissal is where no warning is given in a dismissal based on the results of performance monitoring. For example, a data entry operator who was dismissed without warning on the basis of his or her keystroke rate may be able to claim relief for unfair dismissal. The NSW Industrial Relations Commission has commented that "an employee is entitled to be warned in clear terms, preferably in writing, if his work performance is

---

51. Industrial Relations Act 1996 (NSW) s 84; Workplace Relations Act 1996 (Cth) s 170CE(1)(a).
52. Industrial Relations Act 1996 (NSW) s 83; Workplace Relations Act 1996 (Cth) s 170CB.
53. Byrne and Frew v Australian Airlines Ltd (1995) 185 CLR 410.
54. Industrial Relations Act 1996 (NSW) s 88.
55. Workplace Relations Act 1996 (Cth) s 170CG(3).

unsatisfactory to the extent that he may be dismissed over it".[56]

7.33 However, procedural unfairness does not necessarily render a dismissal unfair. As noted above, whether the use of an unfair procedure renders a dismissal harsh, unjust or unreasonable depends on the whole of the circumstances. Indeed, where serious misconduct is involved, such behaviour can outweigh even substantial procedural unfairness. For example, in Wang and Others v Crestell Industries Pty Ltd and Another,[57] *the clear video evidence of theft of products from the employer's factory was sufficient to outweigh the lack of any reason or explanation being given for the dismissal, the failure to provide the employees with an opportunity to explain their conduct or make out a defence and the lack of any previous warnings indicating the consequences of the conduct, the type of which led to dismissal.*

7.34 Under the New South Wales legislation, the primary remedy for an unfair dismissal is reinstatement.[58] *If it is impractical for the applicant to be reinstated to his or her former position, then the NSW Industrial Relations Commission may order that they be re-employed in a different, suitable position.*[59] *The Commonwealth Act's approach is to provide for reinstatement or re-employment as equally available remedies.*[60] *In both Acts, should neither reinstatement nor re-employment be appropriate remedies, then the applicant may be awarded compensation.*[61]

---

56. *Watters v Zig Zag Railway Lithgow (NSW, Industrial Relations Commission, 3126 of 1993, Connor CC, 9 March 1994, unreported) at 7; see M Baragwanath, Unfair Dismissal in New South Wales (LBC Information Services, Sydney, 1999) at 124.*
57. *Wang and Others v Crestell Industries Pty Ltd and Another (1997) 73 IR 454. This was a decision of the Full Bench of the NSW Industrial Relations Commission.*
58. *Industrial Relations Act 1996 (NSW) s 89(1).*
59. *Industrial Relations Act 1996 (NSW) s 89(2).*
60. *Workplace Relations Act 1996 (Cth) s 170CH(3).*
61. *Industrial Relations Act 1996 (NSW) s 89(5); Workplace Relations Act 1996 (Cth) s 170CH(6).*

Employment contracts

7.35 For those employees not covered by an award or other similar industrial instrument, or by the statutory unfair dismissal provisions, any regulation of surveillance depends upon the express and implied terms of their employment contract. Employees may be able to negotiate a contractual provision regulating the use of surveillance by their employer. As a safeguard over this contractual freedom, the NSW Industrial Commission has the power to declare a contract void or varied, on the basis that it is unfair.[62] *One of the grounds on which a contract may be defined as unfair is that it is unfair, harsh, unconscionable or against the public interest.*[63] *While there is no authority on the point that we are aware of, we consider that certain contractually agreed uses of surveillance could be considered to render a contract unfair.*

7.36 In addition to express contractual provisions, certain provisions are implied in any contract of employment by operation of the common law. The historical roots of the employment contract in the master/servant relationship are clearly reflected in the nature of these implied common law duties and obligations.[64] *For example, while an employee owes a duty to obey orders, an employer owes a duty to provide work. A restriction on the use of surveillance does not sit easily with the general tenor of the common law duties. However, a possible source of control on the use of surveillance is the term implied in employment contracts that an employer will not unreasonably damage or destroy the relationship of trust and confidence between employer and employee.*[65] *The Full*

62. *Industrial Relations Act 1996 (NSW) s 106.*
63. *Industrial Relations Act 1996 (NSW) s 105.*
64. *R McCallum, Employer Controls over Private Life (UNSW Press, Sydney, 2000).*
65. *See Burazin v Blacktown City Guardian Pty Ltd (1996) 142 ALR 144; Mahmud v Bank of Credit and Commerce International SA [1997] 3 WLR 95; Ryan v Aboriginal Gallery of Dreamings (Federal Court of Australia, No VI97/1281, Murphy JR, 20 June 1997, unreported); Fraser v Transport Accident Commission (Federal Court of Australia, No VI 1185 of 1997, Murphy JR, 5 August 1997, unreported).*

Court of the Industrial Relations Court of Australia has identified the purpose of this implied term as being "to protect the employee from oppression, harassment and loss of job satisfaction".[66] *Use of covert surveillance by an employer could implicate this purpose.*

ADEQUACY OF CURRENT FRAMEWORK

7.37 The enactment of the Workplace Video Surveillance Act was a significant step towards addressing the issue of covert surveillance in the employment context. However, the restriction of that Act's provisions to video surveillance renders it clearly inadequate to address the broad issue of employee surveillance. Prevalent surveillance practices, such as telephone call accounting or e-mail monitoring, remain unregulated.

7.38 The negotiation of employment conditions, either at a collective or individual level, is one way in which the lacunae in the Workplace Video Surveillance Act can currently be addressed. However, in the view of the Commission, serious questions must be asked about the desirability of leaving surveillance to be addressed as a negotiable condition of employment. One obvious concern is the inequality of bargaining power between employee and employer that often exists. This inequality is potentially exacerbated by the abstract nature of privacy interests. For example, it is easier to negotiate over a pay increase than over a level of privacy.[67] *A further concern is that any bargaining process may not be an informed one, if employers are not required to disclose their surveillance practices.*[68] *In addition to these practical concerns, there is the issue of whether it is appropriate to reduce a fundamental interest, such as privacy, to a bargaining issue.*[69]

7.39 Unfair dismissal relief is an additional, albeit indirect, way

---

66. Burazin v Blacktown City Guardian Pty Ltd (1996) 142 ALR 144 at 152.
67. D King, "Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging Privacy Gap" (1994) 67 Southern California Law Review 441 at 448.
68. King at 448-449.
69. King at 448.

in which surveillance of employees is currently regulated. A key concern with this form of regulation is the lack of comprehensive coverage and the fact that it only addresses surveillance once it has occurred, rather than preventing unacceptable use of surveillance from the outset. As an example of coverage concerns, reliance on unfair dismissal provisions to address procedurally unfair use of surveillance would leave the 23% of Australians who are employed on a casual basis[70] with no protection.[71] Such a situation is clearly unsatisfactory.

7.40 The current regulatory framework does not provide comprehensive regulation of surveillance by employers. Many forms of surveillance are, at best, only indirectly regulated. Furthermore, in order to trigger the indirect protection of industrial remedies such as relief against unfair dismissal, extreme circumstances must be involved. The Commission considers that it is inappropriate for a matter of fundamental importance, such as personal privacy, to be addressed in such a piecemeal and indirect manner. In accordance with its status, employee privacy should be protected as a matter of course, rather than only gaining protection in circumstances of extreme violation.

7.41 On a more practical note, the vagaries of the current regulatory system are intolerable for both employer and employee. Employers are often unable to obtain confirmation of the legality of their surveillance procedures and employees have no certain basis upon which to challenge an aspect of their workplace surveillance policy. In the view of the Commission, the requisite certainty can only emerge from a legislative model.

---

70. McCallum at 10.

71. Unless they had been engaged by a particular employer during a period of at least 12 months and had a reasonable expectation of continuing employment: Workplace Relations Regulations 1996 (Cth) reg 30B(3). Under the Industrial Relations (General) Regulation 1996 (NSW), the requisite period is at least 6 months: reg 5B(1)(d).

OPTIONS FOR REFORM

7.42 The Commission considers that there are two possible approaches to achieving comprehensive regulation of covert surveillance in the employment context:

(a) amend the Workplace Video Surveillance Act; or

(b) integrate the employment context into the general framework proposed by the Commission, creating separate provisions, where necessary.

A similar expectation of privacy?

7.43 A significant issue in determining the appropriate option for reform is whether or not expectations of privacy in an employment context correspond substantially to expectations of privacy in general. If it is determined that expectations of privacy in an employment context are fundamentally different, then it will be inappropriate to merge regulation of surveillance in employment with the general framework.

7.44 While it is generally accepted that individuals have a privacy expectation in their homes or walking down the street, the concept of an expectation of privacy does not easily translate into the workplace. Some commentators have argued that an employee, who uses the employers' premises, resources and time,[72] and who must accept some form of supervision,[73] cannot have a reasonable expectation of privacy. Indeed, it must be expected that an employer will watch the activities of employees and monitor performance.

7.45 The Commission rejects the argument that employees leave behind any expectation of privacy at the office door. Acceptance of that argument necessarily translates privacy into a property, rather than personal interest. If privacy is viewed as a property interest, then its applicability will vary depending upon the physical

72. L Kearly, "Privacy in the workplace" (1997) 2(8) Privacy Files 1 at 1.
73. V Steeves, "Privacy in the Workplace: A Moral and Legal Right" (1997) 2(8) Privacy Files 2 at 2.

location of an individual. In the Commission's view, this cannot be correct. In this regard, we support the view of the Privacy Committee that the right to privacy is a personal right, which does not appear or disappear based on a person's geographical location.[74] *To similar effect, the Australian Privacy Commissioner has stated that "it is clear that most staff do not expect to completely sacrifice their privacy while at work".*[75]

Third parties

7.46 Having established that expectations of privacy are not fundamentally different in the employment and non-employment contexts, it becomes apparent that both reform options are possible. A matter that impacts on whether we integrate employment surveillance into the general regime is third party interests. As was noted above, at paragraph 7.13, third parties are often inadvertently affected by employment surveillance through communicating with an employee or being present in another persons' workplace. Accordingly, when an employer undertakes surveillance of an employee, that employer will often also be undertaking surveillance of a third party. This dual privacy implication will necessarily exist in surveillance of workplaces such as shops or restaurants. Indeed, unintentional surveillance of third parties will be unavoidable in many situations. Accordingly, rather than isolating surveillance of employees as an industrial issue, the Commission considers that it should, to the maximum extent possible, be regulated consistently with other forms of surveillance. While it is recognised that some employment specific provisions will be necessary, the fundamental framework should be the same, irrespective of whether surveillance is of an employee or a member of the public.

---

74. Privacy Committee of NSW, Submission at 9; see also para 2.26.

75. Australia, Privacy Commissioner, Guidelines on Workplace E-mail, Web Browsing and Privacy (30 March 2000) «http:www.privacy.gov.au/issues/p7_4.html».

Recommendation 57

Surveillance in the employment context should be addressed as part of the general framework proposed by the Commission, with the creation of employment specific provisions where necessary.

REGULATION OF COVERT SURVEILLANCE

7.47 An existing model for the regulation of covert surveillance is the Workplace Video Surveillance Act. Although its applicability is limited to video surveillance, the Commission considers that the basic authorisation framework can apply equally in respect of all forms of surveillance devices. In proposing that the Workplace Video Surveillance Act form the basis of our recommendations for the regulation of covert surveillance in the employment context, we are cognisant of the substantial consultation and consideration that occurred in its gestation.[76] *However, in certain respects, deviation from the Workplace Video Surveillance Act approach will be necessary to ensure that the system for authorising covert surveillance in the employment context is as similar as possible to those applicable to the public interest and law enforcement areas. We are of the view that this similarity is desirable as it will enable a consistent jurisprudence to be developed across the three areas of covert surveillance. Furthermore, as the same basic framework and concerns inform all three areas, it is appropriate that this fundamental similarity is reflected in the authorisation systems.*

76. We refer here to the Privacy Committee Report (1995) and Working Party on Video Surveillance in the Workplace, Report to the Hon J W Shaw QC MLC Attorney General and Minister for Industrial Relations (NSW Department of Industrial Relations, Sydney, December 1996); see also New South Wales, Parliamentary Debates (Hansard) Legislative Council, 26 May 1998 at 5087.

Permitted purpose

A general ability to undertake covert surveillance?

7.48 A view expressed by employer groups is that employers should be able to undertake covert surveillance in a broad range of circumstances in the exercise of a right to protect their business interests.[77] Covert surveillance is cited as a particularly effective means of detecting unlawful activity such as fraud or theft.[78] The Commission acknowledges that employers have a legitimate interest in ensuring a productive and efficient business, but further considers that there must be controls on what conduct is permitted in the pursuit of this interest. Indeed, the law places many limits upon what is acceptable conduct by an employer.[79] For example, anti-discrimination laws and occupational health and safety provisions impose external obligations and conditions upon employer conduct. Such obligations and conditions are based on the protection of fundamental employee interests. The Commission considers that restricting an employer's ability to undertake covert surveillance of an employee is a similarly justified limitation, based as it is on protecting an employee's interest in personal privacy.

7.49 In coming to the view that the protection of employee privacy requires restriction of an employer's ability to undertake covert surveillance, the Commission should not be taken as considering that employee privacy is an absolute right or interest. Rather, as in the case of anti-discrimination protections, limitations can be imposed on an employee's privacy interest where sufficient justification exists. Given the fundamental importance of personal privacy, the Commission considers that utilitarian or cost-benefit justifications are insufficient to merit the severe invasion represented by covert surveillance.[80] However, we do consider that suspicion of unlawful activity or serious misconduct justifying summary dismissal constitute a justifiable limitation on employee

---

77. See eg, Chamber of Manufactures of NSW (Industrial), Submission at 7; Retail Traders' Association of NSW, Submission at 7.

78. See eg, Registered Clubs Association of NSW, Submission at 6; Retail Traders' Association of NSW, Submission at 7.

79. Flanagan at 1273.

80. In this regard, the Commission agrees with Ford at 14.

privacy. These justifications are discussed in greater detail below.

Is surveillance distinguishable from supervision?

7.50 In addition to the general argument outlined above, we note the existence of a specific argument that surveillance of employees is a form of supervision and, accordingly, should not be regulated. This argument draws on the fact that supervision and monitoring of employees is not a new phenomenon; supervisors have always watched employees[81] and surveillance devices, although not as technologically sophisticated as those used today, have been a common feature of employment for over a century. For example, devices attached to typewriters for counting keystrokes were used in the early 1900s.[82] According to this line of thinking, surveillance is merely an extension of the traditional supervisory relationship that is inherent in an employment situation. As such, it is a justifiable intrusion into employee privacy.

7.51 The Commission acknowledges that some degree of supervision is acceptable in employment. However, we disagree that surveillance undertaken by technology equates to traditional forms of supervision, undertaken by another individual. The capacities of modern forms of surveillance render it far more intrusive than traditional supervision; for example, video cameras have powerful zoom mechanisms[83] and new technologies make possible continuous, unseen monitoring.[84] Furthermore, in the case of many forms of surveillance, a permanent, reproducible record of an individual's activities and behaviour is created.[85] The level of intrusion made possible by surveillance devices clearly, in the Commission's opinion, distinguishes it from traditional forms of supervision. It is accordingly appropriate to subject surveillance to more stringent regulation.

Suspicion of unlawful activity

7.52 In accordance with the approach adopted in the Workplace

---

81. Greenbaum at 163.
82. ILO (1993) at 11.
83. Privacy Committee (1995) at 22.
84. Metz at 24.
85. Privacy Committee (1995) at 22.

Video Surveillance Act, the Commission considers that an employer should be permitted to conduct covert surveillance of an employee where unlawful activity is suspected. Where the unlawful activity is suspected to be occurring other than on work premises, it must be employment-related; this requirement flows from the definition of the employment context.

7.53 In coming to this conclusion, we have given consideration to the view expressed in submissions that employers should not be undertaking covert surveillance in any circumstances.[86] *According to certain proponents of this view, should unlawful activity be suspected, then surveillance is appropriately a matter for a law enforcement agency.*[87] *While this approach certainly protects employees from unreasonable intrusions into their personal privacy, the Commission is concerned that it fails to accommodate employers' legitimate interest in addressing unlawful activity on work premises or otherwise employment related. We agree that, in theory, an employer should be able to request police assistance if unlawful activity is suspected. However, where the activity is not occurring on a large scale, the police may well be unable to allocate limited surveillance devices or time to conducting a comprehensive investigation.*[88] *It seems unreasonable to prevent employers addressing unlawful activity in such circumstances.*

Suspicion of serious misconduct justifying summary dismissal

7.54 We have given significant consideration to the question of whether there should be any further basis upon which an employer may be permitted to undertake covert surveillance of an employee. We recommend that the criteria for undertaking covert surveillance be extended to include a reasonable suspicion of serious misconduct justifying summary dismissal. Here, we are drawing on the common law power of employers to summarily dismiss an employee whose misconduct justifies the employer in treating the employment contract as at an end.[89] *This additional justification would*

86. NSW Council for Civil Liberties, Submission at 5; NSW Young Lawyers Criminal Law Committee, Submission at 9.
87. NSW Young Lawyers Criminal Law Committee, Submission at 9.
88. Privacy Committee (1995) at 63.
89. See North v Television Corporation Ltd (1976) 11 ALR 599 for a

encompass behaviour such as falsifying time records[90] and other forms of serious misconduct. Its availability will depend on both the particular employment relationship involved and the relevant conduct.[91]

Recommendation 58

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.

Covert performance monitoring

7.55 It is implicit in the above discussion that the Commission is of the view that performance monitoring is not in itself an acceptable purpose of covert surveillance. This view was shared by the majority of submissions that expressed a view on this specific issue.[92] While we consider that performance monitoring is an unacceptable use of covert surveillance, we are also aware that surveillance installed for a completely separate purpose may often indirectly result in a degree of performance monitoring. To ensure that this function creep is controlled to the greatest extent possible, we recommend

discussion of the requirements for summary dismissal.

90. *Electricity Comm of NSW t/a Pacific Power v Nieass (1995) 39 AILR 5-060.*
91. *Further guidance to its scope can be found in Workplace Relations Regulations 1996 (Cth) reg 30CA.*
92. *Barrington Group, Submission at 1 and 5; Registered Clubs Association of NSW, Submission at 8; Service Station Association Ltd, Submission at 2; M L Sides, Submission at 20; Privacy Committee of NSW, Submission at 30; Price Waterhouse, Submission at 16.*

that the Workplace Video Surveillance Act prohibition on the use of covert surveillance to undertake performance monitoring be carried into the new legislation.

7.56 We do not consider that such a prohibition would preclude employers from monitoring an aspect of an employee's performance, where the purpose of the monitoring was to detect unlawful activity or conduct justifying summary dismissal.

Recommendation 59

There should continue to be an express prohibition on the use of covert surveillance by employers for the purpose of monitoring employee performance.

Covert surveillance in toilets, change rooms and meal rooms

7.57 In IP 12, the Commission raised the issue of whether surveillance should be permitted in certain areas such as toilets and change rooms. The basis of identifying these areas as requiring particular consideration was the heightened expectation of privacy that employees would have in such areas. The current approach of the Workplace Video Surveillance Act is that surveillance is not permitted in any change room, toilet facility, shower or other bathing facility.[93] Surveillance is, however, permitted in a recreation room, meal room or other similar area where employees are not directly engaged in work. The heightened expectation of privacy in such areas is addressed by a requirement that the Magistrate must have regard to the employees' heightened expectation of privacy.[94]

7.58 A number of submissions that expressed a view on this issue considered that surveillance should not be permitted in areas such

93. Workplace Video Surveillance Act 1998 (NSW) s 9(3)(b).
94. Workplace Video Surveillance Act 1998 (NSW) s 13(2).

as toilets and change rooms.[95] Such surveillance practices were viewed by some as being an abuse of covert video surveillance.[96] However, certain submissions conversely stated that there should not be a blanket prohibition and that scope should be retained for employers to undertake covert surveillance in these areas.[97]

7.59 In view of the extremely intrusive nature of carrying out covert surveillance in areas where employees would reasonably expect to have a very high degree of privacy, the Commission has concluded that the prohibition on surveillance in toilets, showers and change room should be retained. Should employers consider that there is a need to undertake surveillance in these areas, the appropriate approach is for a law enforcement agency to become involved.

Recommendation 60

Covert surveillance of employees by employers in toilets, showers and change rooms should be prohibited.

7.60 Limited views were expressed in submissions regarding covert surveillance in areas such as meal and recreational rooms.[98] Clearly, an employees' expectation of privacy will not be as high in respect of a meal room as regarding a toilet. However, the Commission considers that employees' expectations of privacy will reasonably be higher than when they are in an official work space, such as their office or a service counter. Areas such as meal rooms

95. NSW Young Lawyers Criminal Law Committee, Submission at 9; Barrington Group, Submission at 5; Privacy Committee of NSW, Submission at 29; NSW Nurses' Association, Submission at 2.

96. Barrington Group, Submission at 1.

97. Chamber of Manufactures of NSW (Industrial), Submission at 9; Institute of Mercantile Agents, Submission at 3; Retail Traders' Association of NSW, Submission at 10; Registered Clubs Association of NSW, Submission at 8; Price Waterhouse, Submission at 15.

98. The NSW Nurses' Association submitted that such surveillance should be prohibited: Submission at 2; Price Waterhouse considered that surveillance may be appropriate in these areas if there was a demonstrated need: Submission at 15.

are an area of the workplace where employees expect to have time out from the official performance of their duties and to engage in social interactions with other employees.[99] *The particular informal nature of recreational and meal rooms can be accommodated by the current approach of the Workplace Video Surveillance Act.*

Recommendation 61

When considering an application by an employer for a covert surveillance authorisation that will involve surveillance in recreational or meal rooms, regard must be had to the employees' heightened expectation of privacy.

The issuing authority

7.61 Under the Workplace Video Surveillance Act, Magistrates have responsibility for considering applications for covert surveillance authorities. The Commission recommends that this responsibility be moved from Magistrates to Industrial Magistrates and Judicial Members of the Industrial Relations Commission. As the fundamental basis of providing a separate authorisation regime for surveillance by employers is the industrial dimension, it seems appropriate that Industrial Magistrates and the Judicial Members of the Industrial Relations Commission are the issuing authority. We recommend that the function of determining applications by employers for covert surveillance authorisations be restricted to judicial officers for the reasons outlined in relation to warrants in Chapter 5.[100]

7.62 We note that the Registered Clubs Association of NSW considers that it would be inappropriate for the Industrial Relations Commission to have responsibility for authorisations, as

99. Privacy Committee (1995) at 54.

100. The reasons for not limiting the recommendation to judicial officers with the status of Supreme Court Judges are the same as those expressed in ch 5.

it would be the body handling any disputes that might arise out of the surveillance.[101] *In the view of the Commission, this situation would be no different from that where the Industrial Relations Commission must address a dispute arising from an award it has made or an enterprise agreement it has approved.*

Recommendation 62

Applications by employers for covert surveillance authorisations should be determined by an Industrial Magistrate or a Judicial Member of the Industrial Relations Commission.

The application

7.63 Under the Workplace Video Surveillance Act, detailed information must be provided in an application for a covert surveillance authority. We consider that the level of information required is sufficiently detailed to enable the issuing authority to make an informed determination.

101. Registered Clubs Association of NSW, Submission at 7 and 13.

Recommendation 63

The current provisions governing an application by an employer for a covert surveillance authority should be continued. Accordingly, an application by an employer for a covert surveillance authorisation must be in writing, supported by an affidavit, and contain the following information:

(a) the grounds the employer or employer's representative has for suspecting that a particular employee is or employees are involved in unlawful activity or serious misconduct;

(b) whether other managerial or investigative procedures have been undertaken to detect the unlawful activity or serious misconduct and if so, what was the outcome;

(c) who and what will regularly or ordinarily be in view of the cameras;

(d) the dates and times during which the covert surveillance is proposed to be conducted; and

(e) the licensed security operator who will oversee the conduct of the covert surveillance operation.

The issuing authority should have the power to seek further information.

Granting a covert surveillance authorisation in the employment context

7.64 Section 13(1) of the Workplace Video Surveillance Act specifies that, in order to grant a covert surveillance authority, a Magistrate must be satisfied that the application shows that reasonable grounds exist to justify its issue. We consider that this requirement should be expanded to require that the issuing authority must have regard to the matters listed in the application and be satisfied that the application shows that reasonable grounds exist to justify its issue.

7.65 An additional requirement in the Workplace Video Surveillance Act is that a Magistrate must have regard to whether covert video surveillance of the employee or employees concerned might unduly intrude on their privacy or the privacy of any other person.[102] *In the view of the Commission, such an express direction to consider the privacy implications of any proposed covert surveillance is essential. This is particularly so in respect of the requirement to consider whether the covert surveillance might unduly intrude on the privacy of a third party, as there is the potential concern that placing authorisation responsibility with Industrial Magistrates and Judicial Members of the Industrial Relations Commission would cause the industrial dimension to dominate the consideration process. A matter of particular concern is that a predominantly industrial focus may preclude or minimise consideration of the impact of the surveillance on third parties, such as customers or persons with whom employees communicate. This is certainly a significant concern, as a central reason for addressing the issue of employment surveillance within a general surveillance context is the potential impact on third party privacy interests. The Commission recommends that this concern be addressed by the inclusion of a provision directing the issuing authority to give specific consideration to the privacy interests of third parties when considering applications for a covert surveillance authorisation.*

7.66 We note the recommendation above that when considering an application for a covert surveillance authorisation that will involve surveillance in recreational or meal rooms, the issuing authority must have regard to the employees' heightened expectation of privacy. This requirement should form part of the provisions governing the granting of an authorisation.

Recommendation 64

102. Workplace Video Surveillance Act 1998 (NSW) s 14. As noted above, additional mandatory considerations exist when the proposed surveillance will occur in a recreation room, meal room or any other area at a workplace where employees are not directly engaged in work: Workplace Video Surveillance Act 1998 (NSW) s 13(2).

In determining whether to grant an authorisation to conduct covert surveillance in the employment context, the issuing authority must have regard to:

(a) the matters listed in the application;

(b) the extent to which the privacy of an employee or employees is likely to be affected; and

(c) the extent to which the privacy of a third party or third parties is likely to be affected.

When considering an application by an employer for a covert surveillance authorisation that will involve surveillance in recreational or meal rooms, the issuing authority must have regard to the employees' heightened expectation of privacy.

The issuing authority must be satisfied that the application shows that reasonable grounds exist to justify its issue.

Contents of the authorisation

7.67 Under the Workplace Video Surveillance Act, a covert surveillance authority must specify the purpose for which it authorises the carrying out of the covert video surveillance and the licensed security operator who is to oversee the conduct of the surveillance operation.[103] *The Commission considers that the contents of the authorisation should be more detailed, for the reasons given in respect of warrants for law enforcement officers and public interest authorisations.*[104]

103. Workplace Video Surveillance Act 1998 (NSW) s 15.
104. See ch 5 and 6.

Recommendation 65

An authorisation permitting covert surveillance in the employment context should specify:

- **(a) the purpose for which the authorisation is granted;**
- **(b) the licensed security operator who is to oversee the conduct of the surveillance;**
- **(c) where practicable, the name of any person who is to be the subject of surveillance;**
- **(d) the period (being a period not exceeding 30 days) during which the authorisation may be in force;[105]**
- **(e) that the surveillance device(s) may be repaired, tested, moved, maintained, replaced and/or retrieved during the period that the authorisation is in force;**
- **(f) if practicable, the premises on which the surveillance device(s) are to be installed or used;**
- **(g) the type(s) and number of surveillance device(s) to be used;**
- **(h) any conditions on the use of the surveillance device(s);**
- **(i) any conditions on the use, release or publication of any information obtained as a result of the use of the surveillance device(s);[106] and**
- **(j) the time within which the person authorised to use the surveillance device(s) is required to report to the issuing authority and the Attorney General.[107]**

105. This is consistent with the Commission's recommendation concerning warrants for law enforcement officers in ch 5. It is also the maximum duration permitted under the Workplace Video Surveillance Act 1998 (NSW).

106. See ch 9 regarding the Commission's recommendations on the use of information obtained as a result of covert surveillance.

107. See ch 8 regarding the Commission's recommendations on the reporting requirements for covert surveillance.

Retrospective authorisation

7.68 As with public interest authorisations, authorisation for covert surveillance in the employment context should be obtained prior to its commencement. However, in some circumstances, it may not be possible for an employer to obtain an authorisation before engaging in covert surveillance. For example, an employer may reasonably suspect misconduct such as tampering with machinery, which could pose a health risk to other employees and/or third parties. In such a situation, it would be justifiable to commence surveillance as soon as possible. The Commission considers that such justifiable situations will be rare.

Recommendation 66

Where covert surveillance in an employment context is commenced prior to obtaining authorisation, the employer must apply for authorisation as soon as practicable following the commencement.

An application for retrospective authorisation must specify why covert surveillance was commenced prior to obtaining an authorisation.

8. Accountability for covert surveillance

- Introduction
- Reporting measures for covert surveillance
- Reporting to the Attorney General
- Reporting to the issuing authority
- Record-keeping and inspection
- Annual reporting by the Attorney General
- Notifying the subject of surveillance

INTRODUCTION

8.1 This chapter, and the two following chapters, examine the mechanisms for ensuring that those who conduct covert surveillance activities are accountable for their actions. While the system for warrants or authorisations requires the issuing authority[1] to be satisfied that the proposed use of surveillance devices is justified before granting approval, the mechanisms discussed in this chapter are designed to ensure that accountability is an ongoing process that does not cease once the surveillance is authorised. The accountability mechanisms include requirements for reporting the results of covert surveillance and the need for relevant organisations to keep records of their uses of surveillance and make them available for inspection. The chapter also discusses the Attorney General's obligation to report annually to Parliament, and canvasses the extent to which people are to be notified that they have been the subject of surveillance activity. Chapter 9 discusses the uses that can be made of material gathered by means of surveillance and, in particular, examines the extent to which such information may be used as evidence. Finally, Chapter 10 outlines the offences the new legislation will create, and the civil remedies that will be available to those whose interests have been affected by surveillance activities (whether covert or overt).

REPORTING MEASURES FOR COVERT SURVEILLANCE

8.2 Most surveillance legislation, including the Listening Devices Act 1984 (NSW) ("LDA"), require people who apply for a warrant to conduct surveillance to report the results of that surveillance. Reporting helps to assess the level of compliance with surveillance legislation. Reporting on the results of surveillance can also indicate the effectiveness of the legislation itself by revealing the

1. *The term "issuing authority" is used to refer to the judge who decides applications for warrants and the agency or agencies that will be examining applications for public interest and employment authorisations.*

strengths and defects of the provisions, and can assist in determining whether the appropriate balance is being struck between authorised surveillance and privacy. The LDA currently requires reporting from a number of different sources to a variety of audiences. Agencies conducting surveillance pursuant to a warrant must notify the Attorney General of the intention to apply for a warrant,[2] and also report back to the Attorney General and to an eligible judge on the results of the surveillance.[3] The Attorney General must also be notified when agencies use a listening device without a warrant in an emergency situation (in connection with an imminent threat of serious violence to people, damage to property or a serious narcotics offence).[4] Information concerning the number of warrants sought and granted and any other matter relating to the use of listening devices must be reported by the Attorney General annually to Parliament.[5] The LDA also provides that an eligible judge may require the holder of a warrant to notify the subject of the warrant of details concerning the surveillance.[6]

REPORTING TO THE ATTORNEY GENERAL

Reporting before a warrant has been issued

8.3 The LDA currently requires applicants for a listening device warrant to notify the Attorney General or a prescribed officer of:

- *the offence in respect of which the warrant is sought;*
- *where practicable, the type of listening device to be used;*
- *where practicable, the name of any person whose private conversation will be listened to or recorded;*
- *where practicable, the premises where the device is to be installed or the place it is to be used;*
- *whether an attempt has been made to obtain the information*

2. LDA s 17.
3. LDA s 19.
4. LDA s 5(4).
5. LDA s 23.
6. LDA s 20.

sought by other means;

- *what other means there may be of obtaining the information sought;*
- *the period during which the device is meant to be used;*
- *the name of the person who is to use the device; and*
- *details of any previous warrant sought or granted in respect of the same offence.*[7]

8.4 A warrant is not to be granted unless the applicant satisfies the court that the Attorney General has been notified of these particulars and has had an opportunity to be heard in relation to the granting of the warrant.

8.5 The advance notice requirement has been criticised by agencies who regularly seek warrants on the ground that it is time-consuming and achieves little benefit. The Report of the Royal Commission into the New South Wales Police Service ("Wood Report") recommended that the provision be abolished.[8] *The Wood Report noted that delays can occur in the acceptance of the notices by the Attorney General, which can be critical in cases where there is only a limited time in which to obtain evidence. The Report also questioned the policy behind the requirement that the Attorney be notified before a warrant is granted, particularly in relation to law enforcement agencies, stating that while it is appropriate for warrants to be carefully scrutinised, it is doubtful whether there is a need for both the Attorney General and the eligible judge to approve the issuing of warrants.*[9] *The NSW Police Special Services Group and the joint law enforcement agencies agreed with this view.*[10] *The joint law enforcement agencies suggested that, rather than formally notifying the Attorney General in advance of each application, it may be more appropriate to require the applicant to*

---

7. *LDA s 17.*
8. *New South Wales, Royal Commission into the New South Wales Police Service, Final Report (May 1997) Vol 2 at para 7.99 ("Wood Report").*
9. *Wood Report at para 7.99.*
10. *NSW Police Service, Special Services Group, Submission at 10.*

notify the Attorney only when it appears to the applicant that an issue of legal professional privilege may arise.[11] *On the other hand, the Law Society of New South Wales supported the retention of the requirement to give the Attorney advance notice of a warrant.*[12] *The Law Society noted that the requirement, in practice, gives the Solicitor General or the Crown Advocate the power to review warrant applications.*

8.6 The current requirement in the LDA that the Attorney General be notified and given the opportunity to be heard prior to the issuing of a warrant was included in order to ensure "effective representation of the public interest in requiring responsibility in the use of listening devices."[13] *However, it appears that this provision has had little practical effect as an accountability measure. The degree to which the issuing authority is expected to scrutinise an application for a warrant, or other form of authorisation, is, in the Commission's view, sufficient to ensure that the public interest is considered, and that warrants or authorisations are issued only when necessary. Notifying the Attorney General of an application only serves to slow down the process and add an unnecessary layer of bureaucracy. Accordingly, the Commission recommends that the requirement of prior notice to the Attorney General should not be included in the proposed surveillance legislation, both in relation to applications for warrants and public interest and employment authorisations.*

8.7 There may, however, be instances when the views of the Attorney General on the application may be useful to the issuing authority. For example, as noted above, the joint submission of the law enforcement agencies suggested that it may be appropriate to notify the Attorney General when it appears that an issue of legal professional privilege may arise from the use of the surveillance

---

11. NSW Crime Commission (NSWCC), Independent Commission Against Corruption (ICAC), Police Integrity Commission (PIC) and the National Crime Authority (NCA) ("Joint Law Enforcement Agencies"), Submission at 9.

12. Law Society of NSW, Submission at 9.

13. New South Wales, Parliamentary Debates (Hansard) Legislative Assembly, 17 May 1984 at 1095.

device.[14] *In applications for public interest authorisations, the proposed use of surveillance devices may involve police matters and, in that case, it would be appropriate for the issuing authority to seek the Police Commissioner's views on the application. Accordingly, the issuing authority should be given a discretion to notify the Attorney General or any other appropriate person, such as the Police Commissioner, and to give them the opportunity to be heard on the application.*

Recommendation 67

The proposed Surveillance Act should not require an applicant for a warrant or authorisation to notify the Attorney General of the application, subject to the following:

- **the issuing authority must notify the Attorney General when an application raises an issue of legal professional privilege; and**
- **the issuing authority may notify the Attorney General or any other person of an application, if the issuing authority deems it appropriate to do so in the circumstances.**

Reporting the results of surveillance pursuant to a warrant

8.8 In addition to the requirement to notify the Attorney General prior to the issuing of a warrant, the LDA also contains provisions requiring warrant holders to report the results of surveillance undertaken. A warrant holder must report in writing to the Attorney General and to an eligible judge, within a specified period,[15] *as to whether or not the listening device was used pursuant to the*

14. *Joint Law Enforcement Agencies, Submission at 9.*
15. *Usually within 21 days of the expiry of the warrant: Joint Law Enforcement Agencies, Submission at 9.*

warrant.[16] If the device was used, the report must specify:

- *the name, if known, of any person whose private conversation was recorded or listened to by the use of the device;*
- *the period during which the device was used;*
- *particulars of any premises in which the device was installed or the place where any device was used;*
- *particulars of the general use made or to be made of any evidence or information obtained from the use of the device; and*
- *particulars of any previous use of the device with respect to the same offence.[17]*

8.9 Where such a report is given to a judge, he or she may direct that any record of evidence or information obtained from the use of the device to which the report relates be brought into the court[18] and remain in the custody of the court and, if the court orders, be made available to any person.[19] A person who has requested an extension of time to retrieve a listening device must also furnish to the Attorney General and to an eligible judge a report stating whether or not the device was retrieved, and if not, the reasons why the device has not been retrieved.[20]

8.10 These provisions are designed to promote "efficient monitoring of the use that is made of listening devices."[21] Other listening devices legislation contains similar provisions.[22] The statutes in other Australian states contain various time frames for reporting, ranging from as soon as possible following the

---

16. *LDA s 19(1).*
17. *LDA s 19(1)(b).*
18. *LDA s 19(2). Failure to comply with such a direction incurs a maximum penalty of 20 penalty units, imprisonment for 12 months, or both.*
19. *LDA s 19(3).*
20. *LDA s 19(4). Inserted by the Listening Devices Amendment (Warrants) Act 1998 (NSW).*
21. *New South Wales, Parliamentary Debates (Hansard) Legislative Assembly, 17 May 1984 at 1095.*
22. *Listening Devices Act 1972 (SA) s 6b; Drugs Misuse Act 1986 (Qld) s 29A.*

surveillance[23] *to within three months after the cessation of the warrant.*[24] *At the Commonwealth level, the Telecommunications (Interception) Act 1979 (Cth) ("Interception Act") has comprehensive reporting requirements. Heads of Commonwealth agencies are required to provide the Minister with a copy of each warrant as soon as possible,*[25] *and must report to the Minister within three months of the cessation of an interception warrant, details of the interception, including:*

- *the use made by the agency of the information obtained from the interception;*[26]
- *people to whom that information was communicated outside the agency;*
- *the number of arrests that have been made on the basis of the information; and*
- *an assessment of the usefulness of the information obtained under interception warrants.*[27]

8.11 Heads of Commonwealth agencies must also provide annual reports to the Minister relating to their activities.[28] *Information to be reported includes the total expenditure incurred in connection with executing the interception warrant.*[29] *The Minister may also seek further information needed in connection with the preparation of an annual report to Parliament.*[30]

8.12 The Commission considers that reporting to the Attorney

---

23. Drugs Misuse Act 1986 (Qld) s 29A.
24. Listening Devices Act 1991 (Tas) s 19. Other time frames include monthly: Listening Devices Act 1972 (SA) s 6b; within the time specified in the warrant: Surveillance Devices Act 1999 (Vic) s 20(1).
25. Telecommunications (Interception) Act 1979 (Cth) s 94(1).
26. The Director General of the Australian Security Intelligence Organisation (ASIO) must also report to the Attorney General on the extent to which the interception assisted ASIO to carry out its functions: Telecommunications (Interception) Act 1979 (Cth) s 17.
27. Telecommunications (Interception) Act 1979 (Cth) s 94(2).
28. Telecommunications (Interception) Act 1979 (Cth) s 94(3).
29. Telecommunications (Interception) Act 1979 (Cth) s 94(3A).
30. Telecommunications (Interception) Act 1979 (Cth) s 95(1).

General on the results of surveillance conducted under a warrant is a crucial element in ensuring accountability. It can also provide information on how the legislation is working in practice, drawing attention to areas where the law is not being complied with, or where privacy rights are most vulnerable. The information provided to the Attorney General also assists him or her prepare the annual report to Parliament. The Commission recommends that the new surveillance legislation contain a range of reporting requirements broader than those in the LDA. In addition to the current reporting requirements detailed at paragraph 8.8, warrant applicants should have to report to the Attorney General in relation to each warrant on:

- *the type of surveillance device used;*
- *details of any conditions placed by the court on the exercise of the warrant and whether or not those conditions were complied with;*
- *the number of, and reasons for, any warrant renewals;*
- *whether the device was retrieved and, if not, the reasons why it was not retrieved; and*
- *any other information requested by the Attorney General which the warrant holder can reasonably provide.*

8.13 The Joint Law Enforcement Agencies' submission expressed the view that some of these requirements are too stringent and may jeopardise the security of surveillance operations. In particular, they objected to the requirement to name the premises or place where the device was used, arguing that the benefits of revealing such information are unclear, whereas the disadvantages in unveiling investigative techniques may be considerable.[31] The New South Wales Police Special Services Group also objected to providing information concerning the cost of executing the warrants, noting that it would be impossible to provide such information without a huge commitment of resources.[32] The joint law enforcement agencies noted that, since the time for reporting

---

31. NSW Police Service, Special Services Group, Submission at 10; Joint Law Enforcement Agencies, Submission at 9.

32. NSW Police Service, Special Services Group, Submission at 10.

specified in each warrant is usually 21 days after the expiration of the warrant, it is often very difficult to provide accurate details of how information obtained from surveillance has been used, or of arrests and charges, as the investigations are in many cases ongoing.[33]

8.14 The reporting provisions are not intended to prejudice ongoing investigations or impending trials. The information is intended to promote accountability and compliance with the law, as well as indicating the nature of surveillance being undertaken and its relative usefulness. For example, details of the general use of information obtained from surveillance, such as the number and type of cases in which it has been used as evidence and/or resulted in prosecutions, is an important way to assess the balance between the public benefit of surveillance as a law enforcement tool and the interests of privacy. This assessment is also assisted through information on the amount of money (in most cases, public money) that is spent on conducting surveillance. Information on the nature of the premises where surveillance devices are used, and the people to whom the information obtained from the use of such devices is communicated, can serve to alert parliament to any improvements in flexibility or increased privacy protections that may need to be introduced into the legislation.

8.15 The requirement to report to the Attorney General on the results of the execution of the warrant should also apply to holders of public interest authorisations and employment authorisations. The same information which is required of warrant holders should also be included, to the extent applicable, in the reports of holders of authorisations.

---

33. NSW Police Service, Special Services Group, Submission at 10; Joint Law Enforcement Agencies, Submission at 9.

Recommendation 68

The proposed Surveillance Act should require every holder of a warrant or public interest authorisation or employment authorisation to make a report in writing to the Attorney General stating whether or not the surveillance device was used pursuant to the warrant or authorisation. The report should be made within the period specified in the warrant or authorisation, with provision for the Attorney General to approve an extension. If the surveillance device was used, the report should include the following information:

(a) the name, if known, of any person whose private conversation or activity was recorded by the use of the surveillance device;

(b) the period during which the surveillance device was used;

(c) particulars of the types of premises in which the surveillance device was installed or the place where any device was used;

(d) particulars of the general use made or to be made of any evidence or information obtained from the use of the device;

(e) particulars of any previous use of a surveillance device with respect to the same offence or activity subject of the warrant or authorisation;

(f) the type of surveillance device(s) used;

(g) details of any conditions placed by the issuing authority on the exercise of the warrant or authorisation and whether or not those conditions were complied with;

(h) the number of, and reasons for, any warrant or authorisation renewals;

(i) whether the device was retrieved and, if not, the reasons why it was not retrieved; and

(j) any other information requested by the Attorney General.

In the case of surveillance conducted pursuant to a retrospective warrant or authorisation, the report should include, in addition to all the information specified above, information containing the particulars of the circumstances on which a retrospective warrant or authorisation application was based.

Failure to comply with these requirements should constitute an offence.

REPORTING TO THE ISSUING AUTHORITY

8.16 In addition to the information that must be provided to the Attorney General, the LDA requires warrant holders to provide to the eligible judge information concerning the people and places subjected to surveillance under a warrant, the general uses to which the information obtained has been or is intended to be put, the duration of the surveillance and details of past warrants issued in relation to the same offence.[34] *The Commission sees this provision as being an important check on surveillance conducted under a warrant. The information available to the eligible judge will include a record of the number of warrant applications and renewal requests received, granted or refused, reasons for any refusals, and the information contained in the affidavit supporting each warrant application.*[35] *This information could be checked against the reports from warrant holders of the results of the surveillance to see if any discrepancies occur. The issuing authority should record and forward such information, including details of any discrepancies*

34. *LDA s 19(1).*
35. *If the Commission's recommendation to remove the requirement that the Attorney General be notified of warrant applications prior to the warrant being granted is implemented (see Recommendation 67), there is no reason why the Attorney General would have access to information contained in an affidavit supporting a warrant application.*

between what was asked for and granted in a warrant and what actually occurred, to the Attorney General on an annual basis. As a further accountability measure, the Attorney General could verify that the information supplied by the eligible judge corresponds with that supplied directly by the warrant holders. Accordingly, the Commission is of the view that the proposed surveillance legislation should continue to require warrant holders to report the results of surveillance conducted pursuant to the warrant to the eligible judge who issued the warrant. Similarly, a holder of a public interest or employment authorisation should be required to report to the issuing authority.

Recommendation 69

The proposed Surveillance Act should require holders of warrants or public interest authorisations or employment authorisations to report to the issuing authority within the period specified in the warrant or authorisation, with provision for the issuing authority to approve an extension. The report should contain the same information required in the report to the Attorney General. Failure to comply with this requirement should constitute an offence.

Recommendation 70

The proposed Surveillance Act should provide that the registry of the issuing authority should forward annually to the Attorney General such information about applications for warrants or authorisations as it deems appropriate, including:

(a) the number of applications received, granted or refused, and the reasons for refusal;

(b) the number of renewal applications received, granted or refused, and the reasons for refusal;

(c) the number of retrospective warrants granted or refused, and the reasons for refusal; and

(d) any discrepancies the court may have noticed between the affidavit supporting a warrant application and the information provided by the warrant holder concerning the results of the surveillance.

Recommendation 71

The proposed Surveillance Act should provide that the issuing authority:

- **may direct that any record of evidence or information obtained by the use of the surveillance device to which the report relates be brought before it;**
- **may keep such record in its custody; and**
- **may make an order that the evidence or information may be made available to such persons or organisations as the issuing authority directs.**

RECORD-KEEPING AND INSPECTION

8.17 The reporting requirements discussed above focus mainly on the proper execution of warrants or authorisations for particular surveillance operations. However, the execution of warrants and authorisations is only a part of the accountability measures the Commission considers necessary. This chapter and Chapter 9 deal with the regulation of the communication or publication of surveillance information, its use as evidence in court proceedings, its storage, security and destruction, and notification given to surveillance subjects in certain circumstances. The Commission also recommends that compliance with these requirements be monitored. The Commission accepts the Ombudsman's submission

that there is a need for external monitoring of compliance by the relevant agencies with the proposed surveillance legislation.[36]

8.18 The Interception Act contains an effective system of monitoring compliance with its provisions. The Act requires the relevant Commonwealth agencies, namely the Australian Federal Police and the National Crime Authority, to maintain records of the telecommunications warrants issued to them and details about dealings with them, such as particulars of each use of the telecommunications information, communications of the information made to persons other than an officer or staff members of the agency and particulars of the use of information in legal proceedings.[37] *Complementing the record-keeping requirements is the grant of powers to the Commonwealth Ombudsman to inspect the relevant agencies' records and to report to the responsible Minister the results of the inspections, including any breach of the Interception Act by an officer of an agency.*[38] *The record keeping and inspection provisions in the Interception Act are mirrored in the Telecommunications (Interception) (New South Wales) Act 1987 (NSW). Under the New South Wales Act, an eligible authority, which is defined as the Police Force of the State, the State Drug Crime Commission, the Independent Commission Against Corruption, the Police Integrity Commission or the Police Royal Commission, must keep records pertaining to telecommunications interceptions and the State Ombudsman has a comparable power to inspect these records to determine compliance with the requirements of the Interception Act.*

8.19 The Commission has formed the view that the record-keeping and inspection requirements contained in the Telecommunications (Interception) (New South Wales) Act 1987 (NSW) should be adopted in the proposed surveillance legislation. It is a system which has proved to be effective. Inspections have indicated a high level of

---

36. The Commission discusses the views of the Ombudsman in this respect and makes recommendations concerning review procedures under the new legislation at para 8.19-8.22.

37. Telecommunications (Interception) Act 1979 (Cth) s 80-81C.

38. Telecommunications (Interception) Act 1979 (Cth) s 82(b), 84 and 85.

compliance with statutory requirements.[39] *The law enforcement agencies in New South Wales have, for some time now, maintained records of documents and information pertaining to the telecommunications surveillance they conduct and have also complied with the independent audit of these records. These agencies should not have any major practical or policy difficulties with the extension of this system to surveillance activities where surveillance devices other than telephone interception devices are used.*

8.20 The Barrett Review recommended that the Australian Privacy Commissioner should exercise the inspection and reporting functions currently conferred on the Ombudsman under the Interception Act. The Review observed that the accent should be on the protection of privacy rather than simply being an audit of administrative processes.[40] *It may be argued that inspection of covert surveillance operations from the perspective of privacy concerns is required to balance the weight of law enforcement interests that drive those operations. Furthermore, since the Commission proposes a pivotal role for the Privacy Commissioner in the regulation of the overt use of surveillance devices,*[41] *it seems consistent that he or she should have a similar monitoring role in the counterpart regime for the covert use of these devices.*

8.21 On the other hand, there are good reasons for the inspection/monitoring function to be conferred on the Ombudsman. First, the Ombudsman already has the auditing experience in relation to telecommunications interception. Secondly, the familiarity of law enforcement agencies with existing auditing procedures involving the Ombudsman may mean a smoother transition to the new regulatory regime applying to surveillance

---

39. P J Barrett, Telecommunications interception review: review of the longer term cost-effectiveness of telecommunications interception arrangements under section 332R of the Telecommunications Act 1997 (Australian Telecommunications Authority, Canberra, 1999) at para 4.2.11; P Ford, Telecommunication Interceptions Policy Review (Australia, Attorney General's Department, Information and Security Law Division, 1999) at para 4.1.10.

40. Barrett at para 4.2.14.

41. See ch 4 and 10.

devices. Thirdly, granting the Ombudsman this function would enable him or her to make useful comparisons between the use of surveillance devices and telecommunications interceptions.[42] *While the Barrett Review recommended the transfer of the monitoring role from the Ombudsman to the Privacy Commissioner, the Ford Review recommended maintaining the status quo.*[43] *However, the Ford Review was also of the opinion that it is for the individual State to decide which agency should inspect the records of State law enforcement agencies.*

8.22 The Commission does not have a strong view as to whether the role of inspecting records of the relevant organisations and reporting breaches of the proposed surveillance legislation should be that of the Ombudsman or the Privacy Commissioner, seeing the merit in each approach.

Recommendation 72

The proposed Surveillance Act should provide that all law enforcement agencies, private individuals and organisations authorised to apply for either warrants or authorisations, should keep records pertaining to the use of surveillance devices. The records should include:

(a) each application for warrants or authorisations;

(b) a statement as to the result of the application;

(c) the warrant or authorisation issued to the person or organisation;

(d) copies of the reports on the warrant to the Attorney General and to the issuing authority;

(e) particulars of each use by the person or organisation of the information obtained by the use of a surveillance device(s);

42. NSW Ombudsman, Submission at 3.

43. Ford at para 26, 4.1.

(f) particulars of each occasion when the information was communicated to a person or organisation, not being a warrant-holder or authorisation-holder;

(g) particulars of each occasion when, to the knowledge of the person or an officer of the agency or organisation, the information was given in evidence in legal proceedings;

(h) details of instances when the activities of persons other than those named in warrants or authorisations were recorded;

(i) particulars of all cases when surveillance devices were used without a warrant or authorisation, including details of the subjects, dates, times and places of the surveillance, the persons who used the devices and the reasons for their use;

(j) particulars of persons whose private activities were monitored or recorded by the use of surveillance devices, but against whom no criminal proceedings had been instituted or were likely to be instituted; and

(k) particulars of the destruction of the information in compliance with the provisions concerning destruction.

Recommendation 73

The proposed Surveillance Act should provide that the inspecting authority (the Privacy Commissioner or Ombudsman) should be required to:

(a) inspect the records of the relevant law enforcement agencies and private individuals or organisations for the purpose of ascertaining:

- **the accuracy of the entries in the records;**

- **the extent of compliance with the requirements of the proposed surveillance legislation including, but not limited to, those concerning the use, communication or publication of surveillance information, storage and security of information, destruction of information; and**
- **whether notice should be given to a subject of the surveillance;**

(b) report to the Attorney General about the result of inspections; and

(c) do anything incidental or instrumental to the performance of any of the preceding functions.

Recommendation 74

The proposed Surveillance Act should provide that the inspecting authority may, at any time, inspect the records of the relevant agencies, organisations or individuals to ascertain compliance with the proposed Surveillance Act. The inspecting authority should inspect records of law enforcement agencies at least once during each financial year.

Recommendation 75

The proposed Surveillance Act should provide that the inspecting authority may, at any time, report the results of the inspection to the Attorney General and shall do so at least once a year and whenever requested to do so by the Attorney General.

Recommendation 76

The proposed Surveillance Act should give the inspecting authority the power to:

(a) enter, at any reasonable time, premises occupied by any relevant agency, organisation or individual, provided reasonable notice is given;

(b) have full and free access, at reasonable times, to their records;

(c) make copies of, and take extracts from, their records; and

(d) require any person to give such information as the inspecting authority considers relevant to the inspection.

Recommendation 77

The proposed Surveillance Act should provide that the communication of surveillance information:

- **to the inspecting authority for purposes of inspection of records; and**
- **by the inspecting authority to the Attorney General for purposes of complying with the reporting requirements**

should be exempted from the general prohibition on the communication or publication of surveillance information. The inspecting authority should ensure that the privacy of individuals to whom the surveillance information relates be respected at all times.

Recommendation 78

The office of the inspecting authority should be given sufficient resources to enable it to discharge effectively its duties under the proposed Surveillance Act.

ANNUAL REPORTING BY THE ATTORNEY GENERAL

Reporting requirements in the LDA

8.23 The LDA requires the Attorney General to annually report to Parliament on the number of warrants sought, the number of warrants granted and on other relevant matters.[44] Once tabled in Parliament, the report becomes a public document and serves an important accountability function, as it facilitates public access to information concerning the occurrence and effectiveness of surveillance. The most recent report tabled by the Attorney is the 1998 Annual Report.[45] This report contained information on:

- *the overall number of applications received by the Supreme Court;[46]*
- *the organisations that requested the warrants;[47]*
- *the number of warrant applications withdrawn;[48]*
- *the number of warrants refused;[49]*
- *the instances when there was use of a listening device, without a warrant, pursuant to section 5(2)(c)(i) of the LDA to obtain evidence in connection with imminent threats of serious violence to persons or of substantial damage to property,[50] or pursuant to section 5(2)(c)(ii) of the LDA to obtain evidence in connection*

---

44. LDA s 23.

45. New South Wales, Attorney General, Report Pursuant to Section 23 of the Listening Devices Act 1984 for the year ended 31st December 1998 (Government Printer, Sydney, 1999).

46. There were 911 applications seeking a total of 1,555 warrants for the use of listening devices in 1998.

47. The following agencies applied for warrants in 1998: NSW Police Service (758); NSW Crime Commission (476); Police Integrity Commission (239); ICAC (58); National Crime Commission (24).

48. 53 applications were withdrawn.

49. Only 1 was refused.

50. None was recorded. However, it is significant to note that the NSW Police Service lodged 5 applications for warrants in connection with investigations into imminent threats to violence to persons or substantial damage to property. This suggests that there is no need for the legislation to authorise warrantless use of surveillance devices in those circumstances.

with serious drug offences;[51]

- *the number of warrants in respect of which the device was not used or was ineffective;*[52]
- *instances when a warrant was applied for to retrieve a device;*[53]
- *the number of warrants in respect of which information was obtained that led to the arrest and prosecution of offenders;*[54] *and*
- *the number of times when members of the public used listening devices.*[55]

8.24 The information provided in the New South Wales report is scant compared with the information provided in the annual reports of the use of surveillance devices in other jurisdictions.[56] *This is not necessarily a result of the requirements in the LDA itself. The report by the Attorney General can include "appropriate*

---

51. None was recorded.

52. In respect of 649 warrants, the listening device was either not used or ineffective.

53. The NSW Police Service sought 1 retrieval order while the NSW Crime Commission obtained 23 retrieval orders relating to 6 original warrants.

54. In respect of 288 warrants, evidence was obtained which led to the arrest and prosecution of offenders. 40% of the total number of warrants were used in respect of serious drug offences.

55. Three instances were reported, all without the benefit of a warrant. These were reported pursuant to the LDA s 5(4) which requires any person who uses a listening device without a warrant to notify the Attorney General immediately and to subsequently submit a report to the Attorney of the details of such use.

56. See, for example, Australia, Attorney General's Department, Telecommunication Interception Act 1979 Report for year ending 30 June 1998 «http://law.gov.au/publications/interact/welcome.html»; Canada, Solicitor General, Annual Report on the Use of Electronic Surveillance as Required Under Subsection 195 of the Criminal Code 1985 (1996-1997) «http://www.sgc.gc.ca/epub/pol/eESurveillance AR96/eESurveillanceAR96.htm»; Administrative Office of the United States Courts, 1998 Wiretap Report «http://www.uscourts.gov/wiretap98/contents.html».

information" relating to the use of listening devices and the administration of the LDA.[57] *It should also be noted that the statistics provided in the annual report are given in isolation, there being no comparison made with previous years. The types of offences for which warrants were obtained are only identified in respect of those obtained under section 5(2)(c) and there is no general assessment on the success or otherwise of the legislation.*

Reporting provisions in comparable legislation

8.25 South Australia, Tasmania, Victoria, Western Australia and the Northern Territory all require annual reports in respect of their listening or surveillance devices legislation. At a Federal level, the Interception Act contains annual reporting provisions.[58] *Certain overseas jurisdictions have legislation containing fairly comprehensive reporting requirements with respect to electronic surveillance and wiretapping. For example, in the United States, the Administrative Office of the US Courts must report annually to Congress on Federal and State applications for orders authorising or approving the interception of wire, oral, or electronic communications.*[59] *In Canada, the Solicitor General must report to Parliament,*[60] *as must the Attorneys General of each province regarding offences within provincial jurisdiction.*[61]

8.26 In addition to similar requirements as those contained in the LDA, some jurisdictions require information about:

- *the number of warrant applications seeking entry to premises;*[62]
- *a description of the locations where the surveillance was*

57. LDA s 23.
58. Telecommunications (Interception) Act 1979 (Cth) Pt IX.
59. Title 18, United States Code (1948) ("18 USC") s 2519(3). This report is also known as the Wiretap Report.
60. See for example Canada, Department of Justice, 1994 Annual Report on the Use of Electronic Surveillance as Required Under Subsection 195(1) of the Criminal Code 1985.
61. Criminal Code 1985 (Can) s 195(4).
62. Listening Devices Act 1972 (SA) s 6b; Telecommunications (Interception) Act 1979 (Cth) s 100(1)(d).

authorised to take place;[63]

- *the number of warrants issued which specify conditions;*[64] *the average duration of warrants;*[65]
- *the approximate number of people whose communications were intercepted;*[66]
- *the breakdown of the number of intercepts by the type of surveillance device used;*[67]
- *the categories of offences for which warrants were issued;*[68] *the number of people not identified in the warrant but whose alleged commission of an offence became known as a result of an authorised intercept;*[69]
- *a general assessment of the importance of interceptions with respect to the investigation, detection, prosecution and prevention of crime;*[70]
- *the cost of executing the warrants;*[71] *and*
- *where notification of the subject of the warrant is required by law, the number of notifications that were made.*[72]

Submissions and response

8.27 In Issues Paper 12 ("IP 12"), the Commission suggested that

63. *Criminal Code 1985 (Can) s 195; 18 USC s 2519.*
64. *Telecommunications (Interception) Act 1979 (Cth) s 100(1)(e); Criminal Code 1985 (Can) s 195.*
65. *Listening Devices Act 1972 (SA) s 6b; Surveillance Devices Act 2000 (NT) s 49; Telecommunications (Interception) Act 1979 (Cth) s 101; Criminal Code 1985 (Can) s 195; 18 USC s 2519.*
66. *18 USC s 2519.*
67. *Criminal Code 1985 (Can) s 195; 18 USC s 2519.*
68. *Telecommunications (Interception) Act 1979 (Cth) s 100(1)(f); Criminal Code 1985 (Can) s 195; 18 USC s 2519.*
69. *Criminal Code 1985 (Can) s 195.*
70. *Criminal Code 1985 (Can) s 195; 18 USC s 2519.*
71. *Telecommunications (Interception) Act 1979 (Cth) s 103; 18 USC s 2519.*
72. *Criminal Code 1985 (Can) s 195.*

the law should require comprehensive reporting and that more information be included in an annual report.[73]

8.28 A number of submissions favoured strengthening the annual reporting requirements. The New South Wales Ombudsman was of the view that the existing situation "frequently seems to result in the tabling of data that imports little".[74] *The Senior Public Defender considered that the report should contain more extensive and useful information.*[75] *Other submissions supported the Commission's suggestions as being important to assist in the public monitoring of the extent and effectiveness of surveillance, but were of the view that details of warrant applicants and subjects should be restricted to organisations and should not reveal the identity of individuals.*[76]

8.29 A number of submissions considered that the Commission's

---

73. The Commission suggested the following information be included in the report:
- *the number of applications for warrants that were made and by whom they were made;*
- *the number of applications for warrants that were refused;*
- *the number of applications for warrants that were granted, and the result of the use of the information obtained pursuant to those warrants, for example the number of arrests and number of prosecutions;*
- *the type of offence involved in each application;*
- *the period of time the warrant was in force (or the average period);*
- *the number of warrants that had to be renewed;*
- *the number and type of place for which the warrant authorises a listening device to be planted, that is, residential premises, commercial premises, vehicles;*
- *the number of directions made by the court to inform the subject of the surveillance;*
- *any changes to the legislation during the year in review;*
- *any general comments on the operation of the legislation;*
- *comparative statistics from previous years; and*
- *cost of the execution of warrants.*

74. NSW Ombudsman, Submission at 2.

75. M L Sides, Submission at 15.

76. Price Waterhouse, Submission at 11; NSW Council for Civil Liberties, Submission at 5.

suggestions did not go far enough, and advocated introducing provisions similar to those in the Interception Act and in the Canadian and United States legislation.[77] The Ombudsman noted that it was anomalous that the Interception Act contained more stringent reporting requirements than the LDA, since most people would regard a telephone "tap" as being less intrusive than a listening device.[78] Other submissions commented that there should be information given on the type of agencies who apply for warrants,[79] the offences in relation to which warrants are sought,[80] the number of warrant requests refused and the reasons for the refusal[81] and the cost of surveillance.[82] Other suggested inclusions in the annual report were a general description of the surveillance undertaken,[83] the number of devices not removed,[84] and the number of subjects of surveillance who had been notified as required under the LDA.[85] Additionally, some submissions argued that the number of prosecutions and convictions in which surveillance evidence was used should be publicly reported, including any challenges to such evidence, changes in the offence for which a person was convicted and the offence in relation to which the warrant was sought, and the number of prosecutions for breaches of the surveillance legislation, should be publicly reported.[86] The Privacy Committee also suggested that the report should include comparative statistics for at least the previous three years, and should be required to be

77. *NSW Ombudsman, Submission at 2; Law Society of NSW, Submission at 5.*
78. *NSW Ombudsman, Submission at 2.*
79. *NSW Young Lawyers Criminal Law Committee, Submission at 6; Law Society of NSW, Submission at 5.*
80. *NSW Young Lawyers Criminal Law Committee, Submission at 6.*
81. *NSW Young Lawyers Criminal Law Committee, Submission at 6.*
82. *NSW Young Lawyers Criminal Law Committee, Submission at 6; Law Society of NSW, Submission at 5.*
83. *Law Society of NSW, Submission at 5.*
84. *Privacy Committee of NSW, Submission at 26.*
85. *NSW Young Lawyers Criminal Law Committee, Submission at 6; Privacy Committee of NSW, Submission at 26; Law Society of NSW, Submission at 5.*
86. *Privacy Committee of NSW, Submission at 27; Law Society of NSW, Submission at 5.*

tabled within a specific period following the completion of the reporting period.[87] *The Commission's recommendation below reflects some of the suggestions in the submissions.*

8.30 While agreeing with most of the Commission's suggestions for additional reporting requirements, the New South Wales Police Special Services Group and the Joint Law Enforcement Agencies objected to three matters.[88] *First, they argued that revealing the number and type of places where devices are located is damaging to operational methodology. Secondly, they objected to the inclusion of information about the cost of the use of surveillance devices. Thirdly, they submitted that information concerning arrests and prosecutions resulting from surveillance evidence may be inaccurate if reported annually due to time delays in matters going before the courts.*

8.31 In relation to the issue of reporting locations of surveillance operations, it may be argued that an awareness by the public that surveillance devices may be used in certain types of premises may in fact deter the commission of offences in such places. Information about the types of places where these devices are used covertly may be useful in assessing the impact of these sorts of operations in specific locations. In relation to the issue of cost of the execution warrants, the Commission recognises that it may not be practical to include this information in the report that the holder of a warrant or authorisation is required to make to the Attorney General and to the issuing authority. It may be difficult to quantify such costs each time a covert operation is made, given the usually short period of time in which the report is required to be made. Hence, in the recommendations concerning the reporting to the Attorney General and to the issuing authority, the Commission has not recommended that the warrant holder be required to include the cost of the use of the device. However, the Commission considers it important that the various law enforcement agencies give information, through the annual report of the Attorney General, about the annual cost of the use of surveillance devices. This will be useful in weighing, among

87. *Privacy Committee of NSW, Submission at 27.*
88. *NSW Police Service, Special Services Group, Submission at 10; Joint Law Enforcement Agencies, Submission at 9.*

other things, the costs and benefits of using such methods of investigation and policing. Finally, the concern regarding the accuracy of statistics can be addressed simply by explaining in the annual report that some of the arrests and prosecutions in a particular year relate to warrants issued in another year.

Conclusion

8.32 Public reporting of the results of the use of covert surveillance is a vital element in achieving accountability. It will only be truly effective as an accountability measure, however, if the legislation requires comprehensive reporting to Parliament. The same issues about the content of annual reports have been raised in several reviews of the Interception Act.[89] During the course of those reviews, suggestions similar to those discussed above were made with a view to strengthening the reporting requirements in the Interception Act. Many of those suggestions have been adopted in amendments to the Interception Act.[90]

The Barrett Review rejected calls from the Privacy Committee and the New South Wales Council for Civil Liberties to include information such as the nature and frequency of incriminating and other intercepts and the approximate number of people whose communications were intercepted.[91] The Privacy Committee argued that similar material is contained in United States Wiretap reports and that, without such information being publicly available here, Australians are in a poor position to assess the effectiveness of

89. *See Australian Law Reform Commission, Privacy (Report 22, 1983); Australia, Attorney General's Department, 1991 Annual Review of Telecommunications (Interception) Act 1979; P J Barrett, Telecommunications interception review: review of the longer term cost-effectiveness of telecommunications interception arrangements under section 332R of the Telecommunications Act 1997 (Australian Telecommunications Authority, Canberra, 1999).*
90. *For example, the Telecommunications (Interception) Act 1979 (Cth) was amended following the Barrett Review to introduce provisions requiring information concerning the cost of interceptions per warrant, and the proportion of warrants issued which yield information used in the prosecution of an offence.*
91. *Barrett at 66-67.*

surveillance. The Barrett Review noted that while such information would be of interest, it would require resource-intensive monitoring and would have little impact on balancing the right to privacy with the community interest in effective law enforcement or cost effectiveness.[92]

8.33 The aim of an accountability regime should be to provide a method to check that such a balance between effective surveillance and privacy is being achieved. In determining what sort of information should be reported, the difficulty in obtaining and providing the information must be weighed against the usefulness and benefit of having the information publicly available. The Commission is of the view that the proposed surveillance legislation should require more information to be reported than is currently required under the LDA. In the recommendation below, the Commission lists the matters that the proposed surveillance legislation should require be addressed in the annual report. Some of those matters are already contained in the LDA annual report. Others are drawn from the surveillance legislation of other jurisdictions and from suggestions in the submissions. While the recommended reporting requirements may seem onerous, all of the information will be available to the Attorney General from the reports provided to him or her by each holder of a warrant or authorisation, by the issuing authority and by the inspecting authority. The Commission considers that the information required in the recommendation below should facilitate an assessment of the level of compliance with the surveillance legislation and give an indication of whether the legislation is operating efficiently and effectively. The information should be reported in a way which does not identify any individuals who conducted, were the subject of, or may be named in information obtained as a result of, surveillance.

Recommendation 79

The proposed Surveillance Act should require the Attorney General to include, whenever possible, the

92. Barrett at 66-67.

following information in the annual report to Parliament:

with respect to warrants for the use of surveillance devices:

(a) the total number of applications for warrants, including the number of radio, telephone, facsimile or other electronic applications, which organisations made the requests and the number of applications that were granted, refused or withdrawn;

(b) the number of applications for retrospective warrants, by whom they were made and the number of those that were granted, refused or withdrawn;

(c) the number and type of offences for which warrants were issued, and the number of warrants issued for each type of offence;

(d) the number of each type of surveillance device used;

(e) the average period of time each warrant was in force;

(f) the number of renewal applications received, granted, refused or withdrawn;

(g) the number of warrants authorising the installation of devices in premises, an indication of the type of premises where devices were installed and the number of warrants authorising surveillance of a particular individual;

(h) the number of warrant applications requesting entry to premises and the number of warrants granted, refused or withdrawn;

(i) the number of warrants issued specifying conditions or restrictions and the type of conditions or restrictions applied;

(j) the number of devices not removed following the completion of surveillance and the reasons why

the devices were not removed;

(k) the general use to which information obtained pursuant to surveillance devices has been put, including the number of arrests, prosecutions and convictions in which the information was used; and

(l) the annual cost of the covert use of surveillance devices by the different law enforcement agencies;

with respect to public interest authorisations for the use of surveillance devices:

(a) the total number of applications for public interest authorisations, including the number of radio, telephone, facsimile and other electronic applications, the types of organisations that made the requests and the number of applications that were granted, refused or withdrawn;

(b) the number of applications for retrospective authorisations and the number of those that were granted, refused or withdrawn;

(c) the number of each type of surveillance device used;

(d) the average period of time each authorisation was in force;

(e) the number of renewal applications received, granted, refused or withdrawn;

(f) the number of authorisations issued specifying conditions or restrictions, and the type of conditions or restrictions applied;

(g) the number of devices not removed following the completion of surveillance and the reasons why the devices were not removed; and

(h) the general use to which information obtained pursuant to the surveillance has been put;

with respect to employment authorisations for the use of surveillance devices:

(a) the total number of applications for employment authorisations, including the number of radio, telephone, facsimile and other electronic applications and the number of applications that were granted, refused or withdrawn;

(b) the number of applications for retrospective authorisations and the number of those that were granted, refused or withdrawn;

(c) the number of each type of surveillance device used;

(d) the average period of time each authorisation was in force;

(e) the number of renewal applications received, granted, refused or withdrawn;

(f) the number of authorisations issued specifying conditions or restrictions, and the type of conditions or restrictions applied;

(g) the number of devices not removed following the completion of surveillance and the reasons why the devices were not removed; and

(h) the general use to which information obtained pursuant to the surveillance has been put; and

generally:

(i) the extent of compliance with the requirements of the proposed Surveillance Act including, but not limited to, those concerning the keeping and inspection of records, the use, communication or publication of surveillance information, storage and security of information and destruction of information;

(j) the number of notifications to the subject of the surveillance;

(k) a general account of the extent to which "incidental" information is obtained and used, including, for example, information relating to the commission of an offence by a person not identified in the warrant or authorisation was obtained as a result of the authorised use of a surveillance device;

(l) details of breaches of the proposed Surveillance Act, including actions taken, such as criminal, civil or disciplinary proceedings;

(m) any changes to the proposed Surveillance Act during the year in review;

(n) comparative statistics from previous years; and

(o) any general comments on the operation of the proposed Surveillance Act.

NOTIFYING THE SUBJECT OF SURVEILLANCE

The current law

8.34 The LDA currently provides that an eligible judge may direct a person who has used a listening device pursuant to a warrant to supply information to the subject of the surveillance, within a period specified by the judge, concerning the warrant and the use of

the device,[93] where the judge is satisfied that, having regard to the information obtained from the use of the device and to any other matter, the use of the device was not justified and was an unnecessary interference with the privacy of the person concerned.[94] The warrant-holder must comply with the direction, or face a penalty, but has an opportunity to be heard before a direction to notify the subject is made.[95] This provision was included in the legislation as an important safeguard against the unjustified invasion of privacy that may be occasioned by the use of listening devices. It was intended to make persons who may be the victims of improper activity aware of what has been done to them.[96] The Commission is unaware of any case where this discretion has been exercised.

8.35 The provision is based on the assumption that the eligible judge monitors the conduct of covert surveillance to ensure that it occurs in accordance with the warrant, and that he or she initiates action where a breach occurs. However, it may be argued that it is not the role of eligible judges to conduct systematic monitoring of compliance with warrants. This perhaps explains why no notification directions have been made under section 20 of the LDA.

Alternative approaches

Mandatory notice requirement

8.36 In Canada and the USA, it is mandatory to give notice to the subject of the surveillance. The legislation in Canada requires notice to the subject within 90 days after the warrant was authorised or renewed. After the notice is given, the person who gave the notice must certify to the court which approved the authorisation that the notice has been given. The time frame for giving notice may be suspended where the Attorney General or the Solicitor General applies to the court for an extension on the

93. LDA s 20(1).
94. LDA s 20(2).
95. LDA s 20(3) and 20(4).
96. New South Wales, Parliamentary Debates (Hansard) Legislative Assembly, 17 May 1984 at 1096.

grounds that an investigation is continuing and notification of the subject would prejudice the interests of justice. The judge may grant an extension of a period up to three years.[97] It has been ruled that the notice requirement is complied with merely by notifying the person that he or she was the object of an interception. The person has no right to any wider notification such as receipt of a copy of the authorisation.[98] The Law Reform Commission of Canada recommended that the notice should include the dates of the interceptions and a copy of the authorisation,[99] but this has not been implemented in legislation.

8.37 The United States legislation has a mandatory notice requirement in cases where an interception was made in an emergency situation.[100] The law requires the subject of the surveillance to be notified within 90 days of the cessation of a warrant, or, if the warrant application was unsuccessful, 90 days from the date of the application, unless the court sanctions a delay. The content of the notification is broader than that found in the Canadian provision; it must include the fact that the person was the subject of an application for a warrant, the date and period of authorised, approved or disapproved interception, or the denial of the application, and that during that period, communications were or were not intercepted.[101]

8.38 The fundamental argument for mandatory notice is that individuals have the right to know that their privacy has been invaded. Intrusions into privacy should only be in accordance with that permitted by law. The person whose privacy has been invaded should be made aware of the surveillance to allow him or her to challenge its legality and to obtain redress if a breach of the

---

97. Criminal Code 1985 (Can) s 196.

98. Re Zaduk (1978) 38 CCC (2d) 349.

99. Canada, Law Reform Commission, Electronic Surveillance (Working Paper 47, 1986) at 90-93.

100. 18 USC s 2518(7) allows emergency interceptions under certain circumstances but requires that an application for an order approving the interception be made within forty-eight hours after the interception has occurred or begins to occur.

101. 18 USC s 2518(8)(d).

legislation has occurred. It may also be argued that a mandatory notice requirement has the potential to operate as an important accountability measure since agencies conducting surveillance may be less likely to act illegally if they are required to tell the subject of the surveillance. It should also be noted that the Barrett Review concluded that the mandatory notification provisions in the United States and Canada operate without major difficulties.[102]

8.39 The Barrett Review of the Interception Act considered the issue of notice to the subject of a telecommunications interception. It favoured the approach in Canada and the US, although it would have limited the notice requirement it proposed to "innocent persons". It recommended that surveillance agencies should be required to notify any "innocent person" whose telephone had been intercepted of the fact of interception within 90 days of the cessation of the intercept.[103] *Although it did not give a clear definition of who should be considered an "innocent person", the Barrett Review argued that, if the information from telecommunication interception did not result in an arrest or progress in the criminal investigation, the person concerned should be notified of the interception. The Barrett Review summarised the following criticisms that law enforcement agencies made:*

> *– cause unnecessary distress and confusion because no explanation would be able to be divulged;*
>
> *– raise the profile of telecommunications interception among criminal elements;*
>
> *– cause embarrassment to government through public disclosure of sensitive operations;*
>
> *– be likely to compromise an investigation if, unknown to the investigator at the time of notification, the person was in fact associated either directly or indirectly with the true suspects;*
>
> *– be impractical because most investigation involve a number of TI targets, some involve several criminal operations, and some overlap with others and the interrelationships are often*

102. Barrett at para 4.3.3.
103. Barrett at para 4.3.1-4.3.3.

> *not fully understood; investigations may be stopped for a time and later revived when new evidence becomes available.* [104]

8.40 The Barrett Review recognised that these points have some validity but rejected them in light of the lack of concern for them by agencies in Canada and the USA.[105] *The Barrett Review's recommendation on notice to the subject of surveillance was rejected by the Government.*[106] *The Ford Review also did not favour the Barrett Review's recommendation.*[107]

8.41 One of the arguments against mandatory notice is that it has the potential to compromise surveillance operations and criminal investigations in general. For example, if a suspect is notified of the surveillance, he or she may alert others involved in the crime being investigated. Some investigations may continue over an extended period of time and to require notification of the subject within a specified time may prejudice such investigations. It may also be argued that such a requirement is too cumbersome to impose on law enforcement agencies. A provision requiring notice to every person whose activity may be recorded (including those not named in the warrant) may be impractical, or impossible to comply with in some cases because some of the people caught by the recordings may be unknown to the police and difficult to identify. It has also been observed that the differences between North American and Australian legal environments are such that a different approach should be considered.[108] *Further, it may be argued that the proposed surveillance legislation should focus on preventative accountability: the protection of privacy of individuals is better achieved by preventing illegal surveillance in the first place rather than providing for a notice requirement.*

---

104. Barrett at para 4.3.4.
105. Barrett at para 4.3.5.
106. See Australia, Attorney General's Department, 1995 Annual Review of Telecommunications (Interception) Act 1979 at 11.
107. Ford at para 4.4.
108. Barrett at para 4.3.5.

Register of interceptions

8.42 As an alternative to its recommendation to require mandatory notice to innocent persons, the Barrett Review proposed that each surveillance agency be required to maintain a register for the purpose of recording details of incidents where the telephone service of an innocent person was the subject of an interception warrant. The register would be supervised by the inspecting agency which would be able to undertake an inquiry and report to the relevant Minister on whether there is a need to give notice to the subject of the surveillance.[109] This recommendation was adopted in part in the Interception Act, which now provides for the keeping of a register showing details of warrants which have not led to a charge being laid.[110] This register is provided to the Attorney General but not, contrary to the Barrett Review's recommendation, subject to inspection and inquiry by the Privacy Commissioner.

Submissions and response

8.43 In IP 12, the Commission asked whether the new legislation should require people who have been placed under surveillance to be notified where the person is not found to be connected with any criminal activity, and is not prosecuted as a result of the surveillance. The majority of submissions on this point agreed that disclosure should take place.[111] Those who disagreed with disclosure to the subjects of surveillance argued that it would be of very little value,[112] and would not be in the public interest in almost all cases.[113] The Joint Law Enforcement Agencies noted that the fact that a person is not prosecuted may depend on many factors and does not necessarily mean that the surveillance was not justified.[114]

---

109. Barrett at para 4.3.5.
110. Telecommunications (Interception) Act 1979 (Cth) s 81C(1).
111. M L Sides, Submission at 15; NSW Council for Civil Liberties, Submission at 5; NSW Young Lawyers Criminal Law Committee, Submission at 6-7; Privacy Committee of NSW, Submission at 27; Law Society of NSW, Submission at 5-6.
112. Registered Clubs Association of NSW, Submission at 6.
113. Joint Law Enforcement Agencies, Submission at 10.
114. Joint Law Enforcement Agencies, Submission at 10.

The New South Wales Police Special Services Group considered that compliance with a disclosure provision broader than the existing section in the LDA would be impossible, as numerous people may be caught intentionally and unintentionally on surveillance tapes, and were often unknown to the police. The police also argued that disclosure may prejudice ongoing investigations as people would take steps to ensure that no further devices could be installed.[115]

8.44 If it were accepted that the new legislation should contain disclosure provisions, the Commission also asked whether the existing LDA provision was an appropriate model. Two submissions considered that section 20 of the LDA was adequate.[116] *Others argued that section 20 was ineffective as there is no evidence that it has ever been used.*[117] *The Privacy Committee argued that there should be a strong presumption of disclosure unless the warrant applicant can show why the surveillance should remain confidential.*[118] *The New South Wales Council for Civil Liberties considered that section 20 should be replaced with a clear right to notification on the part of the subject of the surveillance.*[119] *The NSW Young Lawyers Criminal Law Committee argued that section 20 operated too narrowly, as it seemed to apply only where the subject was aware that surveillance had occurred.*[120] *Two submissions suggested that the disclosure provisions should be broadened along the lines of the United States and Canadian laws, to enable the judge who authorises the warrant to order disclosure to the subject, perhaps as a condition of granting the warrant.*[121] *It was also suggested that the issue of who should receive the information should be clarified, though it should always include*

115. *NSW Police Service, Special Services Group, Submission at 11. This concern was also echoed by Price Waterhouse, Submission at 11.*
116. *M L Sides, Submission at 15; Director of Public Prosecutions, Submission at 8.*
117. *Privacy Committee of NSW, Submission at 27.*
118. *Privacy Committee of NSW, Submission at 27.*
119. *NSW Council for Civil Liberties, Submission at 5.*
120. *NSW Young Lawyers Criminal Law Committee, Submission at 6.*
121. *NSW Young Lawyers Criminal Law Committee, Submission at 6; Law Society of NSW, Submission at 5-6.*

the subject of the surveillance, and that all of the information obtained from the surveillance and contained in the warrant application should be available for disclosure.[122] *Price Waterhouse suggested that the legislation should contain guidelines for when disclosure was appropriate.*[123]

Conclusion

8.45 The Commission is not convinced that a mandatory notice requirement is justified. To require notice in every case may impose an unnecessary cost on those who use surveillance devices. However, there may be cases when the subject should be made aware of the surveillance, in particular, when surveillance has been illegally conducted. The subject of the surveillance will not be able to obtain the relief provided by the proposed surveillance legislation unless he or she is made aware of the illegality. The Commission considers that the current procedure under the LDA which requires a determination by the eligible judge, on a case-by-case basis, of the need for notice to the subject should largely be adopted in the proposed Surveillance Act. This provision should, however, be extended to include cases involving surveillance pursuant to public interest or employment authorisations. Just as the LDA currently provides, the person or organisation that may be required to give notice should have an opportunity to address the issuing authority on the matter.

8.46 The Commission also recommends that the inspecting authority (being either the Privacy Commissioner or the Ombudsman) should have the power to recommend to the issuing authority that individuals be notified of the improper use of the device and be given such information about the surveillance as may be appropriate. Because of its access to the records of the relevant agencies, the inspecting authority will, in some instances, be in a better position than the issuing authority to assess whether or not privacy interests have been breached. In the case of surveillance without a warrant or authorisation, for example, the issuing

122. NSW Young Lawyers Criminal Law Committee, Submission at 6.
123. Price Waterhouse, Submission at 11.

authority will not have been aware of such occurrence and won't be in a position to determine the need for notice to the subject unless the situation is brought to its attention. The inspecting agency's function of actively and systematically monitoring compliance with the proposed legislation, mainly through the inspection of records of the relevant agencies, makes it ideally placed to recommend the giving of notice to the subject of the surveillance.

8.47 The power to give notice should not be confined, as it is under the Interception Act to so called "innocent persons" or to those against whom no criminal proceedings have been instituted.[124] *Notice to those who have been charged with an offence may be appropriate for a number of reasons. The surveillance could be illegal for non-compliance with the conditions of the warrant or authorisation. It could be unlawful because no warrant or authorisation was issued to authorise it. The Commission is of the view that a notice may be given to any person whose private activity has been the subject of surveillance, including: persons named in warrants or authorisations, whether or not subsequently charged with an offence; persons not specified in warrants or authorisations but whose activities have been incidentally monitored; and persons whose activities were monitored where no warrant or authorisation was issued. To determine the need for notice, the issuing authority must play an active role in examining the proper execution of warrants or authorisations while the inspecting authority should ensure that compliance with the various requirements of the legislation is monitored and should be mindful of any possible infringement of the privacy interests of the persons concerned. The various agencies that carry out surveillance should be required to record as much information about their surveillance operations as possible, such as details of instances when the activities of persons other than those named in warrants or authorisations were recorded, cases when surveillance was carried out without a warrant or authorisation and particulars of persons whose private activities were monitored or recorded but against whom no criminal*

124. Telecommunications (Interception) Act 1979 (Cth) s 81C.

proceedings had been instituted or were likely to be instituted.[125]

8.48 There is also a need to clarify the scope of the notice. The Commission considers merely being told of the fact the person has been the subject of surveillance is inadequate. This would not give the person concerned enough information to allow him or her to determine the legality or propriety of the surveillance. To tell a person that his or her private activities have been covertly monitored, without allowing him or her access to further information, would merely engender anxiety and not assist him or her to pursue any remedies to which he or she might be entitled. The issuing authority should have the discretion to order that the subject of the surveillance be given details of the surveillance, including the date, time and place of the surveillance and the types of devices used. The issuing authority should also be able to make available for inspection by the person under surveillance such portions of the recorded private conversation or activity, applications for the warrant or authorisation and/or the warrant or authorisation as the issuing authority determines to be in the interests of justice.

Recommendation 80

The proposed Surveillance Act should provide that where a surveillance device has been used to record the private conversation or activity of a person, the issuing authority may:

- **direct the person or organisation which used the device to supply to the subject of the surveillance, within a period specified by the issuing authority, such information regarding the use of the device as the issuing authority may specify, including details about the surveillance such as the date, time, place and type of devices used;**
- **upon motion, make available to the subject for inspection such portions of the recorded private**

125. This is contained in Recommendation 72.

conversation or activity, applications for the warrant or authorisation and the warrant or authorisation as the issuing authority determines to be in the interest of justice; and

- **either upon the recommendation of the inspection authority or on its own motion, direct that notice is required to be given, if satisfied that notice is necessary under the circumstances. The issuing authority must give the person or organisation who will be required to give notice an opportunity to be heard on the matter. Failure to comply with a direction to give notice should constitute an offence.**

9. Dealings with covert surveillance information

- Publication and communication of information obtained by the conduct of surveillance
- The use of illegally obtained surveillance material as evidence in legal proceedings
- Incidentally obtained evidence
- Pre-trial disclosure of surveillance evidence
- Suppressing the publication of surveillance evidence
- Security and storage of covert surveillance material
- Destruction of surveillance information

9.1 This chapter looks at the use of information obtained from covert surveillance. Typical purposes of covert surveillance include gathering information leading to the exposure of fraud, theft, corruption and other offences. The information may result in the arrest and prosecution of offenders, and may be used as evidence in legal proceedings. Surveillance material can also assist in private or media investigations. Placing restrictions on the use of information obtained from the conduct of surveillance assists in maintaining a balance between surveillance for legitimate and necessary purposes and the privacy of individuals. It also promotes the accountability of those conducting surveillance.

9.2 The first issue examined in this chapter relates to the publication or communication of information obtained as a result of covert surveillance. In particular, the chapter examines a number of issues relating to the use of evidence in legal proceedings. These are as follows:

- *the admissibility of illegally obtained evidence;*
- *the admissibility of information which relates to matters other than those for which the warrant or authorisation was issued;*
- *pre-trial disclosure requirements where surveillance evidence is relevant or proposed to be used in legal proceedings; and*
- *the power to make suppression orders in proceedings involving surveillance evidence.*

The chapter also looks at whether surveillance legislation should regulate the storage and destruction of covert surveillance information.

PUBLICATION AND COMMUNICATION OF INFORMATION OBTAINED BY THE CONDUCT OF SURVEILLANCE

9.3 Information is often obtained through the conduct of surveillance with the intention of publishing or communicating that information to other people. Publication or communication may be

in the form of telling a colleague, informing the police, passing on police information to prosecutors, using the information in court proceedings or broadcasting the information in the print or electronic media. The Listening Devices Act 1984 (NSW) ("LDA") contains two prohibitions on the publication and communication of private conversations recorded with the use of listening devices. The first, found in section 6 of the LDA, prohibits any person from knowingly communicating or publishing to any other person a private conversation, which has come to person's knowledge as the result of the illegal use of a listening device. There are three exceptions to this prohibition.[1] The first class of exceptions is where the communication or publication is made to a party to the conversation, or with the express or implied consent of all of the principal parties to the conversation, or in proceedings for an offence against the LDA. The second is where the communication or publication is not more than is reasonably necessary in connection with: an imminent threat of serious violence to persons or of substantial damage to property; or a serious narcotics offence. The third is where the listening device was illegally used "to prevent a person who has gained knowledge of the conversation by means other than the illegal use of a listening device, even if they also have knowledge from such illegal use, from publishing or communicating information concerning the conversation."

9.4 Section 6 of the LDA applies only to the situation where the private conversation was obtained through an unlawful use of listening devices. Therefore, private conversations recorded by a listening device authorised by a warrant may, as a general rule,[2] be used for any purpose without breaching section 6.

9.5 The second prohibition, found in section 7 of the LDA, makes it an offence for a person who has been a party to a private conversation and has used a listening device to record the conversation (whether in contravention of the LDA or not) from communicating or publishing any resulting record of that

1. *LDA s 6(2).*
2. *An exception is where the person who wishes to use the private conversation has been a party to the private conversation: LDA s 7.*

conversation.[3] *There are also exceptions to this section.*[4] *These include where the communication or publication:*

- *is made to another party to the conversation or with the express or implied consent of all of the principal parties;*[5]
- *is made in the course of legal proceedings;*
- *is not more than is reasonable necessary for the protection of the lawful interests of the communicator or publisher;*
- *is communicated to a person who has, or is believed to have, such an interest in the conversation as to make the communication reasonable in the circumstances; or*
- *is made by a person who used the listening device pursuant to a warrant under the LDA or an authority granted under the Telecommunications (Interception) Act 1979 (Cth) ("Interception Act") or any other Commonwealth law.*

The law in other Australian jurisdictions

9.6 Listening or surveillance devices legislation in other Australian States and territories have varying approaches to the regulation of the use of surveillance information. The approach of the legislation in Queensland, Tasmania, and the Australian Capital Territory is similar to the LDA. This approach incorporates two basic rules. The first is a general rule prohibiting communication and publication of recorded private conversations, subject to certain exceptions.[6] *The prohibition applies only to private*

---

3. *LDA s 7(1).*
4. *LDA s 7(2).*
5. *The LDA authorises a party to a private conversation to record it if a principal party to the conversation consents to the use of the listening device and the recording is not made for the purpose of communicating or publishing the conversation or a report of it to non-parties: s 5(3)(b)(ii).*
6. *Invasion of Privacy Act 1971 (Qld) s 44; Listening Devices Act 1991 (Tas) s 9; Listening Devices Act 1992 (ACT) s 6.*

conversations unlawfully listened to, leaving the communication and publication of legally recorded private conversations unregulated. The second rule is one that applies specifically to parties to the conversation.[7] This rule also consists of a general prohibition with exceptions, although these exceptions are different from the exceptions to the first rule. Moreover, in contrast to the first rule, the second rule applies regardless of whether a record of the private conversation was obtained legally or not.

9.7 In South Australia, the legislation prohibits, without exception, the communication or publication of information or material obtained unlawfully.[8] Where the information was obtained under a warrant, it is likewise unlawful for a person to knowingly communicate or publish it, except in the course of duty or as required by law.[9] The legislation then makes provisions for a separate rule to apply where the listening device was used by one of the parties (presumably a law enforcement officer) to the conversation for certain purposes. He or she may communicate the recordings if it is: in the course of their duty; in the public interest; or for the protection of their lawful interests. The South Australian legislation differs from the law in New South Wales, Queensland, Tasmania, and the Australian Capital Territory in two fundamental ways. First, it regulates legal recordings. Second, it does not provide for exceptions to the prohibition on the communication of unlawful recordings. However, illegally obtained recordings may be relevant for some purposes, such as in investigations and prosecutions of law enforcement officers who committed the illegality.

9.8 The Surveillance Devices Act 2000 (NT) does not makes a distinction between unlawful and lawful recordings and regulates both.[10] Neither does it have a separate provision for persons who have been party to the private conversations or activities which were the subject of the surveillance.

---

7. Invasion of Privacy Act 1971 (Qld) s 45; Listening Devices Act 1991 (Tas) s 10; Listening Devices Act 1992 (ACT) s 5.
8. Listening Devices Act 1972 (SA) s 6.
9. Listening Devices Act 1972 (SA) s 6a.
10. Surveillance Devices Act 2000 (NT) s 40.

9.9 The Surveillance Devices Act 1999 (Vic) prohibits the communication or publication of private conversations or activities that have been the direct or indirect result of the use of a listening device, an optical device, tracking device[11] or data surveillance device.[12] This is subject to a list of exceptions. It does not distinguish between private conversations or activities that were obtained by the lawful use of the device and those that were obtained unlawfully. It does not have a separate provision for persons who have been party to the private conversations or activities which were the subject of the surveillance.

9.10 The Surveillance Devices Act 1998 (WA) has a framework similar to that of the Victoria and Northern Territory legislation,[13] although some of the exceptions are different. Moreover, it provides for a separate regime for information obtained through the unauthorised use of a surveillance device in the public interest. Private conversation or activity that has come to a person's knowledge as a direct or indirect result of the use of a listening device or optical device in the public interest may be used only if authorised by an order made by a judge.[14]

Conclusion

9.11 The main shortcoming of the LDA provisions is that there are no limits on the use that can be made of information obtained legally under the LDA. For example, private conversations recorded by police with the use of a listening device pursuant to a warrant may be used not only in connection with the investigation and prosecution of a crime but may also be passed on to anybody, without violating the provisions of the LDA. The Commission considers that the protection the law affords the individual's privacy interests should extend beyond ensuring that he or she is not subjected to unjustified surveillance. It should extend to protecting the information obtained from the surveillance activity.

---

11. Surveillance Devices Act 1999 (Vic) s 11.
12. Surveillance Devices Act 1999 (Vic) s 12.
13. Surveillance Devices Act 1998 (WA) s 9.
14. Surveillance Devices Act 1998 (WA) s 31.

This protection should apply regardless of whether the information was obtained lawfully or unlawfully. The mere fact that a covert surveillance operation was lawful does not justify the use of the surveillance information for any purpose, however unrelated to the purpose for which the warrant was granted.

9.12 The Commission is also of the view that the distinction in the LDA between information recorded by parties and non-parties to a private conversation should not be adopted in the proposed surveillance legislation. The rule in the LDA which applies to communication or publication by parties to the private conversation is mainly aimed at complementing its participant monitoring provisions, which allow one party to a conversation to record it without the consent of the other parties when particular conditions have been met.[15] *In Chapter 2, the Commission recommends that the proposed surveillance legislation should not contain participant monitoring provisions. It follows from this recommendation that, in regulating the use of information obtained through the conduct of surveillance, there is no longer a need to distinguish between parties and non-parties.*

9.13 The Commission favours an approach (adopted in Victoria, Western Australia and the Northern Territory) which generally prohibits every person, including parties and non-parties to the activity which was the subject of the surveillance, from communicating or publishing any information obtained as a result of surveillance, whether legal or illegal. The prohibition should be subject to exceptions which should, in the main, be limited to allowing the information to be used for the purposes for which the surveillance was authorised, or where such use is necessary or reasonable under the circumstances.

Exceptions to the prohibition on the communication or publication of surveillance information

9.14 Surveillance technology is increasingly being relied on in the detection and investigation of offences, and in order to gather evidence that will be used in legal proceedings. Electronic evidence gathering has significant advantages over more conventional means

15. LDA s 5(3)(b).

of obtaining information, such as providing a direct and contemporaneous account of an event, which may avoid many of the threshold evidentiary issues.[16] The proposed surveillance legislation should allow the communication of surveillance information for the purpose of investigation and prosecution of offences. It should also allow the information to be used in related proceedings, such as bail proceedings or those involving the confiscation of the profits of a crime or the forfeiture of property that is tainted property in respect of an offence.[17]

9.15 Where surveillance has been conducted illegally, the information gathered from that surveillance will also be relevant in prosecuting the surveillance user, or, where applicable, in disciplinary proceedings. Furthermore, the Commission recommends in Chapter 10 that a civil right of action be available for people whose interests have been affected by unlawful surveillance. In order to establish a cause of action or substantiate a claim for relief, the plaintiff will need to obtain access to surveillance material and communicate it to counsel and the court. By the same token, the defendant to the action may also need to use the material in question for his or her defence.

9.16 The Commission considers it necessary to provide that surveillance information may be published in the interests of public safety. For example, if the subject of surveillance is suspected of having committed serious crimes, it may be in the public interest to publicise the fact that that person has a history of violence and may be dangerous, and/or to publish some of the material gathered through surveillance, such as the suspect's photograph. The law enforcement officers and members of the media should be allowed to use the surveillance information in these circumstances.

9.17 Finally, if all parties to the private conversation or activity that was the subject of the surveillance consented to the

16. *The High Court has acknowledged the importance of recorded evidence, particularly where confessions and admissions in criminal trials are concerned: see McKinney v The Queen (1991) 171 CLR 468 at 473-474 (Mason, Deane, Gaudron and McHugh JJ).*
17. *See Confiscation of Proceeds of Crime Act 1989 (NSW).*

communication or publication of the information obtained from the surveillance, they should be considered to have waived whatever protection the law otherwise gave them.

Recommendation 81

The proposed Surveillance Act should contain a general prohibition on the publication or communication of all information obtained as a result of the conduct of surveillance, whether the surveillance has been authorised or not, subject to the following exceptions. The prohibition should not apply where the communication or publication of the information is made:

(a) by a law enforcement officer:

- **to another law enforcement officer for the purpose of investigating or prosecuting an offence;**
- **to the DPP or other prosecuting officer for the purpose of prosecuting an offence; or**
- **is otherwise made in the performance of his or her duty;**

(b) in the course of, or for the purposes of, legal proceedings, including proceedings for the prosecution of offences, bail proceedings and those involving confiscation or forfeiture of property in relation to an offence;

(c) in the course of, or for the purposes of, investigations or criminal, civil or disciplinary proceedings related to any violation of the proposed Surveillance Act;

(d) in the belief based on reasonable grounds that it was necessary in connection with an imminent threat of serious violence to persons, or of substantial damage to property;

(e) with the consent of all of the parties to the conversation or activity.

Breach of this provision should be an offence.

Publication or communication of surveillance information obtained pursuant to a public interest or employment authorisation

9.18 The information obtained from surveillance pursuant to public interest and employment authorisations merits a different treatment from that obtained from surveillance pursuant to a warrant. While the main purpose of surveillance by law enforcement officers is to investigate offences and gather evidence, the purposes for which private individuals may need to conduct surveillance are more varied. The Commission is of the view that the exceptions that will allow law enforcement agencies to use information obtained from surveillance should not apply to the material gathered by employers, the media and other private individuals. The Commission agrees with the approach in Western Australia, where information obtained pursuant to surveillance in the public interest may be used only upon order by the court.[18]*. Further, since the Commission has recommended that prior authorisation must be obtained to conduct surveillance in the public interest or in the employment context,*[19] *the Commission considers that an applicant should outline in the application for authorisation the intended use of the information. If the holder of the authorisation wants to use the surveillance information for a purpose not stated in the authorisation, he or she should apply to the issuing authority for approval to do so.*

18. *Surveillance Devices Act 1998 (WA) s 31.*
19. *See ch 6 and 7. In Western Australia, the use of optical surveillance devices or listening devices in the public interest without a warrant is allowed by the legislation in certain circumstances: Surveillance Devices Act 1998 (WA).*

Recommendation 82

The proposed Surveillance Act should provide that when a public interest or employment authorisation is made, the order must specify the purposes for which the information obtained though the conduct of surveillance may be used and the circumstances under which the information may be published or communicated. Breach of the terms of the authorisation should constitute an offence. The proposed Surveillance Act should provide that the issuing authority may authorise, at the completion of the surveillance, the use of information obtained by the surveillance for a purpose other than that specified in the authorisation.

THE USE OF ILLEGALLY OBTAINED SURVEILLANCE MATERIAL AS EVIDENCE IN LEGAL PROCEEDINGS

9.19 This section examines the issue of what treatment should be afforded material obtained illegally, but which may be relevant evidence in criminal or civil proceedings. The issue involves balancing two competing interests. On the one hand, there is the public interest in full information being available for the accurate determination of facts in legal proceedings. In criminal trials, in particular, there is a public interest in securing the conviction and punishment of those guilty of a crime. On the other hand, there is a public interest in protecting individuals from infringements of their rights by authorities who have the obligation of enforcing and upholding the law.

9.20 The Commission has considered three alternative approaches for dealing with evidence obtained illegally.

General admission of illegally obtained evidence

9.21 The first approach is to admit illegally obtained evidence. In England, although it is settled that a criminal trial judge has the discretion to refuse to admit evidence where its prejudicial effect outweighs its probative value,[20] it has been ruled that the judge "has no discretion to refuse to admit relevant admissible evidence on the ground that it was obtained by improper or unfair means."[21] In R v Khan,[22] for example, the House of Lords decided that an illegal covert recording of a conversation was admissible, even though obtaining the recording involved trespass and damage to property. Lord Nolan commented that it would be a "strange reflection on the law" if a person who had admitted involvement in an offence could have the conviction set aside because his privacy had been invaded.[23] One commentator has suggested that, on balance, the current English case law favours the admission of illegal or improper surveillance evidence "in the absence of blatant bad faith or oppression on the part of the investigators."[24]

9.22 The advantages of this approach include maximising the amount of evidence admitted for the consideration of the courts and reducing the complexity of the trial by circumventing issues such as the illegality of the evidence.[25] It is arguable that the illegality committed by law enforcement officers is better dealt with, not by

---

20. R v Sang [1980] AC 402; Selvey v DPP [1970] AC 304; Noor Mohamed v The Queen [1949] AC 182; R v Christie [1914] AC 545.

21. R v Sang [1980] AC 402 at 437 (Diplock J). See also Kuruma v The Queen [1955] 1 All ER 236; King v The Queen [1968] 2 All ER 610.

22. R v Khan [1996] 3 WLR 162.

23. [1996] 3 WLR 162 at 175. For a discussion on the ramifications of R v Khan, and the impact of the Police Act 1997 (UK) on English common law discretions so far as electronic surveillance evidence is concerned, see S Sharpe, "Electronic Eavesdropping: A Chance For Accountability?" (1996) 146 New Law Journal 1088; P B Carter, "Evidence Obtained by the Use of a Covert Listening Device" (1997) 113 Law Quarterly Review 468.

24. S Sharpe "Electronic Eavesdropping: A Chance For Accountability?" (1996) 146 New Law Journal 1088 at 1091.

25. Australian Law Reform Commission, Evidence (Interim Report 26, 1985) Vol 1 at para 960.

excluding the evidence they have gathered but, by imposing administrative, civil or penal liability on them.

9.23 The counter argument is that this approach ignores the quality of the evidence. Evidence which was illegally or improperly obtained may not be reliable and, if so, its admission would result in an unfair trial. This approach is not consistent with the duty of the courts to ensure that the criminal process is fair.[26] *It also ignores the reality that victims of unlawful methods of criminal investigation often do not have other avenues to obtain justice apart from having the incriminating evidence against them excluded. This approach may also be criticised on the ground that it involves the court itself in giving, or appearing to give, effect to illegality or impropriety. This perception may damage the repute and integrity of the judicial process.*

Discretion to exclude evidence

9.24 Section 138 of the Evidence Act 1995 (NSW) ("Evidence Act") provides that evidence that was illegally or improperly obtained "is not to be admitted unless the desirability of admitting the evidence outweighs the undesirability of admitting evidence that has been obtained in the way in which the evidence was obtained." This provision reflects the common law.

9.25 At common law in Australia, there is a discretion to exclude unlawfully or improperly obtained evidence. This is commonly referred to as the public policy discretion. The High Court has ruled that when unlawful means are employed to procure evidence, the judge has a discretion to reject it:

> *In the exercise of it, the competing public requirements must be considered and weighed against each other. On the one hand there is the public interest in the protection of the individual from unlawful and unfair treatment. Convictions*

26. ALRC Report 26 at para 960.

> *obtained by the aid of unlawful or unfair acts may be obtained at too high a price. Hence the judicial discretion.*[27]

9.26 The other significant issue relevant to the exercise of the discretion to exclude evidence is the question of fairness.[28] *The fairness discretion is not based on whether the accused has been treated unfairly but whether the reception of the evidence would be unfair to him or her, in the sense that its use would result in an unfair trial, as the reliability of the confession has been affected by the propriety of the means used to procure it.*[29]

9.27 A distinction is made between the fairness and public policy discretions on the basis that while the former is focused on the effect of the illegality or impropriety on the fairness of the trial in question, the public policy discretion is directed at "large matters of public policy"[30] *including the inherent quality of the conduct of the police or other person in a position of authority over the accused. It has, however, been recognised that there is an overlap between the area of focus of each.*[31] *It has been suggested that fairness to an accused is just one relevant factor in the exercise of the public policy*

---

27. *R v Ireland (1970) 126 CLR 321 at 335 (Barwick J); See also Bunning v Cross (1978) 141 CLR 54 at 72 (Stephen and Aickin JJ); Cleland v The Queen (1982) 151 CLR 1 at 19-20 (Deane J); Ridgeway v The Queen (1995) 184 CLR 19 at 30-36 (Mason, Deane and Dawson JJ).*
28. *R v Lee (1950) 82 CLR 133.*
29. *See R v Lee (1950) 82 CLR 133; see also Cleland v The Queen (1982) 151 CLR 1 at 9 (Gibbs J), at 19 (Deane J), and at 33 (Dawson J). Other decisions suggest that the unfairness discretion focuses not just on reliability and on securing a fair trial but also embodies a demand for procedural propriety, that is, a recognition of the accused's rights and privileges within the criminal justice system. For example, in R v Swaffield (1998) 192 CLR 159 at 197 Toohey, Gaudron and Gummow JJ stated: "Unreliability is an important aspect of the unfairness discretion but it is not exclusive. As mentioned earlier, the purpose of that discretion is the protection of rights and privileges of the accused. Those rights include procedural rights."*
30. *Foster v The Queen (1993) 113 ALR 1 at 7.*
31. *R v Swaffield (1998) 192 CLR 159 at 181-183 (Brennan J), at 191 (Toohey, Gaudron and Gummow JJ).*

discretion.[32]

9.28 A number of cases have applied or considered either or both of the public policy and fairness discretions in determining the admissibility of surveillance evidence.[33]

9.29 Section 138 of Evidence Act implements the recommendation of the Australian Law Reform Commission,[34] *which this Commission supported.*[35] *The courts have construed this section as co-extensive with the common law.*[36] *It differs, however, from the common law discretion in a number of ways. For example, section 138 applies to civil proceedings*[37] *while the common law discretion has largely been applied in criminal cases. At common law, the onus is on the accused to prove the illegality or impropriety and justify the exclusion. Under section 138, the party seeking exclusion of the evidence has the threshold onus of establishing that it was improperly or illegally obtained. If that onus is met, it is for the party seeking the admission of the evidence to satisfy the court that the desirability of admitting such evidence outweighs the undesirability of admitting it, given the way in which it was obtained.*[38]

---

32. *R v Swaffield (1998) 192 CLR 159 at 178 (Brennan J).*
33. *R v Smith [1994] 75 A Crim R 327; R v O'Neill (1996) 2 Qd R 257; R v Truong (1996) 86 A Crim R 188; R v Swaffield (1998) 192 CLR 159; R v Suckling [1999] NSWCCA 36; R v Cassar [1999] NSWSC 650.*
34. *See ALRC Report 26, ch 39.*
35. *New South Wales Law Reform Commission, Evidence (Report 56, 1988).*
36. *R v Cassar [1999] NSWSC 650 at para 16 (Sperling J).*
37. *See Klein v Bryant [1998] ACTSC 89. This case also demonstrates that the discretion in s 138 applies to evidence obtained by private individuals, such as private investigators.*
38. *R v Coombe (NSW, Court of Criminal Appeal, No 60239/96, 24 April 1997, unreported); R v Salem (1997) 96 A Crim R 421; R v Rooke (NSW, Court of Criminal Appeal, No 60550/96, 2 September 1997, unreported); R v Nabalarua (NSW, Court of Criminal Appeal, No 60124/97, 19 December 1997, unreported); R v Coulstock (1998) 99 A Crim R 143.*

9.30 Furthermore, section 138 identifies factors relevant in the exercise of the discretion[39] that are wider than those found in common law.[40] The listing of these factors in the legislation was considered necessary to "minimise the inherent difficulties in the exercise of discretionary power, and, to a certain extent, of avoiding the danger of too great a disparity between legal decisions".[41]

9.31 Section 138 does not refer to unfairness to the defendant as a consideration in the exercise of the discretion. However, section 90 of the Evidence Act creates a discretion to refuse to admit evidence if "having regard to the circumstances in which the admission was made, it would be unfair to a defendant to use the evidence."[42] Moreover, section 137 of the Evidence Act provides that in a criminal proceeding, the court must refuse to admit evidence adduced by the prosecutor if its probative value is outweighed by the danger of unfair prejudice to the defendant.

9.32 One of the main advantages of the discretionary approach found in the common law and now in the Evidence Act is that it gives courts flexibility in deciding whether or not to admit illegally obtained evidence. The courts are not bound to uphold a particular interest, for example, the public interest in upholding the rights of the accused which may have been violated by unlawful police

---

39. Section 138(3) of the Evidence Act 1995 (NSW) identifies these factors: (a) the probative value of the evidence; (b) the importance of the evidence in the proceeding; (c) the nature of the relevant offence, cause of action or defence and the nature of the subject matter of the proceedings; (d) the gravity of the impropriety or contravention; (e) whether the impropriety or contravention was deliberate or reckless; (f) whether the impropriety or contravention was contrary to or inconsistent with a right of a person recognised by the International Covenant on Civil and Political Rights; (g) whether any other proceeding (whether or not in a court) has been or is likely to be taken in relation to the impropriety or contravention; and (h) the difficulty (if any) of obtaining the evidence without impropriety or contravention of an Australian law. These factors are non-exhaustive: R v Truong (1996) 86 A Crim R 188 at 196 (Miles J).

40. See specifically those set out in Bunning v Cross (1978) 141 CLR 54.

41. ALRC Report 26 at para 964.

42. This provision is limited to evidence of admissions.

conduct, over all others in all circumstances. It allows them to consider other interests, such as the public interest in the conviction and sentencing of offenders, and to decide each case based on all the relevant facts. The approach recognises the role of courts in balancing the rights of individuals against competing public interests.

9.33 It has also been asserted that a clear advantage of the discretionary rule is that "it keeps the courts continually in touch with current social attitudes and may lead to the eventual evolution of the rules as the courts adapt them to changing social realities."[43]

9.34 However, it can also be argued that the discretionary approach introduces a degree of uncertainty and unpredictability into decision making.[44] *Illegally obtained evidence may be excluded in one case but admitted in another, even where the circumstances are similar. The outcome may depend on an individual judge's view on the weight of a particular interest. A seeming inconsistency in the application of the discretion may weaken the deterrent effect which is sought to be achieved by the exercise of the discretion.*

9.35 The Australian Law Reform Commission recognised the difficulties surrounding the discretionary approach. To minimise them, it stated that it was important "to indicate precisely the nature of the competing interests which should be balanced and to articulate the factors which should be taken into account in the exercise of the discretion."[45] *Section 138 of the Evidence Act does not*

---

43. Law of Evidence Project (Canada), Compellability of the Accused and the Admissibility of His Statements (The Law Reform Commission, Ottawa, 1973).

44. Sharpe, "Electronic Eavesdropping: A Chance For Accountability?" at 1088. The comment was made in relation to the Police and Criminal Evidence Act 1984 (UK) s 78, which broadly provides that the court may exclude illegal evidence if it is of the opinion that "it would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it".

45. ALRC Report 26 at para 964. It identified the following as the interests which courts must balance in cases involving illegally or improperly obtained evidence: ensuring that all reliable evidence is admitted to secure the conviction of the guilty; upholding the rights

identify the competing interests but specifies factors which courts must consider when exercising their discretion.[46]

Exclusionary rule

9.36 The third approach to illegally obtained evidence is to apply a blanket exclusion. This position is best exemplified in the United States where evidence obtained by means of illegal search and seizure methods is excluded,[47] *if a timely application is made to suppress the evidence.*[48] *Once it is established that the means of gathering the evidence was unconstitutional or otherwise unlawful, the courts must hold the evidence as inadmissible. This exclusionary rule in the United States rests upon the prohibition of unreasonable searches and seizures contained in the Fourth Amendment of the Constitution,*[49] *although that Amendment contains no express provision precluding the use of evidence obtained in violation of its provisions.*[50] *The Federal statute which*

---

of individuals; deterring misconduct by law enforcement agencies; and maintaining the legitimacy of the judicial system.

46. *Evidence Act 1995 (NSW) s 138(3).*
47. *State v Fisher 686 P2d 750 (1984); People v Hamilton 666 P2d 152 (1983); State v Johnson 716 P2d 1288 (1986); Thompson v Carthage School Dist 87 F3d 979 (1996); US v Kennedy (1995) 61 F3d 494; US v Medina Reyes 877 F Supp 468 (1995)*
48. *Weeks v United States 232 US 383 (1914); State v Burnley 910 P2d 1294 (1996); US v Wilson 11 F3d 346 (1993).*
49. *Olmstead v United States 277 US 438 (1928); US v Nichols 979 F2d 402 (1992); US v Eastland 989 F2d 760 (1993); US v Kennedy (1995) 61 F3d 494.*
50. *US v Leon 468 US 897 (1984). The Fourth Amendment of the Constitution of the United States of America 1789 (US) states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation and particularly describing the place to be searched, and the persons or things to be seized."*

regulates wire-tapping and electronic surveillance implements the exclusionary rule developed by the US Supreme Court.[51]

9.37 Section 13 of the LDA deals with the question of admission of illegally obtained material in evidence by providing that evidence of a private conversation recorded in breach of the LDA may not be given in any civil or criminal proceedings. Section 13 provides for exceptions[52] *which are not found in the strict US model.*[53] *However, they are very limited in application. For example, the discretion to admit illegally obtained evidence under section 13(2)(d) applies only in proceedings for an offence punishable by penal servitude for life or for 20 years or more, or a serious narcotics offence. The exceptions in section 13 do not dilute the essentially exclusionary nature of the provision.*

9.38 The arguments for the exclusionary rule include certainty and predictability. The stakeholders in the criminal justice system, namely the police, prosecution, the accused, the legal practitioners

---

51. Title 18, United States Code (1948) ("18 USC") s 2515.

52. LDA s 13(2) provides:

"Subsection (1) does not render any evidence inadmissible –

(a) if all of the principal parties to the private conversation concerned consent to the evidence being given;

(b) if the private conversation concerned comes to the knowledge of the person called to give the evidence otherwise than in the manner referred to in that subsection, notwithstanding that the person also obtained knowledge of the conversation in such a manner;

(c) in proceedings for an offence against this Act or the regulations; or

(d) in proceedings for –

(i) an offence punishable by penal servitude for life or for 20 years or more; or

(ii) a serious narcotics offence,

if the court considers that the evidence should be admissible."

53. In the US, the main exception is the so-called good faith exception, namely, the exclusionary rule will not bar the use of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a neutral magistrate which is ultimately found to be defective: Massachusetts v Sheppard 468 US 981 (1984); US v Leon 468 US 897 (1984).

and the judge, know that if the rights of the accused are violated through an illegal method of investigation, the results of such illegality will not be admissible in court.[54] It may be argued that this approach has a greater impact on deterring illegal police action than a case by case discretionary approach. The clarity of the rule provides a strong disincentive to impropriety.[55] It can also be argued that, in matters involving competing public interests, such as those involving the right of the accused and the efficiency of the criminal justice system, it is the legislature which should decide which interest has priority and legislate accordingly instead of leaving this matter for the courts to resolve.[56]

9.39 Several empirical studies have been conducted on the impact of the exclusionary rule on criminal prosecutions in the United States, in an attempt to determine whether the rule has any deterrent effect on illegal conduct by the police.[57] The United States Supreme Court has, with reference to the research, observed that it has not been conclusively established whether the exclusionary rule has the desired deterrent effect in situations where it is applied.[58] It appears that the US Supreme Court continues to rely on the rule on the basis of the Court's own assumptions regarding human nature and the interrelationships between the various components of the law enforcement system, rather than on empirical evidence showing the rule's effectiveness.[59]

9.40 Apart from the lack of evidence demonstrating that the

---

54. ALRC Report 26 at para 961.

55. ALRC Report 26 at para 961.

56. ALRC Report 26 at para 961.

57. Oaks, "Studying the Exclusionary Rule in Search and Seizure" (1970) 37 University of Chicago Law Review 665; Canon, "Is the Exclusionary Rule in Failing Health? Some New Data and a Plea Against a Precipitous Conclusion" (1974) 62 Kentucky Law Journal 681; J Spiotto, "Search and Seizure: An Empirical Study of the Exclusionary Rule" (1973) 2 Journal of Legal Studies 243; Van Duizend, Sutton and Carter, The Search Warrant Process, Preconceptions, Perceptions and Practices (1985); M Orfield, "The Exclusionary Rule and Deterrence: An Empirical Study of Chicago Narcotics Officers" (1987) 54 University of Chicago Law Review 1016.

58. US v Janis 428 US 433 (1975).

59. US v Janis 428 US 433 (1975).

exclusionary rule is effective in deterring improper police conduct, the rule may be criticised for its inflexibility. It treats trivial illegalities in the same manner as deliberate and serious ones.[60] *It also does not take into account the fact that the law enforcement officers involved have been, or are likely to be, punished or that the victim of the illegality may be compensated for the damage done.*[61]

Conclusion

9.41 Courts in Australia have, in recent times, gradually recognised the public interest in upholding the rights of individuals against illegal or improper conduct by the authorities. Allowing illegally obtained evidence to be admitted in court proceedings would be contrary to this trend and, arguably, retrogressive. It ignores the supervisory role of courts in monitoring the operation of the criminal justice system, including ensuring that the rights of individuals are respected. The approach gives the appearance, if not the effect, of courts sanctioning illegality in a way that is incompatible with their fundamental function of upholding the law. Moreover, on occasions, evidence which was illegally or improperly obtained may not be reliable and to allow its admission would result in unfair trials.

9.42 Both the exclusionary and discretionary rules acknowledge the importance of policing abuses of authority which invariably involve violation of rights. The exclusionary rule in the US was developed as a means of deterring police misconduct and is designed to enforce constitutional rights, mainly the right not to be subjected to unreasonable searches and seizures. The public policy discretion was developed in Australia to serve a similar function but differs markedly from the exclusionary rule by the fact that other interests which come into play in the criminal process are balanced against the public interest in protecting individuals from illegal or improper investigation procedures.

---

60. ALRC Report 26 at para 961. See, however, the good faith exception to the exclusionary rule: Massachusetts v Sheppard 468 US 981 (1984); US v Leon 468 US 897 (1984).

61. ALRC Report 26 at para 961.

9.43 For the purposes of the proposed surveillance legislation, the Commission prefers the discretionary approach to the exclusionary rule. The Commission does not subscribe to elevating a particular public interest as superior to all others in every given case, as the exclusionary rule does. The public interest in securing the conviction of the guilty, upholding the rights of individuals, deterring misconduct by law enforcement agencies, and others such as private investigators, and maintaining the legitimacy of the judicial system should all be weighed together in deciding the propriety of admitting illegally obtained evidence.

9.44 Furthermore, the exclusionary rule is too inflexible. As noted above, the rule generally does not distinguish between illegalities committed deliberately and those committed as a result of mistake. It also does not take into account the fact that the law enforcement officers involved have been or are likely to be punished or that the victim of the illegality may have other forms of redress. The Commission is of the view that circumstances such as these should be considered relevant in the admission or exclusion of the illegally obtained evidence.

9.45 There are, in the Commission's view, no sound policy reasons to support a special rule for the admissibility of illegal evidence, when it was obtained through the conduct of surveillance. The rule for evidence procured by illegal surveillance ought to be in line with the rule for all illegally obtained evidence, obtained in any other circumstances.

Recommendation 83

The admission of evidence obtained in violation of the proposed Surveillance Act should be governed by the *Evidence Act 1995* (NSW) and the general law on evidence.

INCIDENTALLY OBTAINED EVIDENCE

9.46 Based on the Commission's consultations with the police and private investigation groups, it would appear that in conducting investigations, it is common for them to encounter material relating to an offence that they had not sought to investigate. The LDA contains provisions regarding the admissibility of evidence obtained incidentally under a listening device warrant. Section 14 of the LDA provides:

> *(1) Where a private conversation has inadvertently or unexpectedly come to the knowledge of a person as a result, direct or indirect, of the use of a listening device pursuant to a warrant granted under Part 4:*
>
> *(a) evidence of the conversation, or*
>
> *(b) evidence obtained as a consequence of the conversation so coming to the knowledge of that person,*
>
> *may be given by that person in any criminal proceedings (including proceedings for or in connection with the grant of bail) notwithstanding that the warrant was not granted for the purpose of allowing the evidence to be obtained.*
>
> *(2) Subsection (1) does not render any evidence admissible if:*
>
> *(a) the evidence relates to an offence in respect of which a warrant could not be granted in Part 4, or*
>
> *(b) the application upon which the warrant was granted was not, in the opinion of the court, made in good faith.*

9.47 Under this provision, evidence would be admissible if obtained under a warrant even if it relates to an offence other than that specified in the warrant. Evidence will not be admissible under this provision, however, if it relates to an offence for which a warrant is not available, that is, an offence that is not punishable on indictment or prescribed under the LDA regulations, or if the court is of the opinion that the warrant application was not made in good faith.[62]

---

62. LDA s 14(2).

9.48 In one case, a listening device warrant was granted under the LDA on the basis of a suspicion that the subject of the warrant application was about to commit the offence of supplying the prohibited drug of cocaine.[63] *The recordings made pursuant to the warrant revealed transactions involving methylamphetamine (not cocaine) and the surveillance subject was charged and convicted of possessing that particular drug, for the purpose of sale. In discussing the admissibility of the recordings, the court observed that section 14 of the LDA, if applicable, would render the recordings admissible because "a warrant could have been obtained in New South Wales on the basis of a suspicion that the offence of supplying methylamphetamine was about to be committed."*[64]

9.49 One issue which arises from section 14 is whether evidence of an offence committed by a person other than the suspect named in the warrant is admissible. If police applied for a warrant in connection with the suspected commission by X of the offence of murder and they recorded material incriminating X and Y for the offence of manufacturing prohibited drugs, would this be admissible under section 14 in proceedings against Y? Will it make a difference if the incidental evidence implicated only Y? The courts have not had the opportunity settle these questions. However, section 14 states that evidence of private conversations inadvertently or unexpectedly recorded may be given "in any criminal proceedings." This language seems broad enough to allow the admission of incidental evidence which incriminates a third person, whether or not such evidence also incriminates the person named in the warrant.

Conclusion

9.50 The Commission agrees with the basic rule contained in section 14. Evidence of crimes committed by the subject other than those authorised in the surveillance warrant should be admitted in

63. *R v Mouhalos (SA, Court of Criminal Appeal, SCCRM-98-27; S6743, 3 July 1998, unreported). This case, while prosecuted in South Australia, involved a warrant issued under the LDA.*
64. *R v Mouhalos at 9 (Doyle CJ).*

evidence. Excluding the evidence would not further any significant privacy interest as the privacy of the individual has already been invaded (lawfully) by the surveillance which was conducted for a designated offence. Formulating a rule which would prevent the use of the inadvertently or incidentally obtained evidence may not change police conduct in the future or protect the privacy of the individual. Furthermore, once the surveillance is authorised by law, there is a public interest in collecting evidence of wrong-doing by the subject of the surveillance. Excluding incidentally obtained evidence may have the effect of insulating a suspect from evidence of one of his or her unlawful activities gathered during the course of a bona fide investigation of another of his or her illegal activities. The Commission considers that a provision similar to section 14 of the LDA should be adopted in the proposed legislation.

Recommendation 84

The proposed Surveillance Act should provide that where a private conversation or activity has inadvertently or unexpectedly come to the knowledge of a person as a result of the conduct of surveillance pursuant to a warrant or authorisation:

(a) evidence of the conversation or activity; and

(b) evidence obtained as a consequence of the conversation or activity

may be given by that person in any criminal proceedings even if the warrant or authorisation was not issued for the purpose of allowing that evidence to be obtained.

This should be subject to the proviso that such evidence will not be admissible if the application upon which the warrant or authorisation was granted was not, in the opinion of the court, made in good faith.

PRE-TRIAL DISCLOSURE OF

SURVEILLANCE EVIDENCE

9.51 In certain overseas jurisdictions, the admissibility of surveillance evidence is contingent on the prosecution giving notice to the accused of the intention to bring forward surveillance evidence. For example, the Crimes Act 1961 (NZ) requires, as a condition of admissibility of lawfully intercepted material, that the party intending to adduce the evidence give reasonable notice of such intention, together with: (1) a transcript of the private communication (where evidence is to be given in the form of recording); or (2) a written statement setting out the full particulars of the private communication (where evidence is to be given orally); and (3) a statement regarding the time, place and date of the private communication, and the parties to it, if known.[65]

9.52 The Canadian Criminal Code has an almost identical provision.[66] *Further, section 190 of the Canadian Criminal Code empowers a judge to order that further particulars be given of the private communication which the prosecution intends to adduce in evidence.*[67]

9.53 United States legislation also has a similar provision whereby evidence will be inadmissible in any trial or other proceeding in a Federal or State court unless each party has, not less than 10 days before, been furnished with a copy of the court order and application upon which the authorisation for the intercept was based. This requirement may be waived if the judge finds it was not possible to furnish this material, and that the other party will not be prejudiced by a delay or by not receiving it.[68]

---

65. *Crimes Act 1961 (NZ) s 312L.*
66. *Criminal Code 1985 (Canada) s 189(5).*
67. *Note also that at common law, a trial judge may also order the production of other (related) intercepted communications, where it would be in the interests of justice to do so: R v Lyons (1982) 140 DLR (3d) 223 (BCCA).*
68. *18 USC s 2518(9).*

9.54 There are a number of reasons for requiring pre-trial disclosures. Thorough pre-trial disclosure is necessary to enable the defendant to decide how to plead. The defendant should understand the facts alleged by the prosecution and the case which he or she would be required to meet.[69] A fair trial also requires that the defence be informed of all material available to the prosecution, whether or not it is formally admissible, which may be of assistance to the defence, including that which the prosecution does not intend to use as part of its case.[70] Compulsory prosecution pre-trial disclosure also addresses, to some extent, the inequality of resources between the prosecution and the defendant.[71]

9.55 By the same token, compulsory pre-trial disclosure by the defence would facilitate the determination of objections to the admissibility of particular evidence on the grounds of relevance. For the purpose of ruling on questions of admissibility, the trial judge will often need information about the defence case to determine the relevance of evidence. Research conducted on juries in New Zealand[72] shows that juries were greatly assisted in understanding the evidence if they were informed at an early stage of the issues in the trial. This can only be effectively done if the issues in the trial have been ascertained by some kind of pre-trial procedure.

9.56 Compulsory pre-trial disclosure on the part of both the prosecution and the defence would improve the efficiency of the criminal justice system. Pre-trial disclosure enhances plea discussions and identifies charges to which the defendant might plead, increasing the number of defendants who plead guilty and encouraging guilty pleas at an earlier stage. Early identification of guilty pleas improves the accuracy of court lists, reduces time wasted by all parties preparing for trial, minimises time wasted by all parties on unnecessary court attendances and also reduces wasted court time. It also leads to earlier and improved

---

69. New South Wales Law Reform Commission, The Right to Silence (Report 95, 2000) at para 3.85.
70. NSWLRC Report 95 at para 3.86.
71. NSWLRC Report 95 at para 3.88.
72. New Zealand, Law Commission, Juries in Criminal Trials (Preliminary Paper 37, 1999, Vol 2).

identification of the issues, facilitating more efficient trial preparation for both parties, shorter trials, fewer adjournments and fewer defence witnesses.[73]

9.57 The LDA does not currently contain any provision for pre-trial disclosure of material obtained by covert surveillance. None of the other Australian jurisdictions currently makes specific statutory provision for pre-trial disclosure between parties where surveillance is involved although some require police-prosecution disclosure.[74]

9.58 The Commission has recently looked at the issues surrounding pre-trial disclosure as part of its reference on the right to silence. In its report,[75] *the Commission expressed the view that the various pre-trial disclosure obligations, which are mainly contained in guidelines,*[76] *should be formalised in legislation.*[77] *It also made recommendations specifically on defence disclosures involving surveillance evidence. It recommended that where the prosecution relies on surveillance evidence (electronic or otherwise), the defence must disclose whether strict proof is required and if so, to what extent.*[78] *Furthermore, in respect of listening device transcripts proposed by the prosecution to be used or tendered, the Commission recommended that the defence should disclose whether the transcripts are accepted as accurate and, if not, in what respects issue is taken.*[79] *The Commission makes no further recommendations on this matter.*

9.59 Subsequent to the Commission's report on the right to silence,

---

73. NSWLRC Report 95 at para 3.90-3.91, 3.107.

74. Invasion of Privacy Act 1971 (Qld) s 45(2)(c); Listening Devices Act 1972 (SA) s 7(2); Listening Devices Act 1991 (Tas) s 9(2)(a); Surveillance Devices Act 1999 (Vic) s 11(2)(c), 12(b) and 12(c); Surveillance Devices Act 1998 (WA) s 9(2)(a).

75. NSWLRC Report 95.

76. See for example, New South Wales, Office of the Director of Public Prosecutions, Prosecution Guidelines: Issued December 1995 (Sydney, 1995).

77. NSWLRC Report 95 at para 3.98.

78. NSWLRC Report 95, Recommendation 5(f).

79. NSWLRC Report 95, Recommendation 5(h).

the NSW Parliament introduced the Criminal Procedure Amendment (Pre-trial Disclosure) Bill 2000, which would give courts the power to order, in criminal proceedings relating to the trial of a person on indictment, both the prosecution and the accused to undertake pre-trial disclosure.

9.60 The Commission is of the view that there is no need for provisions in the proposed surveillance legislation to deal with pre-trial disclosure of surveillance material. The provisions in the Criminal Procedure Amendment (Pre-trial Disclosure) Bill 2000, if enacted,[80] are wide enough to require the prosecution to disclose material obtained through surveillance that the prosecution proposes to use or is relevant at the trial, as well as to require the defence to give notice as the whether or not it accepts the accuracy of the proposed surveillance evidence.

SUPPRESSING THE PUBLICATION OF SURVEILLANCE EVIDENCE

9.61 The LDA, in section 13(4), gives courts the power to make suppression orders, that is, orders that limit what may be published about legal proceedings. Their function is to restrict publicity that may prejudice a fair trial or the administration of justice in general. The power given by section 13(4) is limited to orders for the non-publication of evidence obtained in breach of the LDA provisions.[81] Moreover, such orders can be made only in two situations:[82] for offences against the LDA or its regulations; and for offences punishable by penal servitude for life or for 20 years or more, [83] or a serious narcotics offence.[84]

---

80. The bill was passed in the Legislative Assembly on 23 November 2000 and was sent to the Legislative Council for concurrence. The Council passed the bill on 7 December 2000 with amendments and sent it back to the Assembly, which is considering the amended bill for concurrence.

81. LDA s 13(4).

82. LDA s 13(4).

83. Examples of these offences under the Crimes Act 1900 (NSW)

9.62 The common law has long recognised that a judge may, in certain circumstances, order reports of proceedings to be postponed where such an order would further the interests of justice.[85] *The general position as to whether and to what extent such a non-publication order may bind non-parties to the proceedings remains unclear in New South Wales.*[86] *There is dicta to the effect that courts do have the power to make orders, binding on those not present at court, which prohibit or postpone the reporting of what has been heard in open court.*[87] *However, in a number of other cases, such a power has also been doubted or denied.*[88] *Overall, the weight of common law authority in New South Wales seems to*

---

include murder (s 19A(1)), manslaughter (s 24), aggravated sexual assault (s 61J) and other serious sex offences (see s 61K, 66A, 66B, and 80A).

84. *A serious narcotics offence is defined in s 3 of the LDA as an offence under Div 2, Pt 2 of the Drug Misuse and Trafficking Act 1985 (NSW) or an offence that is punishable as provided by s 235 of the Customs Act 1901 (Cth).*
85. *R v Clement (1821) 4 B & Ald 218 at 233; 106 ER 918; Scott v Scott [1913] AC 417.*
86. *Attorney General (NSW) v Mayas Pty Ltd (1988) 14 NSWLR 342 at 348 (Mahoney J).*
87. *Ex parte Queensland Law Society Incorporated [1984] 1 Qd R 166 at 170 (McPherson J); Raybos Australia Pty Ltd v Jones (1985) 2 NSWLR 47 at 63 (Priestley J) which suggested that it was probable that the court had an inherent power to make such orders in rare situations; John Fairfax & Sons Ltd v Police Tribunal (NSW) (1986) 5 NSWLR 465 at 471-472 (Mahoney J); Attorney General (NSW) v Mayas Pty Ltd (1988) 14 NSWLR 342 at 345-347 (Mahoney J); Re Bromfield; Ex parte West Australian Newspapers Ltd (1991) 6 WAR 153 at 167 (Malcolm J) and at 180-181 (Rowland J).*
88. *Attorney General v Leveller Magazine Ltd [1979] AC 440; John Fairfax & Sons Ltd v Police Tribunal (NSW) (1986) 5 NSWLR 465 at 477 (McHugh J) (Glass J concurring); Raybos Australia Pty Ltd v Jones (1985) 2 NSWLR 47 at 55 (Kirby J); Attorney General (NSW) v Mayas Pty Ltd (1988) 14 NSWLR 342 at 355, 358 (McHugh J) (Hope J concurring); United Telecasters Sydney Ltd v Hardy (1991) 23 NSWLR 323 at 333-334 (Samuels J) (Meagher and Clarke JJ concurring); Re Savvas (1989) 43 A Crim R 331 at 334; Re "Mr C" (1993) 67 A Crim R 562 at 563 (Hunt J) (Smart and James JJ concurring).*

support the position that if courts have an inherent power to make non-publication orders, such an order will only be binding on the parties, witnesses and other persons present in the courtroom. It cannot apply to persons outside the courtroom (media persons, for example) who have no connection with the proceedings in question. The main argument against the existence of such a power is based on the separation of powers between the judiciary and the legislature: an order purporting to bind people generally is in the nature of an exercise of legislative power and therefore beyond the power of a court.[89]

9.63 Some statutory provisions in New South Wales empower tribunals or commissions to issue suppression orders in certain circumstances. The Administrative Decisions Tribunal,[90] *Royal Commissioners and others holding official inquiries of a similar nature*[91] *and the coroner*[92] *are among those who have the power to make suppression orders. In criminal proceedings, section 119 of*

---

89. *"Courts have no general authority, however, to make orders binding people in their conduct outside the courtroom. Judicial power is concerned with the determination of disputes and the making of orders concerning existing rights, duties and liabilities of persons involved in proceedings before the courts. An order made in court is no doubt binding on the parties, witnesses and other persons in the courtroom. But an order purporting to operate as a common rule and to bind people generally is an exercise of legislative – not judicial – power: John Fairfax & Sons Ltd v Police Tribunal (NSW) (1986) 5 NSWLR 465 at 477 (Mc Hugh J) (Glass J concurring).*
90. *Administrative Decisions Tribunal Act 1997 (NSW) s 75(2).*
91. *See Special Commission of Inquiry Act 1983 (NSW) s 7 and 8; Independent Commission Against Corruption Act 1988 (NSW) s 31.*
92. *The coroner may prohibit publication of evidence given at an inquest or inquiry if that would be in the public interest to do so having regard to the administration of justice, national security or personal security: Coroners Act 1980 (NSW) s 44(5) and 44(6); Fairfax Publications Pty Ltd v Abernethy [1999] NSWSC 820. Another power lies under s 44(2) for the coroner to order that no report of the proceedings be published in circumstances where a death or suspected death appears to be self-inflicted. Under s 44(2A) the coroner may also order that identifying particulars of the person concerned or relative of that person not be published.*

the Criminal Procedure Act 1986 (NSW) confers a power on any judge to make suppression orders forbidding publication of the evidence in proceedings before him or her. However, the power contained in section 119 is limited in that it applies only to criminal, not civil proceedings and only to proceedings for specific sexual offences. It is subject to the veto power of parties to the proceedings and cannot be invoked in preliminary proceedings like bail applications.

9.64 The Commission has recently published a Discussion Paper, Contempt by Publication ("DP 43"), which deals in part with suppression orders and includes a detailed analysis of section 578 of the Crimes Act 1900 (NSW), the precursor to section 119 of the Criminal Procedure Act 1986 (NSW). In DP 43, the Commission proposed the adoption of a new statutory provision which would grant any court in any proceedings the power to suppress the publication of reports of any part of the proceedings (including documentary material), where such publication would create a substantial risk of prejudice to the administration of justice. The proposed section is not intended to replace the common law or existing statutory powers (such as section 13(4) of the LDA) to restrict publication of court proceedings. The proposal is discussed in detail in Chapter 10 of DP 43. The Commission notes, however, that some of the issues discussed in DP 43 apply equally to the power to issue suppression orders contained in section 13(4) of the LDA. These issues include: the appropriate test for the exercise of the power; the power to suppress names; and the extent of the application of the power.

A test for the use of the power to issue suppression orders

9.65 The Commission considers it essential that any statutory power to issue suppression orders should be governed by a clear test. A possible test is whether the publication of the surveillance evidence will prejudice a fair trial. This test focuses on the potential risk of prejudice which the publication of the evidence may create in the minds of the jurors. An example of an application of this test is

where surveillance evidence which is damaging to persons not party to the proceedings, and who do not have an opportunity of rebuttal, is given in a pending proceeding. Where such persons are themselves the subject of separate proceedings, this evidence may prejudice the fairness of their future trial and publication may, therefore, need to be suppressed. Another example is the use of surveillance evidence in preliminary proceedings. If the media were permitted to report on the nature of evidence given at the preliminary hearing, there is a risk that potential jurors in the substantive proceedings will be made aware of, and be influenced by, material that is not subsequently admitted by the court as evidence in the substantive proceedings.

9.66 An alternative test for restricting the publication of surveillance material is whether it would be in the interests of, or in order to prevent prejudice to, the administration of justice. A number of jurisdictions in Australia and overseas have adopted this test, although in varying formulations.[93] This test is broader than the fair trial test as it looks at the issue of the fair and efficient administration of justice rather than the fairness of one particular proceeding. In DP 43, the Commission discusses the meaning of the administration of justice and how suppression orders may be used to protect it:

> *The administration of justice is a very broad term, which covers the detection, prosecution and punishment of offenders. Its proper administration requires not only that trials be fair, but that persons who can assist in its administration be encouraged to participate. Damaging personal publicity may have a negative effect on necessary requirements of the proper administration of justice such as the reporting of crimes, the institution of proceedings or the giving of testimony in court. Publication of court proceedings may also deter law enforcement or national security agencies from giving accurate testimony, where, for example, public knowledge of the details of secret operations or agents would undermine the efficacy of the work of the agency.*
>
> *The power of courts to issue suppression orders in terms of the*

93. NSWLRC DP 43 at para 10.59-10.63, 10.65-10.67.

> *"administration of justice" therefore incorporates both the need to prevent prejudice to a fair trial and the need to restrict publicity where this would be prejudicial to the judicial system generally because it would deter popular participation.*[94]

9.67 Consistent with the position taken in DP 43, the Commission favours the second of the alternative tests. The proposed surveillance legislation should allow the suppression of surveillance material where this is necessary to prevent substantial risk of prejudice to the administration of justice. The court should consider not just the potential prejudice to a particular trial as a result of the publication of surveillance material but also broader issues relating to the administration of justice, such as the risk of deterring participation in the particular, or similar, proceedings. For example, publication of evidence from covert surveillance by law enforcement officers may disclose details about ongoing similar operations which may jeopardise the investigations or compromise the safety of those involved such as police officers or informants, thereby discouraging them from testifying in court. Apart from police officers and informants, victims of certain crimes, for example blackmail, may be discouraged from participating in the process if the evidence is disclosed.

9.68 This is not to say that harm, hurt or embarrassment to individuals should be a sufficient basis for a suppression order.[95] *While these factors may be taken into account, the basis of any legislative power to issue suppression orders must be primarily to secure justice.*[96]

The power to suppress names as well as evidence

9.69 An order made under section 13(4) of the LDA operates only to

---

94. NSWLRC DP 43 at para 10.57-10.58 (footnotes omitted).

95. For a discussion on "undue hardship" as a basis for making suppression orders, see NSWLRC DP 43 at para 10.87-10.93.

96. See discussion in Raybos Australia Pty Ltd v Jones (1985) 2 NSWLR 47 at 61 (Samuels J).

suppress evidence, not names. Some New South Wales statutes contain a presumption in favour of non-publication of names in certain cases such as those involving children, participants in adoption and family law proceedings, or sexual offence complaints.[97] *The coroner can also suppress names as well as evidence where media reporting of such information would render impracticable the administration of justice.*[98] *Most other jurisdictions provide a general power for suppression of publication of identifying particulars as well as evidence.*[99] *Some jurisdictions specifically provide that the publication of identifying particulars of witnesses and of defendants may also be prohibited, irrespective of whether such publication would lead to identification of the complainant.*[100]

9.70 The Commission has formed the view that the power to make suppression orders under the new surveillance legislation should be extended to cover material which would lead to the identification of parties and witnesses, where suppression is necessary to prevent a substantial risk of prejudice to the administration of justice. The

---

97. *Children (Care and Protection) Act 1987 (NSW) s 68; Children (Criminal Proceedings) Act 1987 (NSW) s 11; Adoption of Children Act 1965 (NSW) s 53; Crimes Act 1900 (NSW) s 578A.*
98. *Coroners Act 1980 (NSW) s 44. See Mirror Newspapers Ltd v Waller (1985) 1 NSWLR 1 at 26 (Hunt J).*
99. *Evidence Act 1971 (ACT) s 83 (evidence and names); Evidence Act 1939 (NT) s 57 (evidence and names); Evidence Act 1929 (SA) s 68 and 69 (evidence and names); Magistrate's Court Act 1989 (Vic) s 126; County Court Act 1958 (Vic) s 80 and 80AA; Supreme Court Act 1986 (Vic) s 18 and 19 (report or information derived from proceedings, which includes names).*
100. *The provisions of the following Acts all relate to the prohibition of publication of identifying particulars in specific sexual offence cases: Criminal Law (Sexual Offences) Act 1978 (Qld) s 6 and 7 (complainant, defendant); Sexual Offences (Evidence and Procedure) Act 1983 (NT) s 6 and 7 (complainant, witness, defendant); Evidence Act 1910 (Tas) s 103AB (complainant, witness); Evidence Act 1929 (SA) s 71A (defendant or prospective defendant, complainant); Protection of the complainant only is afforded in the following jurisdictions: Evidence Act 1971 (ACT) s 76E; Judicial Proceedings Reports Act 1958 (Vic) s 4; Evidence Act 1906 (WA) s 36C.*

courts should be able to consider whether the publication of identities of witnesses and parties may for some reason, such as fears for their safety, deter them from participating in the particular or similar legal proceedings.

The extent of the application of the power

9.71 The power to issue suppression orders under section 13(4) of the LDA applies to very specific situations. The power cannot be used to prohibit the publication of surveillance evidence which was legally obtained. Nor can it be used in criminal proceedings other than those identified in the section and it cannot be invoked at all in civil proceedings.

9.72 There are clear arguments for suppressing the publication of illegally obtained evidence, especially in proceedings relating to the breach of the law. The non-disclosure of the evidence, as well as the identity of the victims of illegal surveillance, may be an effective means of encouraging the victims and other witnesses to participate fully in the prosecution of those who violated the legislation. However, if the standard for the issue of suppression orders is the prevention of substantial risk to the administration of justice, distinguishing between legally and illegally obtained surveillance evidence cannot be justified. The risk of prejudice in the publication of the evidence may occur regardless of how the evidence was gathered. Legally obtained surveillance evidence which incriminates X and Y, and is admitted in proceedings against X alone, may need to be suppressed to prevent a risk of prejudice in separate proceedings against Y. The publication of evidence from a covert surveillance operation conducted lawfully may cause a risk of prejudice to the administration of justice if parties or witness are deterred from participating in the process. The power to order the non-publication of surveillance material and the identity of participants in these proceedings should depend, not on whether the evidence was legally or illegally obtained, but on the risk of prejudice to the administration of justice which the publication of the evidence may create.

9.73 A distinction has also traditionally been drawn between civil

and criminal proceedings and the extent to which restrictions upon their openness should be imposed. This was based on the assumption that derogation from the principle of open justice in the criminal context should be more strictly controlled because the public has a greater interest and role to play in criminal proceedings. If members of the public were deterred by publicity and did not notify the commission of a crime or give testimony in court, a broader public interest was seen to be affected than if a person decided not to bring a civil action or aid in its adjudication.[101] *A greater public interest was also said to arise where there is some moral component in the wrongdoer being brought to justice.*[102]

9.74 However, this distinction between civil and criminal proceedings has been questioned.[103] *There are many civil issues such as discrimination, defamation and civil actions for assault, including sexual assault, which raise issues of great public interest and importance. The Commission's view is that the power of courts to restrict publication in matters such as these should be based on the same grounds as in criminal matters. The public interest in the proper administration of justice is equally important in such cases, and the courts should only be able to restrict reporting of court proceedings where publication would create a substantial risk of prejudice to the administration of justice.*

Recommendation 85

The proposed Surveillance Act should provide that any court, in any proceedings where evidence obtained through the conduct of surveillance is relevant or admitted in evidence, has the power to suppress the publication of reports of any part of the proceedings, where such publication would create a substantial risk of prejudice to the administration of

101. *See discussion in G Nettheim, "Open Justice Versus Justice" (1985) 9 Adelaide Law Review 488 at 492-493.*
102. *See discussion in M McDowell, "The Principle of Open Justice in a Civil Context" (1995) 2 New Zealand Law Review 214 at 223-224.*
103. *McDowell, "The Principle of Open Justice in a Civil Context".*

justice, either generally, or in relation to specific proceedings (including the proceedings in which the order is made). The power should apply in both civil and criminal proceedings and should extend to suppression of publication of the evidence as well as material which would lead to the identification of parties and witnesses involved in proceedings before the court. Breach of a suppression order should constitute a criminal offence.

SECURITY AND STORAGE OF COVERT SURVEILLANCE MATERIAL

9.75 The LDA does not deal with storage and security of material obtained as a result of the use of a listening device. This can be contrasted to the covert use of video cameras in the workplace where the regulation under the Workplace Video Surveillance Act 1998 (NSW) requires that the licensed security operator who conducts the covert surveillance for the employer should take all reasonable "security safeguards" to ensure that the material is "protected from loss or unauthorised access.[104] *The Workplace Video Surveillance Act 1998 (NSW) itself contains provisions designed to protect the security of the video recordings by: (a) restricting what the security operator may supply to the employer to only such portion of the video recordings as is relevant to the suspected involvement of the employee in an unlawful activity in the workplace; and (b) prohibiting the operator from giving any other person access to the video recordings.*[105]

9.76 Surveillance legislation in some other Australian States provides for secure storage. For example, the Surveillance Devices Act 1999 (Vic) provides that the chief law enforcement officer in an investigation must ensure that every record or report obtained by the use of a surveillance device "is kept in a secure place that is not accessible to people who are not entitled to deal with the record or

104. Workplace Video Surveillance Regulation 1999 (NSW) s 9.
105. Workplace Video Surveillance Act 1998 (NSW) s 17(1).

report".[106] The legislation in South Australia and Western Australia contain provisions which use very similar language.[107]

9.77 Recent changes to the law in the United Kingdom contain a requirement that the Secretary of State make such arrangements as he or she considers necessary to ensure that the storage of covert surveillance material (and copies of such material) is secure.[108] The relevant legislative provisions in the United States require that material obtained pursuant to a surveillance warrant be "sealed" immediately after the expiration of the warrant (or extensions thereof) by the issuing judge.[109] The judge who seals the record also makes provision for its safe custody.[110]

9.78 There are two reasons for making legislative provision for the secure storage of material obtained by covert surveillance. The first is to protect the confidentiality of the material, and thus the privacy of the persons subject of the surveillance.[111] People who are not entitled to deal with the record or report should be prevented from gaining access to it. The second rationale is to protect the reliability and integrity of the material. The United States Supreme Court has stated that the relevant US provisions are directed at preventing law enforcement agencies from having an opportunity to tamper, alter or edit the recorded conversations.[112]

9.79 The protection of individual privacy, within the constraints of a realistic legal framework for surveillance, as well as the need to ensure the integrity of material obtained by surveillance, requires provision for safe storage to be included in the proposed surveillance legislation.

---

106. Surveillance Devices Act 1999 (Vic) s 36(1).
107. Listening Devices Act 1972 (SA) s 6c(a); Surveillance Devices Act 1998 (WA) s 41(1)(a).
108. Regulation of Investigatory Powers Act 2000 (UK) s 15(5).
109. 18 USC s 2518(8)(a).
110. 18 USC s 2518(8)(a).
111. For the privacy rationale for the storage of surveillance material in the private/workplace context, see New South Wales, Privacy Committee, Invisible Eyes: Report on Video Surveillance in the Workplace (Report 67, 1995) at para 4.2.
112. US v Rios 495 US 257 (1990).

Recommendation 86

The proposed Surveillance Act should provide that a person who has obtained material through the conduct of surveillance must ensure that the material and all copies, extracts, summaries or reports of it must be kept in a secure place that is not accessible to people who are not entitled to deal with it. Breach of this requirement should be an offence.

DESTRUCTION OF SURVEILLANCE INFORMATION

9.80 Section 22 of the LDA provides that "a person shall, as soon a practicable after it has been made, cause to be destroyed so much of the record, whether in writing or otherwise, of any evidence or information obtained by the person by the use of a listening device … as does not relate directly or indirectly to the commission of a prescribed offence."

9.81 Section 22 presents a number of difficulties. The first relates to its restricted coverage. It applies only where a listening device is used: (a) pursuant to a warrant; or (b) in connection with (i) an imminent threat of serious violence to persons or of substantial damage to property, or (ii) a serious narcotics offence, if it is necessary to use the device immediately to obtain evidence or information.[113] It does not apply to other circumstances where use of a listening device without a warrant is authorised by the LDA.[114]

113. LDA s 22(1).

114. These include: (a) the unintentional hearing of a private conversation by means of a listening device; (b) when a listening device is used to record a refusal to consent to the recording of an interview by a member of the police force in connection with the commission of an offence; (c) when all the principal parties to the conversation consent, expressly or impliedly, to the listening device being so used; or (d) when a principal party to the conversation consents to the device being used under specific circumstances listed in s 5(3)(b) of the LDA.

Hence, for example, a recording by the police of a refusal by a suspect to consent to the recording of an interview need not be destroyed, regardless of whether the police proceed with the investigation or not.

9.82 Section 22 also does not apply to illegally obtained material. The LDA has not provided for the destruction of this type of material. Consequently, if the police recorded a private conversation in breach of the LDA, they are not required to destroy the recording even if it turns out to be irrelevant for the purposes of an investigation or subsequently ruled by the court to be inadmissible.

9.83 It is unclear why section 22 applies to certain cases where the listening device was used lawfully but not in others. Neither is there an apparent policy reason why its intended benefit does not extend to information obtained illegally. If the aim is to minimise the unnecessary storage of information about individuals and to discard that which is not relevant for any purpose, then a "destruction" provision such as section 22 should apply in every case, regardless of the manner in which the surveillance was conducted.

9.84 Another issue with respect to section 22 relates to the basis for the destruction of the recorded conversation. Under section 22, the recording of the conversation will be destroyed if the person who used the listening device has determined that the recording is not relevant to the commission of a prescribed offence. The surveillance legislation of most of the other Australian States and territories similarly makes the destruction of surveillance material depend upon whether it is relevant to the offence for which use of the device was authorised.[115] This, however, fails to consider that the material may have other uses. If for example, the surveillance was conducted illegally, the surveillance material may be used as evidence in the proceedings prosecuting the illegality. Moreover, if the Commission's recommendations in this report on a civil right of action in respect of a breach of the surveillance legislation are adopted,[116] the material will be relevant to such an action.

115. See para 9.87-9.89.
116. See ch 10.

The material may also be relevant to disciplinary proceedings, if any are available, which may be taken against the persons who conducted the surveillance illegally. The "destruction" provision in the Surveillance Devices Act 1999 (Vic), for example, recognises the relevance of surveillance material in disciplinary proceedings.[117]

9.85 The concern to prevent destruction of material which might assist the subject of the surveillance, either in a civil or in a criminal context, is the basis for the provision in the United States which prohibits, rather than provides for, destruction. Section 2518(8)(b) of the United States Code provides that surveillance records are not to be destroyed except on the order of a judge, and not before ten years have elapsed.[118]

9.86 Another important issue which the LDA does not address is the destruction of relevant material once it is no longer relevant. Recordings of private conversations which are useful to a police investigation need not be destroyed under section 22 because they relate to an offence. If, however, the material turns out to be irrelevant for prosecution purposes, it is unclear whether the police and the prosecution officers are under an obligation to destroy them. It appears, however, that material which may have been relevant, and in fact used in criminal proceedings, may be retained after the proceedings have terminated. The police can hold indefinitely recordings of private conversations even if the accused was acquitted of the charges. While the law correctly provides for the destruction of surveillance material which are irrelevant from the start as a way of minimising the effects of the intrusion on the subject's privacy, the law should likewise provide for the destruction of relevant material once it ceases to have any purpose.

The law in other Australian jurisdictions

9.87 The "destruction" provisions in the surveillance legislation in Tasmania and Queensland use terms similar to section 22 of the LDA: recordings of private conversations should be destroyed if they

117. Surveillance Devices Act 1999 (Vic) s 36(1)(b).
118. 18 USC s 2518(8)(b).

do not relate directly or indirectly to the commission of an offence.[119] *In South Australia, Western Australia and the Northern Territory, the relevant chief law enforcement officer is required to destroy material where it is not likely to be required in connection with: the investigation in respect of which the warrant (or the emergency authorisation) was issued (or the investigation of another offence); the making of a decision whether or not to prosecute for any offence; or the prosecution of any offence.*[120] *The destruction provisions in these States provides a clearer guidance for the destruction of surveillance material by specifying the purposes for which the material may be relevant. Furthermore, it gives a more precise test for determining relevance – whether or not the material is not likely to be required in the specified relevant purposes.*

9.88 The Surveillance Devices Act 1999 (Vic) applies the same test as that applied in the South Australian, Western Australian and Northern Territory legislation, but identifies a broader number of proceedings where the surveillance material may be relevant by including: the making of an application under its law on the confiscation of profits from criminal offences; and any disciplinary proceedings.[121]

9.89 None of the surveillance legislation of the other Australian jurisdictions makes provision for the eventual destruction of relevant surveillance material.

9.90 At the Commonwealth level, the Customs Act 1901 (Cth) provides that the chief officer of a Commonwealth law enforcement agency which receives a surveillance warrant is required to destroy surveillance records where he or she is satisfied that they will not assist in narcotics inquiries or are not likely to be required in connection with a relevant proceeding.[122] *The Australian Federal*

---

119. Listening Devices Act 1991 (Tas) s 21(2); Invasion of Privacy Act 1971 (Qld) s 47.

120. Listening Devices Act 1972 (SA) s 6c(b); Surveillance Devices Act 1998 (WA) s 41(1)(b); Surveillance Devices Act 2000 (NT) s 36(b).

121. Surveillance Devices Act 1999 (Vic) s 36(1)(b).

122. Customs Act 1901 (Cth) s 219G.

Police Act 1979 (Cth) contains the same provisions in relation to offences generally.[123] *The Interception Act requires the chief officer of the agency conducting the surveillance to destroy the restricted record where the officer is "satisfied that the restricted record is not likely to be required for a permitted purpose in relation to the agency".*[124] *However, this provision in the Interception Act differs from corresponding provisions in other Australian legislation in that it provides for supervision by the Minister for Police and makes provision for the destruction of records which are illegally, as well as legally, obtained.*[125]

The law in foreign jurisdictions

9.91 In Canada, the agent of the State who intercepts a private communication in order to prevent bodily harm, is required to destroy, as soon as practicable, any material or notes relating to that interception if nothing in the private conversation suggests that actual, attempted or threatened bodily harm has occurred, or is likely to occur.[126]

9.92 The Crimes Act 1961 (NZ) makes a distinction between relevant and irrelevant material. The law requires the Commissioner of Police to destroy every record of the information lawfully obtained through a listening device and which relates to the offence for which a warrant or emergency permit was granted "as soon as it appears that no proceedings, or no further proceedings, will be taken in which the information would be likely to be required to be produced in evidence."[127] *Under this provision,*

123. *Australian Federal Police Act 1979 (Cth) s 12L(aa).*
124. *Telecommunications (Interception) Act 1979 (Cth) s 79(1)(b); see the definition of "permitted purpose" in the definition section.*
125. *Section 79(1) of the Telecommunications (Interception) Act 1979 (Cth) makes provision for the destruction of "restricted records", which are defined as "a record obtained by means of interception, whether or not in contravention of s 7(1), of a communication passing over a telecommunications system".*
126. *Criminal Code 1985 (Canada) s 184(3).*
127. *Crimes Act 1961 (NZ) s 312J(1); Misuse of Drugs Act 1975 (NZ)*

material which was relevant to the investigation must be destroyed as soon as it becomes clear that it will not be required in criminal proceedings. The requirement also operates where the material was used in a trial but the proceedings (including appeal proceedings) have terminated. On the other hand, the law requires the destruction of irrelevant material at an earlier stage by providing that every person who lawfully intercepts a private communication in pursuance of an interception warrant or any emergency permit, shall, as soon as practicable after it has been made, destroy information that does not relate directly or indirectly to the commission of an offence for which a listening device may be used.[128]

9.93 In the United Kingdom, general safeguards in the Regulation of Investigatory Powers Act 2000 (UK) require that intercepted material and any related communications data be destroyed "as soon as there are no longer any grounds for retaining it as necessary for the authorised purposes".[129]

Submissions and Response

9.94 In Issues Paper 12 ("IP 12"), the Commission raised two issues with respect to the destruction of surveillance evidence. The first was whether information obtained illegally pursuant to a listening device warrant should be destroyed if it is excluded from

---

s 22(1).

128. *The Crimes Act 1961 (NZ) s 312I(1) provides that: "Every person who intercepts a private communication pursuant to a warrant or an emergency permit shall, as soon as practicable after it has been made, destroy any record, whether written or otherwise, of the information obtained by the interception if none of the information directly or indirectly relates to the commission of an offence described in s 312B(1) of this Act [relating to the issuing of interception warrants] or a drug dealing offence." The Misuse of Drugs Act 1975 (NZ) s 21 is in the same terms, but requires destruction if the information does not relate to a drug dealing offence.*
129. *Regulation of Investigatory Powers Act 2000 (UK) s 15(3).*

trial on that basis.[130] *Submissions on this issue were divided.*

9.95 The Director of Public Prosecutions ("DPP") submitted that "mandatory destruction of illegally obtained material could potentially prejudice ongoing or future police investigation or future prosecutions or other related proceedings (for example, confiscation proceedings or disciplinary proceedings)".[131] *However, the DPP is in favour of the inclusion of a provision which permits the destruction of illegally obtained material after a specified period, subject to provision being made for cases where the significance of particular material changes in light of new circumstances, or having regard to information not known to those initially assessing the material.*[132]

9.96 The New South Wales Crime Commission, the Independent Commission Against Corruption, the Police Integrity Commission and the National Crime Authority, in their joint submission opposed compulsory destruction of illegally obtained surveillance for the following reasons:

- *There may be an appeal of the decision which found the material illegal;*
- *Material may be required in trial of co-defenders or an unrelated matter such as a Royal Commission;*
- *Evidence ruled inadmissible in a criminal trial may nevertheless be admitted in civil confiscation proceedings, tribunals and examinations in other jurisdictions or in hearings conducted by an agency; or may be relevant to an investigation being conducted by an agency. The relevance of a piece of listening device material may not become evident until much later.*[133]

However, this submission also expressed the view that "it should be

---

130 New South Wales Law Reform Commission, Surveillance (Issues Paper 12, 1997) Issue 15.

131. Director of Public Prosecutions, Submission at 5.

132. Director of Public Prosecutions, Submission at 5.

133. NSW Crime Commission (NSWCC), Independent Commission Against Corruption (ICAC), Police Integrity Commission (PIC) and National Crime Authority (NCA) ("Joint Law Enforcement Agencies"), Submission at 6.

permissible to destroy material where the agency head or a senior officer with delegated authority determines on the basis of specified criteria that it is appropriate to do so".

9.97 The NSW Police Special Services Group submitted that no agency wishes to retain information unnecessarily. It favoured a provision which permits, but does not require, the destruction of illegally obtained information within a specified period. It said that requiring the destruction of such information should not be compulsory as it may be relevant in appeal proceedings, civil proceedings, or where such information may be relevant in another unrelated matter.[134] It suggested that the material should not be confiscated for a period of five years.[135]

9.98 Judge Sides QC (formerly Senior Public Defender) drew a distinction between material which is presented in court as evidence and that which never reaches the court. For material used in court proceedings, he argued that the court should be given the power to destroy those parts of the information that have been ruled inadmissible. For information not used in legal proceedings, Judge Sides stated that its destruction should be required after a specific period.[136]

9.99 Price Waterhouse submitted that evidence obtained illegally, excluded from trial for that reason, should be considered for destruction on a case by case basis by either the presiding trial judge or a Supreme Court judge. It suggested that arguments for preserving the integrity of our legal system by destroying illegally obtained evidence may have to give way to considerations of the overall public good.[137]

9.100 The Registered Clubs Association approved of the destruction of video surveillance which has been obtained illegally and excluded from trial, subject to the need to retain the

134. NSW Police Service, Special Services Group, Submission at 6.
135. NSW Police Service, Special Services Group, Submission at 6.
136. M L Sides, Submission at 16.
137. Price Waterhouse, Submission at 9

information for other proceedings.[138]

9.101 The Privacy Committee saw no justification for keeping illegally obtained evidence rejected by the court and submitted that it should be destroyed as it has the potential to be extremely damaging to subject.[139] *The NSW Council for Civil Liberties submitted that all illegally obtained evidence should be "destroyed by court officers, with stiff penalties for the retention of such information."*[140]

9.102 The related issue raised in IP 12 was whether a specific period of time should be inserted for the destruction of records made from information obtained through a listening device used in accordance with the LDA. This was raised out of concern as to whether the phrase "as soon as practicable" in section 22 of the LDA "is sufficient, or whether a finite period of time should be included."[141] *The submissions were divided on this issue.*

9.103 The Privacy Committee favoured destruction within a specified period after the surveillance, providing the records are not intended to be used in criminal proceedings.[142] *The NSW Young Lawyers Criminal Law Committee expressed the same view.*[143] *The Law Society of NSW submitted that the period within which records should be destroyed should be two years.*[144] *Judge Sides submitted that legislation should provide for the destruction of records within six or twelve months where prosecution has not been instituted.*[145] *The NSW Police Special Services Group submitted that destruction should be at the discretion of the senior investigator for a period of up to five years, with automatic destruction thereafter.*[146]

---

138. Registered Clubs Association of NSW, Submission at 5.
139. Privacy Committee of NSW, Submission at 25.
140. NSW Council for Civil Liberties, Submission at 5.
141. NSWLRC IP 12 at para 5.49, Issue 23.
142. Privacy Committee of NSW, Submission at 27
143. NSW Young Lawyers Criminal Law Committee, Submission at 7.
144. Law Society of NSW, Submission at 6.
145. M L Sides, Submission at 16.
146. NSW Police Service, Special Services Group, Submission at 11.

9.104 On the other hand, Price Waterhouse submitted that there should be no specific time set for destruction of material other than "as soon as practicable" because further information may come to light which may, in conjunction with the surveillance material, be relevant to the investigation and prosecution of a crime.[147] *The Registered Clubs Association favoured keeping records as long as there is a real prospect of claims (such as unfair dismissal and insurance fraud) being filed based upon the information.*[148] *The New South Wales Crime Commission, the Independent Commission Against Corruption, the Police Integrity Commission and the National Crime Authority, in their joint submission, were not in favour of a specific time period for the destruction of records.*[149] *The Director of Public Prosecutions was of the same view, arguing that the significance of particular material may change in light of future circumstances, or having regard to information not known to those initially assessing the material.*[150]

Conclusion

9.105 The Commission agrees with the underlying policy of section 22 of the LDA, requiring the immediate destruction of surveillance information which is not relevant to an offence. However, the Commission considers that the requirement should apply not just to the cases specified in section 22 but in all cases where surveillance is conducted, whether authorised or not.

9.106 The LDA does not currently provide for the destruction of material which, although initially relevant, subsequently becomes irrelevant or which has simply served its purpose. Surveillance legislation should regulate these situations. Information about individuals should only be stored for as long as there is justification for doing so. For example, law enforcement officers should not be able to hold surveillance information about a person once a decision not to prosecute has been made or once the proceedings where the

147. *Price Waterhouse, Submission at 12.*
148. *Registered Clubs Association of NSW, Submission at 7.*
149. *Joint Law Enforcement Agencies, Submission at 10.*
150. *Director of Public Prosecutions, Submission at 5 and 8.*

material may have been relevant have terminated.

9.107 The Commission is also of the view that the destruction of surveillance material should not be based solely on whether or not it is relevant to the offence for which the device was authorised. Section 22 of the LDA assumes that the material is only relevant to the persons who conducted the surveillance. The proposed surveillance legislation should recognise that surveillance material may be relevant for other purposes. In particular, where the surveillance involved an offence or a breach of some kind, the material may be relevant in criminal, civil, administrative or disciplinary proceedings that may be taken as a result of the wrongdoing. The law should ensure that material that is relevant in those proceedings should only be destroyed when the proceedings are finalised.

9.108 In connection with surveillance pursuant to a public interest or employment authorisation, the purpose may not be to investigate or prosecute offences. For example, a public interest authorisation may be granted to a private investigation agency which is investigating an insurance fraud. The test for the relevance of the information obtained through the warrants system will not be applicable to information gathered through public interest and employment authorisations. The Commission considers that this type of information, and every record of it, should be destroyed when it appears that: the material is not likely to be relevant or useful to the purpose for which the authorisation was issued; or the purpose for which the authorisation was issued has been accomplished.

9.109 The subject of the surveillance who obtains possession of surveillance information solely about him or her need not be bound by the same requirements to destroy the material. There can be no policy objections to an individual retaining information about himself or herself, unless the information affects or concerns another person.

Recommendation 87

The proposed Surveillance Act should provide that every person who obtains information through the conduct of surveillance is required to destroy the information and any record of it as soon as it appears that none of the information directly or indirectly relates to the commission of an offence.

The proposed Surveillance Act should also provide that every person who obtains information through the conduct of surveillance that relates wholly or partly to the commission of an offence is required to destroy the information and any record of it as soon as it appears that no investigations or proceedings will be taken in which the information would be likely to be relevant.

The requirements in these provisions should apply in all cases where information is obtained through the conduct of surveillance, whether the surveillance is authorised or not.

These provisions should be subject to three provisos:

(1) The information should not be destroyed if the person who obtained it is notified that it may be required in criminal, civil, administrative or disciplinary proceedings in connection with the breach of the proposed Surveillance Act. In such case, the information should be destroyed as soon as the proceedings are terminated or it becomes clear that none of them will proceed.

(2) Where the information was gathered under the authority of a public interest or employment authorisation, the information and every record of it should be destroyed as soon as it appears that:

- **the material is not likely to be relevant or useful to the purpose for which the authorisation was issued; or**
- **the purpose for which the authorisation was issued has been accomplished.**

(3) A person who was the subject of surveillance need not destroy the information about him or her obtained as a result of the surveillance and which is in his or her possession unless the information affects or concerns another person.

Information obtained through the conduct of surveillance should not be retained for a period of more than 5 years, unless it remains relevant as provided in the preceding paragraphs. Where information is stored for such length of time, the relevant organisation should conduct periodic reviews to confirm that the justification for its retention remains valid.

The proposed Surveillance Act should provide that the requirements to destroy surveillance information do not apply to material which has been received into evidence in legal proceedings.

Breach of these provisions should constitute an offence.

10. Breaches of the Surveillance Act

- Overview
- Criminal offences and civil breaches
- Complaints and review procedures
- Sanctions and remedies

OVERVIEW

10.1 There are currently very few regimes, either at common law or in statute law, proscribing behaviour related to, and arising out of, surveillance, or remedies or channels of complaint available for those adversely affected by surveillance activities. Except as noted below, neither is there a legislated framework for reviewing surveillance systems and operation.

10.2 The Surveillance Devices Act 2000 (NT) proscribes the attachment, installation, use, maintenance or retrieval of a "surveillance device"[1] unless authorisation is given under the Act.[2] However, the Act then provides for exceptions to this blanket prohibition.[3] Criminal penalties are imposed for offences against the Surveillance Devices Act 2000 (NT).[4] The Act does not make provision for a complaints mechanism, nor remedies, for persons adversely affected by surveillance activities.

10.3 The Listening Devices Act 1984 (NSW) ("LDA") contains provisions governing offences against the LDA or its regulations, and prescribes penalties for convictions.[5] Offences under the LDA arise out of the use of "listening devices" to listen to private conversations. The only other legislation determining offences arising out of aural surveillance is Commonwealth legislation applying to Commonwealth bodies,[6] although one of these statutes also covers New South Wales agencies using telephone interception

1. *As defined in s 3.*
2. *Surveillance Devices Act 2000 (NT) s 5.*
3. *Surveillance Devices Act 2000 (NT) s 6, 7.*
4. *Surveillance Devices Act 2000 (NT) s 5, 38-41, 45.*
5. *LDA s 10-11, 24-26, and 29-30.*
6. *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 surveillance devices by members of the Australian Security Intelligence Organization is regulated by the Australian Security Intelligence Organisation Act 1979 (Cth) s 26.*

devices to investigate offences under New South Wales law.[7] *In each case, breach of the legislation is a criminal offence attracting criminal penalties. In addition, the Telecommunications (Interception) Act 1979 (Cth) ("Interception Act") makes provision for an "aggrieved person" to apply for civil remedies.*[8] *The LDA contains no such provision for civil remedies.*

10.4 There is presently no legislation in New South Wales regulating other types of surveillance, except for covert use within the workplace.[9] *At common law, remedies are available in certain circumstances for conduct which may be connected with the surveillance, including trespass, nuisance, defamation and breach of confidence. These remedies will be inapplicable in the majority of cases and, for the reasons outlined at paragraphs 1.50-1.56 may provide unsatisfactory sanctions and relief in other cases. More importantly, there is no general law directly and specifically regulating the use of surveillance devices and providing redress for persons affected by the misuse of such devices.*[10]

10.5 This chapter considers the consequences of infringing provisions of the proposed surveillance legislation, recommends avenues of complaint and review of alleged breaches and appropriate remedies where a breach is established. As explained in Chapter 2, the Commission makes a distinction between overt and covert surveillance for the purposes of devising a regulatory framework. It follows from this approach that offences and sanctions should be related to whether the surveillance in question was overt or covert and should not depend on the type of

---

7. *Telecommunications (Interception) Act 1979 (Cth) s 105-107. The relevant agencies are the New South Wales Police Service, the New South Wales Crime Commission, the Independent Commission Against Corruption and the Royal Commission into the New South Wales Police Service.*
8. *Telecommunications (Interception) Act 1979 (Cth) s 107A-107F. An "aggrieved person" is a person who was a party to the communication the interception of which contravened s 7 of the Act, or the relevant communication was made on the person's behalf.*
9. *See the discussion at para 1.38. See Workplace Video Surveillance Act 1998 (NSW).*
10. *See para 1.56.*

surveillance device which was in use.

10.6 In summary, the Commission recommends a three-fold approach:

- *Where surveillance is overt, a breach of the applicable sections of the proposed Surveillance Act would give rise to civil liability; a complaint in respect of the surveillance would first be conciliated by the Privacy Commissioner and then heard by a specialist division of the Administrative Decisions Tribunal ("ADT"), which would have the power to order a range of remedies, not limited to compensation.*
- *Where surveillance is covert, breaches should be dealt with by criminal proceedings and criminal sanctions should apply; in addition, a person aggrieved would have access to the remedies and review mechanisms available in the case of overt surveillance.*
- *Where the surveillance has taken place in the context of employment, a person who suffers damage as a result of the surveillance can elect to seek redress in either the Industrial Relations Commission ("IRC") or through the Privacy Commissioner and the ADT.*[11]

10.7 Instigating action for relief under the proposed Surveillance Act would not preclude litigating a common law action in respect of the surveillance.

Codes of practice

10.8 The Commission is of the view, outlined at paragraphs 2.86 and Chapters 3 and 4, that regulation of surveillance should be, primarily, by legislation, supplemented by voluntary codes of practice. Breaches, or threatened breaches, of the legislation would be litigated, or prosecuted, in accordance with the mechanisms provided for in the legislation and give rise to the prescribed

11. See discussion at para 10.39-10.51 below. A person aggrieved by workplace surveillance could seek relief in each of the two forums, providing there is no duplication of remedies obtained.

penalties and remedies. Under the proposed Surveillance Act, a voluntary code setting out standards of practice for an industry, or a section of an industry, would not be enforceable. Relief under the legislation for breaches of codes not amounting to breaches of surveillance legislation could not be sought, nor could sanctions be imposed. However, assuming a code of practice is drafted so as to accord with the legislation, it is probable that conduct breaching the code would likewise breach the legislation. Furthermore, it is difficult to envisage a case where a breach of a code resulted in damage of some kind, or interference with privacy, and did not also amount to a breach of the legislation.

10.9 That is not to say that a code of practice could not itself stipulate that disputes arising under the code are to be resolved by the application of the statutory complaints and review processes, or that the statutory remedies are to be available for breaches of the code. Similarly, a code of practice could formulate its own dispute resolution mechanisms for breaches of the code, including providing for access to Alternative Dispute Resolution schemes.

CRIMINAL OFFENCES AND CIVIL BREACHES

Overt surveillance

10.10 Pursuant to the Commission's proposed regulatory framework, breaches of the provisions governing overt surveillance, together with breaches of the principles enunciated in the proposed legislation,[12] will give rise to civil liability and will bring into operation the complaints and review mechanisms discussed in paragraphs 10.25-10.35 below. A person aggrieved by a breach, or a threatened breach, will have recourse to the civil and equitable remedies outlined in paragraphs 10.52-10.63.

Recommendation 88

12. See ch 4.

A breach of an overt surveillance provision of the proposed Surveillance Act should give rise to civil liability.

Covert surveillance

10.11 In the Commission's view, breaches of the provisions regulating covert surveillance should constitute criminal offences for the reason that covert surveillance is potentially more intrusive than surveillance carried out overtly. One of the principles which the Commission recommends should be contained in surveillance legislation is that a person has a reasonable expectation of privacy.[13] When surveillance is covert, the breach of this reasonable expectation is so much greater; if the breach of privacy has come about because of illegally conducted covert surveillance, the offender should be punished more severely than if the surveillance had been overt.

10.12 The Commission has recommended in Chapter 5 substantially adopting the provisions of the LDA to regulate covert surveillance generally, irrespective of the type of device in use. In following this approach, covert surveillance could only be carried out with authorisation, either pursuant to a warrant, or authority granted by or under the Interception Act or any other Commonwealth law, or granted by a panel established under the ADT or granted by the IRC.

10.13 It follows that any covert surveillance carried out without such authorisation would constitute an offence. Furthermore, if the terms of the authorisation are breached, including terms governing the release of information obtained, this would also give rise to an offence. Exceptions to this general position would arise in the circumstances set out in Chapter 9. The Commission has also recommended that the proposed legislation contain provisions requiring reporting of the results of covert surveillance.[14] Breaches of these provisions would attract criminal sanctions.

---

13. See ch 4 at para 4.41-4.43.

14. See ch 8.

10.14 Chapter 5 recommends that the eligible judge should have the power to authorise the warrant-holder to employ all reasonable means necessary in order to gain entry to premises where the surveillance devices are to be installed, retrieved, repaired, tested, moved, maintained or replaced, as well as other premises where the warrant-holder has been authorised to enter for those purposes, whether or not the means employed would otherwise amount to damage to property or trespass.[15] The Commission recommends that the legislation create an offence of "unreasonable force" where the means employed in the execution of the warrant are found to be unreasonable. It should also be an offence for a person unreasonably to obstruct a warrant-holder from exercising the authority given to him or her by the warrant.

10.15 The Irish Law Reform Commission in its Report on Privacy recommended creating three new criminal offences targeting "invasions of privacy in well-defined circumstances where the expectation of privacy is at its highest (ie, on a private dwelling) or where the activity in question (ie, conversations) is inherently private".[16] The recommended offences are: installing a surveillance device in a private dwelling or engaging in surveillance of a private dwelling; trespass done for the purpose of surveillance; and using devices to spy on private conversations.[17]

10.16 These offences all impliedly relate to covert surveillance. In our recommended framework, if for all covert surveillance authorisation is required, a threshold test must be satisfied that the surveillance, as well as any attendant entry onto property, is necessary or justified according to the provisions of the legislation regulating the granting of authorisation. This approach makes it unnecessary to imitate the Irish Law Reform Commission model and identify situations of particular vulnerability or sensitivity for the imposition of prohibitions on covert surveillance.

---

15. *Recommendation 33.*
16. *Ireland, Law Reform Commission ("ILRC"), Report on Privacy: Surveillance and the Interception of Communications (Report 57, 1998) at para 9.04.*
17. *ILRC at para 9.06-9.012.*

Recommendation 89

A breach of a covert surveillance provision of the proposed Surveillance Act should constitute a criminal offence.

Workplace surveillance

10.17 The Commission proposes that the framework applying to overt and covert surveillance would essentially apply to surveillance in the workplace, including the provisions governing breaches and offences, but with some extensions and modifications. The reasons for distinguishing workplace surveillance are set out at paragraph 2.108.

10.18 There are two main areas where it is proposed that regulation of surveillance in the workplace will differ from regulation of surveillance generally. First, if it is intended that the surveillance be overt, the Commission recommends that employees must have "actual knowledge" of the surveillance.[18] The reasons for imposing this additional requirement are set out at paragraph 2.80. Just as anyone carrying out overt surveillance must do so in accordance with the eight principles contained in the legislation,[19] or incur civil liability for breaches, employers will be liable for breaches of these principles.

18. *Actual knowledge will be imparted by giving at least 14 days' notice in writing (or a shorter period if agreed to by the employer and employee, or someone acting on behalf of an employee, namely an industrial organisation) that the surveillance will commence: see ch 2 at para 2.81.*
19. *See ch 4 at para 4.38-4.66.*

10.19 If an employee does not have "actual knowledge", the surveillance will be deemed covert and consequently regulated by the covert surveillance provisions. The second main area where the regulation of workplace surveillance will be distinguished from regulation of surveillance generally is in relation to authorisations. Although employers will need to obtain authorisation to carry out covert surveillance in the workplace, in the same way as all covert surveillance must be authorised, it is proposed that an authorisation will only be granted if the surveillance is for one of three specified purposes. That is, the Commission recommends that an employer will only be entitled to obtain a covert surveillance authorisation if:

- *unlawful activity on work premises is reasonably suspected;*
- *employment-related unlawful activity is reasonably suspected; or*
- *serious misconduct justifying summary dismissal is reasonably suspected.*[20]

10.20 Covert surveillance carried out without authorisation, or for a purpose different from one of the above three purposes, would constitute a criminal offence. In this regard, the Commission proposes that regulation of covert workplace surveillance be modelled on the Workplace Video Surveillance Act 1998 (NSW) ("Workplace Video Surveillance Act") and that similar offence provisions be adopted in the new surveillance legislation.

10.21 There are three main offence provisions in the Workplace Video Surveillance Act which could guide the drafting of offences in the proposed Surveillance Act. Subject to a number of exceptions,[21] *section 7 prohibits covert video surveillance of an employee unless it*

---

20. Recommendation 58. These purposes are explained fully at para 7.52-7.54. See ch 7 for a full discussion of covert surveillance in the workplace.

21. These relate to surveillance by a law enforcement officer, surveillance of correctional centres or offenders in custody, surveillance under the Casino Control Act 1992 (NSW) and surveillance of legal proceedings or proceedings before a law enforcement agency.

is carried out solely for the purpose of establishing whether or not the employee is involved in any unlawful activity in the workplace.

10.22 Section 8 makes it a criminal offence to use a recording obtained by covert video surveillance for an irrelevant purpose. An "irrelevant purpose" is defined by the Workplace Video Surveillance Act to include a purpose not directly or indirectly related to:

- *establishing whether or not an employee is involved in unlawful activity in the workplace;*
- *taking disciplinary action or legal proceedings against an employee as a consequence of the established unlawful activity; or*
- *establishing security arrangements or taking other measures to prevent or minimise the opportunity for the unlawful activity identified by the surveillance.*[22]

10.23 The use by an officer of a law enforcement agency of a recording for any purpose relating to the detection or investigation of an unlawful activity of a person other than an employee in the workplace is excepted from the general prohibition.

10.24 Section 9 makes it clear that an employer cannot obtain authorisation to carry out covert video surveillance for the purpose of monitoring an employee's work performance or to carry out surveillance of an employee in any toilet facility or shower or other bathing facility, and that any such surveillance is a criminal offence. The Commission has recommended that there should continue to be an express prohibition of the use of covert surveillance for the purpose of monitoring performance[23] *and in toilets, showers and change rooms.*[24]

22. Workplace Video Surveillance Act 1998 (NSW) s 8(3).
23. Recommendation 59.
24. Recommendation 60.

Recommendation 90

A breach of a provision of the proposed Surveillance Act in the workplace should constitute either a civil breach, if the surveillance was overt, or a criminal offence, if the surveillance was covert.

COMPLAINTS AND REVIEW PROCEDURES

Overt surveillance

10.25 There are two pieces of legislation in New South Wales which have enacted effective complaints and review processes, and which, in the Commission's view, provide ideal blueprints for dealing with alleged breaches, or threatened breaches, of the proposed Surveillance Act in relation to overt surveillance. The Anti-Discrimination Act 1977 (NSW) ("Anti-Discrimination Act") and the Privacy and Personal Information Protection Act 1998 (NSW) ("Privacy and Personal Information Protection Act") have established procedures to prevent or remedy, in the case of the former, unlawful discrimination, and, in the case of the latter, interference with the privacy of individuals in public sector agencies. The Privacy and Personal Information Protection Act is of particular interest both because of its subject matter and because it provides for the appointment of a Privacy Commissioner. These frameworks are described in the following paragraphs 10.26-10.28.

Anti-Discrimination Act 1977 (NSW)

10.26 Pursuant to the Anti-Discrimination Act, a person complaining of discrimination can lodge a complaint with the President of the Anti-Discrimination Board, who is then obliged to investigate that complaint. The primary role of the President is to conciliate the matter. If conciliation fails, the complaint is referred to the Equal Opportunity Division of the ADT. The functions of the ADT are to hear, and make findings in relation to, disputed claims about alleged unlawful discrimination and, where a complaint of unlawful conduct is upheld, to order remedies.

Privacy and Personal Information Protection Act 1998 (NSW)

10.27 The Privacy and Personal Information Protection Act regulates the protection of personal information and privacy of individuals within public sector agencies. The Act also provides for the appointment of a Privacy Commissioner [25] who has a number of functions,[26] including receiving, investigating and conciliating complaints about privacy related matters,[27] and conducting inquiries and making investigations into privacy related matters.[28] The Privacy Commissioner may also refer a complaint to any person or body considered by the Privacy Commissioner to be appropriate in the circumstances for the purposes of investigation or other action.[29] In dealing with a complaint, the Privacy Commissioner must endeavour to resolve the matter by conciliation.[30]

10.28 Where a person is aggrieved by a contravention of the Privacy and Personal Information Protection Act, the first step in the complaints process is for the public sector agency concerned to carry out an internal review of the contravention.[31] The Privacy Commissioner may play a role in this process, including actually conducting the review, or at the very least must be kept informed.[32] If the complainant is not satisfied with the outcome of the internal review, he or she can then apply to the ADT for a review of the offending conduct.[33] An order or decision of the ADT at first instance can be appealed to an Appeal Panel of the ADT.[34]

Advantages of the Anti-Discrimination Act and the Privacy and

---

25. Privacy and Personal Information Protection Act 1998 (NSW) s 34.
26. Privacy and Personal Information Protection Act 1998 (NSW) s 36.
27. Privacy and Personal Information Protection Act 1998 (NSW) s 36(2)(k).
28. Privacy and Personal Information Protection Act 1998 (NSW) s 36(2)(l).
29. Privacy and Personal Information Protection Act 1998 (NSW) s 47.
30. Privacy and Personal Information Protection Act 1998 (NSW) s 49.
31. Privacy and Personal Information Protection Act 1998 (NSW) s 52, 53.
32. Privacy and Personal Information Protection Act 1998 (NSW) s 54.
33. Privacy and Personal Information Protection Act 1998 (NSW) s 55.
34. Privacy and Personal Information Protection Act 1998 (NSW) s 56. See Administrative Decisions Tribunal Act 1997 (NSW) Ch 7, Pt 1.

Personal Information Protection Act models

10.29 The equivalent framework in the proposed Surveillance Act would provide for conciliation by the Privacy Commissioner and hearings of unresolved complaints by a specialist division of the ADT. The benefits of providing access to conciliation in the first instance, and determination by a division of the ADT in the second instance, are several. The conciliation process is:

- *readily accessible by complainants;*
- *relatively inexpensive;*
- *not intimidating; and*
- *can bring flexibility and informality to bear on the resolution of complaints.*[35]

10.30 Furthermore, a Privacy Commissioner would obviously develop specialist skill and expertise in conciliating breaches of the proposed Surveillance Act. The Commission recommends that the Privacy Commissioner should also have the power to conduct inquiries and initiate investigations into surveillance related matters, including breaches, or threatened breaches, of the proposed Surveillance Act.

10.31 The Anti-Discrimination Act provides that the President of the Anti-Discrimination Board has the power to refer a complaint to the ADT at any time if satisfied that "the nature of a complaint is such that it should be referred".[36] *In its Review of the Anti-Discrimination Act 1977 (NSW) ("Report 92"), the Commission reasoned that the inference to be drawn from the structure of the Anti-Discrimination Act as a whole is that a referral can be made without attempting conciliation.*[37] *The Commission recommended*

---

35. For example, the Privacy and Personal Information Protection Act 1998 (NSW) provides that the Privacy Commissioner may determine the procedures to be followed in exercising his or her functions under the Act; is to act in an informal manner as far as possible; is not bound by rules of evidence; and is to act according to the substantial merits of the case without undue regard to technicalities: s 39.

36. Anti-Discrimination Act 1977 (NSW) s 94(1)(c).

37. New South Wales Law Reform Commission, Review of the Anti-Discrimination Act 1977 (NSW) (Report 92, 1999) at para 8.154.

that this inference be made explicit and that it should further be made clear that the President of the Anti-Discrimination Board has power to refer whether or not an investigation into the complaint has been undertaken or completed. As well, the Commission recommended that the President should not refer a complaint without the consent of the complainant unless there are exceptional circumstances.[38] *The Commission considered that although a respondent should have the opportunity of being heard on why a complaint should not be referred, the respondent should only be able to resist the referral where he or she asserts that the claim has been settled by agreement and the respondent remains ready, willing and able to abide by the terms. The Commission is of the view that it is equally appropriate for the proposed Surveillance Act to empower the Privacy Commissioner to refer a complaint to the ADT, whether or not the matter has been investigated or conciliated. The ancillary recommendations made in Report 92 with respect to the conditions governing the exercise of the power, referred to above, are correspondingly appropriate.*

10.32 It is intended that the jurisdiction of the ADT will be expanded in the near future to accommodate the review functions given to it by the Privacy and Personal Information Act. It is anticipated that amendments to the Administrative Decisions Tribunal Act 1997 (NSW) will establish either a Human Rights Division of the ADT which would encompass privacy, or a specialist Privacy Division. In either event, it would seem that the ADT is an ideal forum for a complaints and review mechanism for surveillance disputes given the link with privacy. The Commission proposes that the ADT will perform any function given to it under the proposed Surveillance Act.

10.33 The litigation of breaches of the proposed Surveillance Act in a specialist division of the ADT, rather than in a civil court, is likely to be more expeditious, less expensive and would, once it was up and running, capitalise on the specialist division's accumulated expertise in privacy matters.

10.34 The Commission recommends that the proposed Surveillance

38. NSWLRC Report 92, Recommendation 121.

Act should give standing to bring a complaint to the Privacy Commissioner and proceedings in the ADT to the following:

- *a person affected to some degree by the conduct of the surveillance;*[39] *and*
- *where the surveillance has taken place in the workplace, an industrial organisation on behalf of the employee(s) who have been affected by the conduct of surveillance.*[40]

The Privacy Commissioner should also have standing, including in a representative capacity, to bring proceedings in the ADT.[41] *In this Chapter, where references are made to "a person aggrieved, the term is used in the sense of those who will have standing under the proposed Surveillance Act.*

---

39. See Australian Law Reform Commission, Beyond the Door-Keeper: Standing to Sue for Public Remedies (Report 78, 1996) at para 3.8-3.12 for a discussion of the tests for determining who is a person affected. The most common tests are "person aggrieved", "persons whose interests are affected" and "persons interested".

40. The Anti-Discrimination Act 1977 (NSW) makes express reference to a complaint lodged "by a representative body on behalf of a named person or named persons": s 88(1A)-(1C). A "representative body" is defined in s 87 as a body "(whether incorporated or unincorporated) which represents or purports to represent: (a) a group of people within New South Wales; …". NSWLRC 92 notes that a trade union or industrial organisation may properly be accepted as the representative of its members, although, in the Commission's opinion, its powers should be limited to complaints relating to employment: para 8.32.

41. See ALRC Report 78 at para 3.12: "The courts have recognised that the conduct of litigation involving a public issue ought to be entrusted to an applicant who is capable of representing the public interest …".

10.35 In relation to the details of procedural requirements, such as the form that a complaint should take, rules governing lodgment and acceptance of a complaint, time constraints, and the practices and procedures governing the conduct of proceedings, it is envisaged that the proposed Surveillance Act would largely follow the Anti-Discrimination Act in this regard.[42]

Recommendation 91

A complaint relating to a breach of an overt surveillance provision of the proposed Surveillance Act should be made to the Privacy Commissioner.

Recommendation 92

The proposed Surveillance Act should give standing to make a complaint to the Privacy Commissioner to the following:

- **a person affected to some degree by the conduct of the surveillance; and**
- **where the surveillance has taken place in the workplace, an industrial organisation on behalf of the employee(s) who have been affected by the conduct of surveillance.**

Recommendation 93

42. *See NSWLRC Report 92, ch 8 and Recommendations 101-110, 112-114, 119, 122 and 123; see also ch 9 and Recommendations 138, 145 and 146. NSWLRC Report 92 makes a number of recommendations for amendments to the Administrative Decisions Tribunal Act 1997 (NSW) which, although made in the context of anti-discrimination law, are appropriate recommendations to make in the context of the proposed Surveillance Act: see Recommendations 130, 132, 135, 136, 137, 139, 140, 141 and 142. The reasons for making these recommendations are set out fully in NSWLRC Report 92, ch 8 and 9.*

Where the Privacy Commissioner dismisses or declines to entertain a complaint for any reason, the complainant should be able to require the Privacy Commissioner to refer the complaint to a specialist division of the Administrative Decisions Tribunal.

Recommendation 94

The Privacy Commissioner should, in the first instance, conciliate a complaint. Where a complaint remains unresolved 12 months after the date of lodgement of the complaint:

- **either party to the complaint should be able to make a request in writing to the Privacy Commissioner to refer the matter to a specialist division of the Administrative Decisions Tribunal for hearing;**
- **the Privacy Commissioner should be required to refer the complaint within 28 days of such a request, unless the Privacy Commissioner believes the complaint can be conciliated;**
- **where the complainant objects to the referral of the complaint and the Privacy Commissioner is satisfied that the complaint cannot be conciliated, the complaint should lapse.**

Recommendation 95

The Privacy Commissioner should have the power, of his or her own motion, to conduct inquiries and initiate investigations into surveillance related matters, including breaches, or threatened breaches, of the proposed Surveillance Act.

Recommendation 96

An agreement reached pursuant to conciliation should be enforceable by the Privacy Commissioner.

Recommendation 97

The Privacy Commissioner should have the power to decide not to proceed with a complaint where:

- **the dispute has been settled or resolved by agreement between the parties;**
- **the complainant, or person on whose behalf the complaint was made, does not wish to proceed with the complaint; or**
- **the complainant has allowed the complaint to remain inactive for an extended period of time or abandoned the complaint.**

Recommendation 98

The Privacy Commissioner should have the power to refer a complaint to the Administrative Decisions Tribunal at any time if he or she is satisfied that the nature of a complaint is such that it should be referred. The Privacy Commissioner should be able to exercise this power whether or not an investigation into the complaint has been undertaken or completed. The Privacy Commissioner should not refer a complaint without the consent of the complainant unless there are exceptional circumstances. The respondent should be given the opportunity to be heard on why a complaint should not be referred, but should only be able to resist referral on the grounds that the complaint has been settled by agreement and the respondent remains ready, willing and able to abide by the terms.

Recommendation 99

The proposed Surveillance Act should give standing to bring proceedings in the Administrative Decisions Tribunal to the following:

- **a person affected to some degree by the conduct of the surveillance;**
- **the Privacy Commissioner, including in a representative capacity; and**
- **where the surveillance has taken place in the workplace, an industrial organisation on behalf of the employee(s) who have been affected by the conduct of surveillance.**

Recommendation 100

The Administrative Decisions Tribunal should have the power to grant the Privacy Commissioner leave to intervene on behalf of a complainant, where considered appropriate, in proceedings before it.

Recommendation 101

The *Administrative Decisions Tribunal Act 1997* (NSW) should adopt a comprehensive set of procedural and machinery provisions, similar to the provisions contained in the *Federal Court of Australia Act 1976* (Cth), to deal with the conduct of representative complaints under the proposed Surveillance Act.

Recommendation 102

The proposed Surveillance Act should contain provisions similar to the Anti-Discrimination Act regulating procedural requirements in relation to complaints and the practices and procedures governing the conduct of proceedings.

Covert surveillance

10.36 As the Commission has formed the view that a breach of the provisions regulating covert surveillance should constitute a criminal offence, prosecution for such offence should take place within the criminal courts system. Both the Workplace Video Surveillance Act[43] *and the Privacy and Personal Information Protection Act*[44] *provide that proceedings for offences against those Acts are to be dealt with summarily before a Local Court constituted by a Magistrate sitting alone. The LDA also provides that offences against the Act generally may be prosecuted summarily, before a Local Court constituted by a Magistrate sitting alone, or before the Supreme Court in its summary jurisdiction.*[45] *However, offences against Part 2 of the LDA*[46] *may be prosecuted either summarily or on indictment.*[47] *Where an offence against Part 2 of the LDA is prosecuted summarily, if the court decides that the offence should be dealt with as an indictable offence, and no evidence has been led by the defendant, the court may order that the proceedings are to become committal proceedings.*[48]

10.37 The Commission agrees with the approach taken under the

43. *Workplace Video Surveillance Act 1998 (NSW) s 29.*
44. *Privacy and Personal Information Protection Act 1998 (NSW) s 70.*
45. *LDA s 24 and 25.*
46. *LDA Pt 2 contains prohibitions on: the use of listening devices in certain circumstances (s 5); communication or publication of private conversations unlawfully listened to (s 6 and 7); possession of unlawful records of private conversations (s 8); and manufacture, supply or possession of a listening device for unlawful use (s 9).*
47. *LDA s 25.*
48. *LDA s 26.*

LDA and recommends that it be adopted in the proposed Surveillance Act.

10.38 Since surveillance is an area where both public and private rights may be infringed, it should be possible for a private action to lie concurrently with a prosecution for a criminal offence.[49] *Hence, a person aggrieved by conduct infringing covert surveillance legislation should have access to the complaints and review processes available in relation to breaches of overt surveillance provisions, both generally and in the workplace.*

Recommendation 103

Prosecution for a breach of a covert surveillance provision of the proposed Surveillance Act, or for breach of a provision which the proposed Surveillance Act specifies will give rise to a criminal offence, should be through the criminal justice system.

Recommendation 104

Offences against the proposed Surveillance Act generally should be prosecuted summarily, before a Local Court constituted by a Magistrate sitting alone, or before the Supreme Court in its summary jurisdiction. There should be provision within the proposed Surveillance Act for prescribed offences to be able to be prosecuted either summarily or on indictment. There should also be provision in the proposed Surveillance Act for summary proceedings to become committal proceedings if the court decides that the offence should be dealt with as an indictable offence, and no evidence has been led by the defendant.

49. See ch 8 at para 8.34-8.48 in relation to disclosure of covert surveillance activity to the subject of the surveillance.

Recommendation 105

A person aggrieved by the conduct of covert surveillance, or a breach of a provision giving rise to a criminal offence, should have access to the complaints and review processes available in relation to breaches of overt surveillance provisions, both generally and in the workplace.

Workplace surveillance

10.39 The Commission is of the view that there is no reason why a person aggrieved by surveillance in the workplace should not have recourse to the complaints and review procedures available to persons aggrieved by surveillance generally, or, if he or she so chooses, should be able to pursue the matter through the IRC. The latter course may in some instances be preferred because of the availability of employment-specific remedies, such as reinstatement.

10.40 A precedent for this approach exists in relation to the Anti-Discrimination Act whereby people complaining of discrimination in relation to employment may elect to process the complaint in the Equal Opportunity Division of the ADT or in the IRC. Furthermore, a nexus between the Industrial Relations Act 1996 (NSW) ("Industrial Relations Act") and surveillance already exists as surveillance is listed as an example of an industrial matter.[50] One of the functions of the IRC is to hear and determine industrial matters.[51]

10.41 Although "industrial dispute" is defined in the Industrial Relations Act as a dispute about an "industrial matter", this does not furnish an existing, satisfactory, mechanism for the hearing of workplace surveillance complaints. There are several reasons for this. First, pursuant to section 130, the persons or bodies who may

50. *Industrial Relations Act 1996 (NSW) s 6(2): "examples of industrial matters are as follows: … (j) the surveillance of employees in the workplace; …". See Chapter 7.*
51. *Industrial Relations Act 1996 (NSW) s 146(1)(c).*

notify the IRC of an industrial dispute do not include an individual employee. An employee aggrieved by surveillance would have to persuade his or her representative union to lodge a notice of dispute on his or her behalf. Unless it was an issue affecting a number of employees, an aggrieved person would have no certainty that the union would take up the complaint. While the IRC can act on its own initiative to resolve an industrial dispute,[52] query whether an employee could approach the IRC to take action against the employer. The IRC may also on its own initiative inquire into any industrial matter[53] but an "industrial matter" is not an "industrial dispute" giving rise to the power to make "dispute orders".[54]

10.42 Secondly, the "dispute orders" which the IRC may make would not always provide sufficient remedy for breaches of the proposed Surveillance Act. Pursuant to Part 2, "Dispute Orders", the IRC has the power to order reinstatement or re-employment[55] but may not order payment of compensation, lost remuneration or any other amount.[56] If the surveillance of the employee resulted in his or her dismissal, then that employee may have grounds for arguing that the dismissal was unfair and may apply to have the matter conciliated, or arbitrated if conciliation is unsuccessful, by the IRC.[57] The orders which can be made in respect of an unfair dismissal include reinstatement, re-employment, remuneration and compensation.[58] However, these unfair dismissal provisions of the Industrial Relations Act would be relevant to breaches of surveillance legislation only incidentally and in limited circumstances.

10.43 To provide a satisfactory complaints and review process, as well as satisfactory remedies, for a person aggrieved by surveillance in the workplace, the Industrial Relations Act would need to be amended to bring the provisions of the proposed Surveillance Act directly within its ambit.

---

52. Industrial Relations Act 1996 (NSW) s 130(2).
53. Industrial Relations Act 1996 (NSW) s 162(j).
54. See Industrial Relations Act 1996 (NSW) Pt 2.
55. Industrial Relations Act 1996 (NSW) s 137(1)(b).
56. Industrial Relations Act 1996 (NSW) s 137(3).
57. Industrial Relations Act 1996 (NSW) Pt 6.
58. Industrial Relations Act 1996 (NSW) s 89.

10.44 The Commission envisages that an employee could elect to have the complaint dealt with in one of two ways:

- *the complaint would be referred to the Privacy Commissioner for conciliation, and if unresolved, heard by a specialist division of the ADT; alternatively*
- *the complaint would be conciliated by the IRC, and if unresolved, would proceed to arbitration.*

10.45 A question arises as to whether an election to have the matter determined in the ADT should preclude the matter being dealt with in the IRC. Section 90 of the Industrial Relations Act provides that the IRC is precluded from determining an application in relation to an unfair dismissal if the applicant is entitled to obtain redress under another Act or statutory instrument and the applicant has commenced proceedings under that Act or instrument, or has not given an undertaking not to do so. However, section 169(2) of the Industrial Relations Act provides that an issue that is the subject of proceedings before the Equal Opportunity Division of the ADT may not be the subject of proceedings before the IRC without the leave of the IRC, implying, obviously, that it is possible for proceedings to be on foot in both jurisdictions, although not, presumably, if the complaint is one of unfair dismissal.

10.46 In relation to the regulation of anti-discrimination, the Anti-Discrimination Act does not specifically prohibit a person who has been compensated under the Industrial Relations Act from lodging a complaint with the ADB, nor is the ADB prohibited from accepting a complaint after the matter has been heard by the IRC. These facts may arguably be taken into account by the President of the ADB in considering whether to decline a complaint,[59] and by the Equal Opportunity Division of the ADT in deciding whether to dismiss a complaint.[60] Pursuant to section 95A of the Anti-Discrimination Act, the Equal Opportunity Division of the ADT must give leave for an employee to commence proceedings in that tribunal on an issue that is currently the subject of proceedings

59. Anti-Discrimination Act 1977 (NSW) s 90(2)(a).
60. Anti-Discrimination Act 1977 (NSW) s 111(1).

before the IRC or Industrial Court.[61]

10.47 The Commission considered, in Report 92, whether it would be preferable to provide expressly in the Anti-Discrimination Act that an employee who elects to pursue redress in one jurisdiction should forgo the right to process the complaint in another jurisdiction.[62] *The Commission concluded that where the rights to take action and the redress are not identical in the available jurisdictions, complainants could be allowed to take advantage of the remedies offered by each jurisdiction, so long as the relief obtained in each is not identical (and that there is not, therefore, "double dipping") and the granting of different relief does not cause undue prejudice to the respondent. The Commission recommended that section 95A be amended to provide expressly that it be a condition of granting leave that any relief received previously is not duplicated and that granting the relief sought would not cause undue prejudice to the respondent.*[63]

10.48 By the same reasoning, an employee who is adversely affected by workplace surveillance could pursue different remedies in the IRC and the ADT, with the same provisos as recommended in relation to section 95A.

10.49 If proceedings concerning unlawful discrimination under the Anti-Discrimination Act are commenced in the IRC, the President of the ADB may intervene in these proceedings.[64] *It would similarly be feasible to provide that the Privacy Commissioner could intervene in proceedings before the IRC concerning unlawful surveillance. However, as the IRC is a determinative body and there is no office of "Industrial Relations Commissioner" corresponding to that of Privacy Commissioner, the proposed Surveillance Act could not make provision for a member of the IRC to intervene in proceedings before the ADT.*

10.50 As set out in paragraph 10.34 above, the Commission

---

61. Anti-Discrimination Act 1977 (NSW) s 95A.
62. NSWLRC 92 at para 4.83.
63. NSWLRC 92, Recommendation 11.
64. Industrial Relations Act 1996 (NSW) s 167.

recommends that the proposed Surveillance Act give standing to an industrial organisation to bring a complaint in the ADT on behalf of employees who have been affected by the conduct of surveillance in the workplace.[65]

10.51 As with general covert surveillance, an action through the IRC could lie concurrently with a prosecution for a criminal offence.

Recommendation 106

A person aggrieved by a breach of the provisions of the proposed Surveillance Act in the workplace should have access to the complaints and review processes available for surveillance generally, or, if the person so chooses, should be able to pursue the complaint in the Industrial Relations Commission.

Recommendation 107

The *Industrial Relations Act 1996* (NSW) should be amended to enable the Industrial Relations Commission to hear complaints under the proposed Surveillance Act.

Recommendation 108

The *Industrial Relations Act 1996* (NSW) should be amended to provide that an issue that is the subject of proceedings under the proposed Surveillance Act before the Administrative Decisions Tribunal may, with the Commission's leave, be the subject of proceedings before the Industrial Relations Commission. It should be a condition of granting leave that any relief received previously is not

65. Recommendation 99.

duplicated and that granting the relief sought would not cause undue prejudice to the respondent

Recommendation 109

The proposed Surveillance Act should provide that an issue that is the subject of proceedings under that Act before the Industrial Relations Commission may, with the leave of the Administrative Decisions Tribunal, be the subject of proceedings before the Tribunal. The proposed Surveillance Act should provide expressly that it be a condition of granting leave that any relief received previously is not duplicated and that granting the relief sought would not cause undue prejudice to the respondent.

Recommendation 110

The Administrative Decisions Tribunal should have the power to transfer proceedings brought under that Act to the Industrial Relations Commission on the application of the complainant or in any such circumstances as to the Tribunal seems just.

Recommendation 111

The Industrial Relations Commission should have the power to transfer proceedings brought under the proposed Surveillance Act to the Administrative Decisions Tribunal on the application of the complainant or in any such circumstances as to the Commission seems just.

SANCTIONS AND REMEDIES

Overt surveillance

10.52 Just as the Anti-Discrimination Act and the Privacy and Personal Information Protection Act provide exemplars for a complaints and review framework for surveillance legislation, the remedies available in those Acts would also translate well to the surveillance context. As those Acts already confer power on the ADT to make a range of orders for anti-discrimination and privacy breaches respectively, there would be no obstacle to conferring similar powers in respect of surveillance breaches under the proposed Surveillance Act.

Anti-Discrimination Act

10.53 ***Damages.*** *Under the Anti-Discrimination Act, where the ADT finds an individual complaint substantiated, the orders it may make include: an award of damages not exceeding $40,000; an injunction to stop the respondent repeating or continuing the unlawful act; and/or an order that the respondent "perform any reasonable act or course of conduct" to redress any loss or damage suffered by the complainant.[66] However, orders for damages and orders requiring the respondent to redress loss or damage are expressly excluded from orders which can be made in representative proceedings.[67] In the case of vilification complaints, the ADT has the power to order the respondent to: publish an apology or a retraction; and/or develop and implement a program or policy aimed at eliminating unlawful discrimination.[68]*

10.54 In Report 92, the Commission examined criticisms of the remedies available under the Act and recommended a number of reforms.[69] In relation to the ceiling of $40,000 on an award of damages, the Commission concluded that the amount was inadequate, but that it was appropriate nonetheless to cap damages

66. *Anti-Discrimination Act 1977 (NSW) s 113(1).*
67. *Anti-Discrimination Act 1977 (NSW) s 113(1)(b)(i) and 113(1)(b)(iii).*
68. *Anti-Discrimination Act 1977 (NSW) s 113(1)(b)(iiia) and 113(1)(b)(iiib).*
69. *NSWLRC Report 92 at para 10.14, Recommendations 148-155.*

in certain circumstances, depending on the constitution of the panel hearing the matter. Under the Administrative Decisions Tribunal Act, the President of the ADT, or the Head of a Division, has the power to constitute panels for the purposes of particular cases.[70] *The Commission concluded that, where a case in the ADT was presided over by a District Court judge, it was appropriate that the jurisdiction of the ADT reflect that of the District Court. In that case, the ADT's powers to make orders would be those available under the District Court Act 1973 (NSW) and the jurisdictional limit current at the time of making an order in a case would be that of the District Court. In other cases, where the ADT was constituted by a non-judicial panel, the Commission recommended that there be a statutory ceiling on the amount of damages recoverable. Acknowledging that setting a limit was a somewhat arbitrary exercise, the Commission recommended that the limit be increased from $40,000 to $150,000. The Commission is of the view that these recommendations should be applied to the proposed Surveillance Act.*

10.55 ***Nature of damages.*** *Case law has considered the nature of damages recoverable under the Anti-Discrimination Act, generally finding that they should be treated as analogous to those recoverable in an action in tort, rather than as an action in contract.*[71] *It has also been held that a court is not bound to principles of tort, and should be open to the possibility of taking a different approach to the assessment of damages where a case may require it.*[72] *Damages that the ADT has the power to award include amounts to cover disbursements, loss of wages, future loss of earnings, general damages for pain and suffering (including for embarrassment, humiliation and injury to feelings) and aggravated damages. Under the Anti-Discrimination Act, there is no power to order exemplary damages. This form of damages is "intended to punish the defendant, and, presumably, to serve one or more of the*

70. Administrative Decisions Tribunal Act 1997 (NSW) s 22.

71. Allders International v Anstee [1986] EOC 92-157 at 76,556 (Lee J), cited with approval in Maloney v Golden Ponds Corporation Pty Ltd [1995] EOC 92-674.

72. Hall v Sheiban (1989) 20 FCR 217; Australian Iron and Steel Pty Ltd v Najdovska (1988) 12 NSWLR 587.

objects of punishment – moral retribution or deterrence".[73] *In the case of the Anti-Discrimination Act, exemplary damages have been held not to be available because the power to award damages is limited to providing compensation for loss.*[74] *The Commission, in Report 92, noted that the availability of exemplary damages in civil actions generally has been criticised:*

> *primarily on the ground that it is inappropriate and unjust to dispense punishment to offenders on the balance of probabilities, which is a lower standard of proof than that required by the criminal law. Punishment, it is argued, is more appropriately left to the criminal justice system, which contains appropriate safeguards for defendants. Opponents of exemplary damages also consider them an unfair windfall to plaintiffs.*[75]

10.56 The Commission also observed that the availability of exemplary damages under statute is diminishing in New South Wales[76] *and concluded that they should not be available under the Anti-Discrimination Act.*[77] *Likewise, the Commission does not support the availability of such damages under surveillance legislation.*

10.57 ***Injunctions.*** *In relation to the power to order injunctive relief, the Commission did not doubt that this was necessary and proper but queried whether it should be available to a particular complainant who is no longer subject to the unlawful conduct. For example, a person who loses his or her employment as a result of discriminatory conduct may not seek reinstatement but may seek an injunction to prevent the continuation, or repetition, of the discrimination. The Commission concluded that there may well be circumstances where it was appropriate for the ADT to grant, on the*

---

73. Uren v John Fairfax & Sons Pty Ltd (1966) 117 CLR 118 at 149 (Windeyer J).

74. Hall v Sheiban (1989) 20 FCR 217; Squires v Qantas Airways Ltd [1985] EOC 92-135; Spencer v Dowling [1994] EOC 92-625 (Vic) at 77,332.

75. NSWLRC Report 92 at para 10.43.

76. NSWLRC Report 92 at para 10.44.

77. NSWLRC Report 92 at para 10.45.

application of an individual complainant, an injunction in respect of conduct affecting persons other than the complainant.[78] *These circumstances would include: where the complaint had been lodged in a representative capacity; where the president of the Anti-Discrimination Board had been notified of the application and been given the opportunity to be heard; and in any other case where the ADT, in the exercise of its discretion, thinks fit.*[79]

10.58 One can envisage circumstances where a person aggrieved by a breach of the proposed Surveillance Act may no longer be affected by the surveillance but would wish to seek an injunction preventing the unlawful conduct. This may occur in circumstances of general surveillance, not just in relation to workplace surveillance. The Commission is of the view that the ADT should have discretionary power to grant injunctive relief where it holds that this is warranted. It would also be appropriate for the ADT to hear submissions from the Privacy Commissioner on an application for injunctive relief.

10.59 ***Mandatory orders.*** *As noted above, under the Anti-Discrimination Act, the ADT has the power to order that the respondent perform any reasonable act aimed at redressing loss or damage suffered by the complainant. The ADT can also now order the implementation of an equal opportunity plan, but only in relation to vilification complaints.*[80] *Applying this to surveillance, conferring on the ADT the power to order the implementation of a Code of Practice to ensure compliance with the proposed Surveillance Act would be particularly useful.*

10.60 The Commission, in Report 92, addressed two problems which arise in relation to mandatory orders, namely, that the cost of compliance may exceed the tribunal's jurisdictional limit, and that the order may require on-going monitoring.[81] *However, the Commission was of the view that the potential for these problems to arise did not justify the exclusion of the power to make such orders.*

---

78. NSWLRC Report 92 at para 10.47-10.49.
79. NSWLRC Report 92, Recommendation 149.
80. Anti-Discrimination Act 1977 (NSW) s 113(1)(b)(iiib).
81. NSWLRC Report 92 at para 10.53-10.56.

The Commission is presently of the view that, in relation to the proposed Surveillance Act, the availability of mandatory orders would have particular relevance and would offer, in many circumstances, an appropriate remedy to a complainant. For example, the ADT could order the removal of surveillance devices, alteration of surveillance practices, or destruction of surveillance material, or could order that a Code of Practice be amended to comply with the legislation, or order compliance with an authorisation. It would be proper for a respondent to have the right of appeal from a mandatory order where the cost of compliance with that order exceeded the ADT's statutory limit. The ADT could appoint the Privacy Commissioner to monitor compliance with the order. The proposed Surveillance Act should also give the Privacy Commissioner the right to apply for a mandatory order, independently of the instigation of proceedings by a complainant.

10.61 ***Declarations.*** *Under the Anti-Discrimination Act, although the ADT must find a complaint substantiated before granting relief,*[82] *it does not presently have the express power to declare that certain conduct is unlawful. In Report 92, the Commission recommended that it would be desirable for the ADT to be given an express power to make a declaration, whether or not it proceeds to other relief.*[83] *It would also be useful for the ADT to have declaratory powers under the proposed Surveillance Act. There may be occasions where a declaration would have the effect of bringing about a change in unlawful practice, or a change in a deficient Code of Practice, without it being necessary to commence proceedings against the surveillance user. A declaration would operate as an effective bargaining tool in negotiations for change. A declaration may also achieve a purpose comparable to an interim order, in cases where an interim injunction is not appropriate, while other steps are being taken to resolve a complaint or a prosecution. As with other orders, the Privacy Commissioner should have standing to apply for a declaration.*

Privacy and Personal Information Protection Act

10.62 When an internal review is conducted under section 53 of the

82. Anti-Discrimination Act 1977 (NSW) s 113(1)(b).
83. NSWLRC Report 92, Recommendation 151.

Privacy and Personal Information Protection Act, the public sector agency whose conduct was under review can: make a formal apology to the applicant; take such remedial action as it thinks appropriate, such as the payment of compensation; and provide undertakings, and implement administrative measures to ensure, that the conduct will not occur again. The agency must give reasons for the action which it proposes taking, and the applicant has a right to have the proposed action reviewed by the ADT.[84]

10.63 Where conduct alleged to be in breach of the Privacy and Personal Information Protection Act is reviewed by the ADT, the orders which the ADT can make include: an award of damages not greater than $40,000; an order restraining any conduct or action in contravention of, or an order requiring performance of, an information privacy principle or a privacy code of practice; an order requiring personal information that has been disclosed to be corrected by the agency; an order requiring the agency to take steps to remedy any loss or damage; an order requiring the agency not to disclose personal information; and such ancillary orders as the ADT thinks appropriate.[85] *An order for compensation is not limited to financial loss but can include damages for psychological or physical harm resulting from the agency's conduct.*[86] *These remedies available under the Privacy and Personal Information Protection Act give some guidance for appropriate remedies to include under the proposed Surveillance Act.*

84. Privacy and Personal Information Protection Act 1998 (NSW) s 53(8).
85. Privacy and Personal Information Protection Act 1998 (NSW) s 55(2).
86. Privacy and Personal Information Protection Act 1998 (NSW) s 55(4)(b).

Recommendation 112

The proposed Surveillance Act should provide that in proceedings brought under that Act, the Administrative Decisions Tribunal should have the power to grant the following relief:

- **an award of damages to the limit of $150,000, except in cases where the panel has a District Court judge as its presidential member where the limit should reflect the jurisdiction of the District Court;**
- **an injunction;**
- **a mandatory order;**
- **a declaration that certain conduct is unlawful under the Surveillance Act;**
- **an order that a respondent publish an apology or retraction in relation to unlawful conduct under the proposed Surveillance Act;**
- **an order that a respondent implement a program or policy aimed at eliminating all forms of unlawful conduct under the proposed Surveillance Act;**
- **an order that the respondent not disclose information obtained as a result of the surveillance; and**
- **such other orders as seems to the Administrative Decisions Tribunal to be just and appropriate in the circumstances.**

Otherwise, the powers of the Administrative Decisions Tribunal with respect to orders should be those available under the *District Court Act 1973* (NSW).

Recommendation 113

The Administrative Decisions Tribunal should have the power to make interim orders to preserve the rights of the parties, on the application of either the Privacy Commissioner or a party to the proceedings.

Recommendation 114

The Administrative Decisions Tribunal's power to award damages should not be limited to financial loss, but should include the power to award damages for psychological or physical harm resulting from the unlawful surveillance.

Recommendation 115

The Administrative Decisions Tribunal should have the power to grant an injunction which extends to the conduct of surveillance affecting persons other than the individual complainant in the following circumstances:

- **where the complaint has been lodged in a representative capacity;**
- **where the Privacy Commissioner has been notified and given the opportunity to make submissions; or**
- **in any other case, where the Tribunal believes that the particular circumstances warrant such action.**

Recommendation 116

Where the Administrative Decisions Tribunal makes a mandatory order which is not by consent and the cost of compliance would exceed the statutory maximum, the respondent should have a right of appeal in relation to the appropriateness of the order.

Recommendation 117

The proposed Surveillance Act should give the Privacy Commissioner the power to monitor compliance with mandatory and injunctive orders made by the Administrative Decisions Tribunal.

Recommendation 118

The proposed Surveillance Act should give the Privacy Commissioner standing to apply for injunctive, mandatory and declaratory orders, whether or not proceedings have been instigated by a complainant.

Recommendation 119

Where proceedings have been brought by an industrial organisation or by the Privacy Commissioner in a representative capacity, the Administrative Decisions Tribunal should have the power to make similar orders for relief as is available in representative proceedings under the *Federal Court of Australia Act 1976* (Cth).

Recommendation 120

The proposed Surveillance Act should give the Privacy Commissioner the power:

- **in the case of an individual complaint, to take steps to enforce an order on behalf of a complainant with their consent; and**
- **in the case of a representative complaint (or in any other case where the Privacy Commissioner believes that the public interest demands), to take steps to enforce an order on his or her own motion.**

Covert surveillance

10.64 For the reasons noted above, the Commission is of the view that breaches of the provisions regulating covert surveillance should carry criminal sanctions. The Commission envisages that the penalty which would be appropriate in the majority of cases would be a fine. In some cases, courts would decide that the proper sentence was the imposition of a fine on terms, including a suspension of the fine. In more serious circumstances, a custodial sentence may be appropriate.

10.65 The proposed Surveillance Act should also confer the right to apply to the ADT for an injunction to restrain conduct which will result in an offence under the Act, or for mandatory orders to compel the carrying out of particular conduct, in the absence of which an offence under the Act will be committed. The Commission is of the view that this right should be given to the Privacy Commissioner, as well as persons who may be affected by unlawful conduct.

10.66 As noted above, the LDA, covering covert aural surveillance, creates criminal offences for breaches of that Act.[87] The penalties imposed by that Act for contraventions of Part 2 where the offence is summarily tried are fines not exceeding 40 penalty units and/or a custodial sentence not exceeding a term of 2 years for individuals or corporations.[88] Where the offence was committed by a corporation and the proceedings are taken before the Supreme Court in its summary jurisdiction the penalties increase to a fine not exceeding 500 penalty units.[89] The penalty for a conviction on indictment of an offence against Part 2 of the LDA is a fine not exceeding 100 penalty units and/or a custodial sentence not exceeding a term of 5 years. The Commission is of the view that the LDA provides a sentencing framework appropriate to surveillance offences.

87. *See LDA Pt 2.*
88. *LDA s 11(a).*
89. *LDA s 11(b).*

Recommendation 121

The proposed Surveillance Act should provide for criminal penalties in line with the framework contained in the LDA.

10.67 Where a person has suffered harm or loss as a result of unlawful covert surveillance, the remedies available to redress the wrong should be all those available to a person aggrieved by breaches of the overt surveillance provisions. To provide otherwise would be inconsistent and may lead to unfairness. The person adversely affected by covert surveillance would, as with overt surveillance, lodge a complaint with the Privacy Commissioner for the matter to be conciliated. If no resolution of the grievance resulted, the ADT would proceed to hear the matter and could order any of the remedies within its power to order in relation to overt surveillance.

Workplace surveillance

10.68 The consequences of unlawful surveillance in the workplace will be determined by whether the surveillance was overt or covert, in the same way as it would be for surveillance carried out generally. It is not intended that there will be a separate regime unique to the context of employment.

10.69 Paragraphs 10.44-10.48 above describe the opportunity which employees, aggrieved by workplace surveillance, will have to elect whether to lodge a complaint in the IRC or, alternatively, with the Privacy Commissioner and the ADT. The redress that can be obtained depends on the path chosen, a factor which obviously will have influenced the election.

10.70 The IRC already has the power, in respect of unfair dismissals, to order reinstatement, re-employment, lost remuneration if the employee is reinstated or re-employed, or

compensation if the employee is not so re-instated or re-employed.[90] *The only limit placed on an award of compensation is that it not exceed the amount of remuneration of the applicant during the period of six months immediately before being dismissed.*[91] *If there is a threat of dismissal, the IRC can order the employer not to dismiss the employee in accordance with that threat.*[92] *In relation to industrial disputes, the IRC has the power to order reinstatement or re-employment, or that a threat to dismiss not be carried out, but, as pointed out in paragraph 10.42 above, cannot order the payment of compensation, lost remuneration or any other amount.*[93] *The full range of remedies available in the case of an unfair dismissal should be available to an employee adversely affected by surveillance.*

10.71 If the employee seeks redress through the ADT, the remedies available would be those set out in paragraphs 10.53-10.63 above. Although the Equal Opportunity Division of the ADT, when hearing claims under the Anti-Discrimination Act, has the power to order reinstatement in employment related matters, it has declined to make such orders.[94] *The Commission is of the view that the proper forum in which to seek an order for reinstatement is in the Industrial Relations Commission as that tribunal has the expertise to decide whether it is appropriate to grant such specifically employment-related relief.*

90. Industrial Relations Act 1996 (NSW) s 89.
91. Industrial Relations Act 1996 (NSW) s 89(5).
92. Industrial Relations Act 1996 (NSW) s 89(7).
93. Industrial Relations Act 1996 (NSW) s 137.
94. NSWLRC Report 92 at para 4.81.

Appendices

- Appendix A
  Justice Adams' dissent on participant monitoring and the use of listening devices
- Appendix B
  Submissions

APPENDIX A:

Justice Adams' dissent on participant monitoring and the use of listening devices

A1 The majority recommendation (see paragraphs 2.99-2.107) is based upon the view that covert recording by one person of a conversation to which that person is party is a breach of privacy and confidentiality. Whilst in some senses this is correct, I am of the view that it is not true in any important sense justifying legislative intervention, still less creating a criminal offence where at present there is none. I agree, however, that covert recording of images without a warrant should be prohibited.

A2 At present a participant has a legal right to record conversations to which he or she is party. It is obvious that there are many completely legitimate reasons that such a person might have for so doing. To require that person to first obtain permission from the State on pain of criminal prosecution is a substantial interference with his or her legal rights. It is true that some persons might wish to make such a recording for illegal purposes, but they will not be deterred by sanctions of the type envisaged in the recommended legislation. On the other hand, there is no general right to privacy or confidentiality in our law, either civil or criminal. Nor is it appropriate for the Commission to make any recommendations about this question. The Commission is considering the question of surveillance. Where one person is in the presence of another, he or she is necessarily aware of the fact. It is obvious that the parties to the conversation consent, or even desire, that the others should be aware of what is said. I am unable to see how the mere covert recording of what is said within the hearing of the recording party can reasonably be seen as surveillance, let alone as activity that should be regarded as criminal.

A3 Nor do I see what real issues of privacy or confidentiality are raised by a participant recording a conversation which takes place in his or her presence.

A4 To take the question of confidentiality first, it is not proposed by the majority – nor could it be – that a mere breach of confidence, however outrageous or destructive of reputation or other private interest, should be a criminal offence. Many conversations that might be covertly recorded. moreover, would not be regarded as confidential in the sense that a party would reasonably suffer a sense of grievance by one of the participants conveying the content of the conversation to another or others. I do not see how an assumption about confidentiality is a safe or even reasonable basis for creating a criminal offence, not for breaching the confidence but for doing so in a particular way, namely, by making a record which is capable of being replayed to another person. The criminal law should not depend upon such unreal distinctions and is brought into disrepute by punishment which depends on them.

A5 Even where there is an agreement (which, of course, might be implicit or explicit) that no recording is being made of a conversation, the mere fact that one party – even deceitfully – is in breach of that agreement has nothing to do with confidentiality, since disclosure of the matter recorded is not involved. Yet this is the activity that the majority consider should be criminal unless permitted by a warrant obtained from a relevant designated person. Upon the assumption that the matter is disclosed, what is proposed to be prohibited is not the disclosure as such, but the disclosure by a particular mode, namely by reliance on a particular mode of recording. Thus, if what is disclosed (say, from memory or notes made shortly afterwards) is the same as that which might have been disclosed by the recording, this is nevertheless permitted.

A6 So far as privacy is concerned, it is self evident that the communication is not kept private from the individuals who are present. Thus the occasion is not, in its very nature, a private one so far as they are concerned. Even if there is an explicit agreement that each of the participants is to keep the communication secret from others not present and this undertaking is broken, no crime will be committed and the majority do not suggest that the protection of privacy is so great a value as to justify creation of such an offence. Again, merely recording the conversation cannot, of itself breach the privacy of the occasion. That can only happen when the recording is conveyed to another.

A7 I cannot see that there is a difference in substance between, on the one hand, relaying a conversation by means that do not involve a recording and relaying it by means that do. The only practical difference is that the latter is both irrefutable and more accurate. Thus, dealing with this issue realistically, the other Commissioners on this Reference consider that it is necessary to make criminal both the secretive making and subsequent disclosure of an accurate record of an event by one of the parties to it, whilst conveying it by means that might be inaccurate and might plausibly be denied (as by relaying a recollection, perhaps supported by notes) should not be subject to such a sanction. The breach of confidence, as such, is not prohibited.

A8 In reality, therefore, what is sought to be made criminal here is potential disclosure without the permission of the State of an accurate and undeniable record, leaving untouched the right to make an inaccurate and deniable disclosure. And what is sought to be protected is the right of the other parties to a conversation to falsely deny or lie about the conversation should its occurrence or content ever become an issue. It is important to emphasise that that the matter recorded has already been disclosed to the person making the recording. Thus, surveillance is not really the issue. I do not agree that the criminal law should be used to qualify the right to make a record or to protect the right to lie.

A9 Accordingly, I agree with the majority view of the Australian Law Reform Commission as expressed in its report on Privacy which is cited in the Report.[1]

A10 It may be that recording the particular event is dishonest and relaying it to others completely vile but not every dishonesty or every vile act is or should be subject to a criminal sanction. Righteous indignation is not a basis for criminal law reform. There must be a clearly discernible public interest involved. With respect to the Commissioners forming the majority on this issue, they have not enunciated such a public interest: Reasonable expectations do not, of themselves, create such a public interest. The rights of a person to make such recordings at present is a substantive legal right. There

1. *See para 2.101.*

is no convincing reason given as to why this right is less important than the interest of the other individuals in controlling the mode of recording a particular event in which he or she is a participant.

A11 It should be clearly understood that we are not here considering the use by a participant of a transmitting or recording device pursuant to an agreement to relay information to others not present. So far as they are concerned, it is clear that surveillance is being undertaken and can only be lawful if it is permitted by an appropriate warrant. Moreover, in the absence of a warrant, not only do the "outsiders" commit an offence but the participant is clearly their accomplice and hence liable to prosecution even if, had been no transmission but, say, only a recording made by him or her. Again, if there is a recording that is made pursuant to a prior agreement by the participant with "outsiders" for the purpose of giving those "outsiders" information, then I think there is a relevant monitoring and its lawfulness will depend upon a warrant. This simply follows from the law of accessorial criminal liability.

APPENDIX B:

Submissions

Australian Broadcasting Corporation (31 July 1997)

Australian Centre for Security Research, University of Western Sydney Macarthur (31 July 1997)

Australian Federation of Business and Professional Women Inc (8 August 1997)

Australian Institute of Private Detectives (29 July 1997)

Australian Press Council (31 July 1997)

Australian Security Industry Association Limited (26 July 1997)

Baird, Mr P (2 June 1997)

Barrington Group (8 August 1997)

Chamber of Manufactures of New South Wales (Industrial) (renamed Australian Business Limited) (6 August 1997)

Confidential (11 February 1998)

Director of Public Prosecutions, Mr N R Cowdery QC (28 July 1997)

Fairfield City Council (1 August 1997)

Fisher, Ms E M (3 June 1997)

Institute of Mercantile Agents Limited (18 November 1996)

Insurance Council of Australia Limited (17 July 1997)

Joint Law Enforcement Agencies (NSW Crime Commission, Independent Commission Against Corruption, Police Integrity Commission, National Crime Authority) (13 August 1997)

Law Society of New South Wales (13 October 1997)

Law Society of New South Wales (17 December 1998)

Lismore City Council (8 August 1997)

Motor Traders' Association of New South Wales (1 September 1997)

New South Wales Council for Civil Liberties (30 July 1997)

New South Wales Department of Corrective Services (21 August 1997)

New South Wales Department of Training and Education Co-ordination (20 June 1997)

New South Wales Nurses' Association (23 June 1997)

New South Wales Ombudsman (4 August 1997)

New South Wales Police Service, Special Services Group (29 July 1997)

New South Wales Young Lawyers Criminal Law Committee (11 August 1997)

Price Waterhouse (30 July 1997)

Privacy Committee of New South Wales (22 August 1997)

Publishing and Broadcasting Limited (30 July 1997)

Registered Clubs Association of New South Wales (29 July 1997)

Retail Traders Association of New South Wales (30 July 1997)

Service Station Association Limited (20 July 1996)

Shepherd, Mr D (6 June 1997)

Sides, M L, Senior Public Defender (now District Court Judge) (18 July 1997)

Simpson, Dr Brian (30 July 1997)

Sydney Futures Exchange Limited (15 August 1997)

Sydney Harbour Casino (25 June 1997)

Teiffel, E S & H P (17 July 1997)

TABLE OF LEGISLATION

Commonwealth

New South Wales

Listening Devices Act 1984 (continued)

Queensland

South Australia

Tasmania

Victoria

Western Australia

Australian Capital Territory

Northern Territory

Canada

Germany

New Zealand

Sweden

United Kingdom

United Nations

United States of America

TABLE OF CASES

SELECT BIBLIOGRAPHY

AUSTRALIA, ATTORNEY GENERAL'S DEPARTMENT, Review of Telecommunications (Interception) Act 1979 (Canberra, 1991)

AUSTRALIA, AUSTRALIAN NATIONAL AUDIT OFFICE, Management of Tax File Numbers: Australian Taxation Office (Audit Report 37, AGPS, Canberra, 1998-99)

AUSTRALIA, AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE, Annual Report 1998-99 (AGPS, Canberra, 1999)

AUSTRALIA, COMMONWEALTH INTERDEPARTMENTAL COMMITTEE ON QUASI-REGULATION, Grey-Letter Law (AGPS, Canberra, 1997)

AUSTRALIA, DEPARTMENT OF FINANCE, Review of the Long Term Cost Effectiveness of Telecommunications Interception (AGPS, Canberra, 1994)

AUSTRALIAN LAW REFORM COMMISSION, Beyond the Door-Keeper – Standing to sue for public remedies (Report 78, AGPS, Canberra, 1996)

AUSTRALIAN LAW REFORM COMMISSION, Evidence: Vol 1 (Interim Report 26, AGPS, Canberra, 1985)

AUSTRALIAN LAW REFORM COMMISSION, Evidence (Report 38, AGPS, Canberra, 1985)

AUSTRALIAN LAW REFORM COMMISSION, Open Government (Report 77, AGPS, Canberra, 1995)

AUSTRALIAN LAW REFORM COMMISSION, Privacy (Report 22, AGPS, Canberra, 1983)

AUSTRALIA, Parliamentary Debates (Hansard) House of Representatives, 14 May 1997

AUSTRALIA, Parliamentary Debates (Hansard) Legislative Assembly, 18 June 1997

AUSTRALIA, PRIVACY COMMISSIONER, Covert Optical Surveillance in Commonwealth Administration – Guidelines (Canberra, February 1992)

AUSTRALIA, SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE, Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000 (AGPS, Canberra, October 2000)

AUSTRALIA, TASKFORCE ON INDUSTRY SELF-REGULATION, Draft Report (Department of Treasury, AGPS, Canberra, 2000)

AUSTRALIAN BROADCASTING AUTHORITY, Commercial Radio Inquiry: Report of the Australian Broadcasting Authority Hearing into Radio 2UE Sydney Pty Limited (Sydney, 2000)

Australian Torts Reporter (CCH Common Law Editors, Sydney, 1984)

BALKIN R P and DAVIS J R, Law of Torts (2nd edition, Butterworths, Canberra, 1996)

BALZ S D and HANCE O, "Privacy and the Internet: Intrusion, Surveillance and Personal Data" (1996) 10(2) International Review of Law, Computers and Technology 219

BANISAR D and DAVIES S, "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments" (1999) 18(1) John Marshall Journal of Computer and Information Law 1

BARAGWANATH M, Unfair Dismissal in New South Wales (LBC Information Services, Sydney, 1999)

BARRETT P J, Telecommunications Interception Review: Review of the longer term cost-effectiveness of telecommunications interception arrangements under section 332R of the Telecommunications Act 1997 (Australian Telecommunications Authority, Canberra, 1999)

BLACKWELL, BRYSON C, and DAY M, "Workplace Surveillance Poses Legal, Ethical Issues" The National Law Journal (11 January 1999)

BRAUE D, "Every Breath You Take" The Bulletin (25 January 2000)

BRAUE D, "Invasion of the data-snatchers" The Bulletin (9 May 2000)

BRONITT S, "Electronic Surveillance, Human Rights and Criminal Justice" (1997) 3(2) Australian Journal of Human Rights 183

BROOME J, "Electronic Surveillance in Criminal Investigations: Balancing Law Enforcement with Civil Liberties" in Electronic Surveillance in Criminal Investigations: Balancing Law Enforcement with Civil Liberties (Institute of Criminology, Sydney, 1998)

BROWN B, CCTV in Town Centres: Three Case Studies (Home Office Police Department, Police Research Group Crime Detection and Prevention Series No 68, London, 1995)

BRUCE V, "Fleeting Images of Shade: Identifying People Caught on Video" (1998) 11(7) The Psychologist 331

BUDNITZ M E, "Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Reg is Inadequate" (1998) 49 South Carolina Law Review 847

BUFORD B, "Thy Neighbour's Life" New Yorker (5 January 1998)

BURROWS Q, "Scowl Because You're on Candid Camera: Privacy and Video Surveillance" (1997) 31 Valparaiso University Law Review 1079

CAMPBELL A J, "Self-Regulation and the Media" (1999) 51(3) Federal Communications Law Journal 711

CANADA, DEPARTMENT OF COMMUNICATIONS AND DEPARTMENT OF JUSTICE, Privacy and Computers: a report of a Task Force established jointly by the Department of Communications and the Department of Justice (Ottowa, 1972)

CANADA, DEPARTMENT OF JUSTICE, Annual Report on the use of Electronic Surveillance as Required Under Subsection 195(1) of the Criminal Code 1985 (1996-1997)

CANADA, LAW REFORM COMMISSION, Electronic Surveillance (Working Paper 47, Ottawa, 1986)

CANADA, PRIVACY COMMISSIONER, Annual Report 1998-1999 (Ottawa, Canadian Human Rights Commission, 1999)

CARTER P B, "Evidence Obtained by the Use of a Covert Listening Device" (1997) 113 Law Quarterly Review 468

CITY OF SYDNEY, Report to Ratepayers 1997-98

CLARKE R V (ed), Situational Crime Prevention: Successful Case Studies (2nd edition, Harrow and Heston, New York, 1997)

COLVIN M, Under Surveillance: covert policing and human rights standards (Justice, London, 1998)

COOPER J and GOODVACH A, "Employment law" (May 1999) 51(4) Australian Company Secretary 184

DAVEY K, "Privacy Protection for Internet E-mail in Australia: Part 1" (1997) 33 Computers and the Law 7

DAVEY K, "Privacy Protection For Internet E-mail in Australia: Part 2" (1997) 34 Computers and the Law 8

DAVIES S G, "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity" in P E Agre and M Rotenberg (eds), Technology and Privacy: The New Landscape (MIT Press, Massachusetts, 1997)

DAVIES S, "Privacy and Surveillance: The Surveillance Devices Act 1998" 27(1) Brief (February 2000)

"Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (Directive 95/46/EC of 24 October 1995) (Official Journal L 281, 23/11/1995 p 0031 – 0050)

DITTON J, SHORT E, PHILLIPS S, NORRIS C and ARMSTRONG G, The Effect of Closed Circuit Television on Recorded Crime Rates and Public Concern About Crime in Glasgow (Scottish Office Central Research Unit, Edinburgh, 1999)

DIXON T, "Workplace Video Surveillance – Controls Sought" (1995) 2(8) Privacy Law and Policy Reporter 141

EDWARDS C, SAVAGE N and WALDEN I (eds), Information Technology and the Law (2nd edition, Macmillan, London, 1990)

ELECTRONIC PRIVACY INFORMATION CENTRE, Vol 6.15 EPIC Alert (23 September 1999)

ELLIOT I, "Listening Devices and the Participant Monitor: Controlling the Use of Electronic Surveillance in Law Enforcement" (1982) Criminal Law Journal 327

ENGLAND AND WALES, HOME OFFICE, Report of the Committee on Privacy and Related Matters (HMSO, Cm 1102, London, 1990)

FEDERATION OF AUSTRALIAN COMMERCIAL TELEVISION STATIONS, Commercial Television Industry Code of Practice (April 1999)

FLAHERTY D H, "Controlling Surveillance: Can Privacy Protection Be Made Effective?" in P E AGRE and M ROTENBERG (eds), Technology and Privacy: The New Landscape (MIT Press, Massachusetts, 1997)

FLANAGAN J, "Restricting Electronic Monitoring in the Private Workplace" 43 Duke Law Journal 1256

FORD M, Surveillance and Privacy at Work (Institute of

Employment Rights, London, 1998)

FORD P, "Who's Listening? Recording and Monitoring of Personal and Business Communications" (1998) 48(2) Telecommunications Journal of Australia 75

FORD P, Telecommunication Interceptions Policy Review (Australia, Attorney General's Department, Information and Security Law Division, 1999)

FYFE N R and BANNISTER J, "City Watching: Closed Circuit Television Surveillance in Public Spaces" (1996) 28 Area 37

GALLAGHER H, "1984 1997" (September 1997) 32(8) Australian Lawyer at 4

GRABOSKY P N and SMITH R G, Crime in the Digital Age (The Federation Press, Sydney, 1998)

GRABOSKY P N, "Crime Control and Policing in the 21st Century" paper presented at the 14th Annual Conference of the Australian and New Zealand Society of Criminology (Perth, 27-30 September 1999)

GREENBAUM M L, "Employee Privacy, Monitoring and New Technology" Chapter 6 in Proceedings of the Forty-First Annual Meeting of the National Academy of Arbitration, Washington, DC 1988 (Bureau of National Affairs, Washington DC, 1989)

GRENNAN H, "Cops and robots" The Bulletin (17 June 1997)

Halsbury's Laws of Australia (Butterworths, Sydney, 1996)

HANDLEY R P , "Trespass to Land as a Remedy for Unlawful Intrusion on Privacy" (1988) 62 Australian Law Journal 216

HANSEN M, "No Place to Hide" (August 1997) 83 ABA Journal 44

HENDERSON A and MCDONOUGH A, "Call monitoring – legalities and regulation" (1999) 2(8) Telemedia 97

HINTON R, Information Technology and How to Use It: a

Handbook of Effective Practice (ICSA Publishing, Cambridge, 1988)

HUDSON M, "Virtual Privacy: The Impact of Electronic Technology on Communications" (1998) 3(1) Media and Arts Law Review 18

INTERNATIONAL LABOUR OFFICE, "Workers' Privacy Part II: Monitoring and Surveillance in the Workplace" (1993) 12(1) Conditions of Work Digest

INTERNATIONAL LABOUR OFFICE, Code of Practice, Protection of Workers' Personal Data (Geneva, 1997)

IRELAND, LAW REFORM COMMISSION, Privacy: Surveillance and the Interception of Communications (Report 57, 1998)

JENERO K and MAPES-RIORDAN L, "Electronic Monitoring of Employees and the Elusive 'Right to Privacy'" (1992) 18(1) Employee Relations Law Journal 71

KANG J, "Information Privacy in Cyberspace Transactions" (1998) 50 Stanford Law Review 1193

KEARLY L, "Computer-Based Surveillance" (1997) 2(8) Privacy Files 5

KEARNS T B, "Technology and the Right to Privacy: the Convergence of Surveillance and Information Privacy Concerns" (1999) 7 William and Mary Bill of Rights Journal 975

KING D, "Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging Privacy Gap" (1994) 67 Southern California Law Review 441

KINLEY D & BRONITT S, "Undercover Policing: Detection or Deception?" in H Selby (ed), Tommorrow's Law (Federation Press and Law Foundation of NSW, Sydney, 1995)

KOOMEN K, "Under Surveillance: Fergie, Photographers and Infringements on Freedom" (1993) 17(2) University of Queensland Law Journal 234

KUCERA B, "Outsourcing the Nation's Policing – Business Opportunities for the Private Sector" 35(5) The Agent (Institute of Mercantile Agents Ltd, May 2000)

LAW OF EVIDENCE PROJECT (CANADA), Compellability of the Accused and the Admissibility of his Statements (The Law Reform Commission, Ottawa, 1973)

LUSTGARTEN L and LEIGH I, In from the Cold: National Security and Parliamentary Democracy (Clarendon Press, Oxford, 1994)

MCCALLUM R, Employer Controls over Private Life (UNSW Press, Sydney, 2000).

MCDOWELL M, "The Principle of Open Justice in a Civil Context" (1995) 2 New Zealand Law Review 214

MCHARG A, "Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights" (1999) 62 Modern Law Review 671

METZ H, "They've got their eyes on you. They can see you. They can hear you. New high-tech tools let employers watch you while you work – and you won't even know" 22(6) Student Lawyer 22

MOLOMBY T, "Could Monica Lewinsky and Linda Tripp do it here?" (March 1998) 37(5) Law Society Journal 51

MULLALLY J, Communications Law Centre, "Privacy: Are the Media a Special Case?" paper presented at The New Privacy Laws: a symposium on preparing privacy laws for the 21st Century (Sydney, 19 February 1997)

NATIONAL CRIME AUTHORITY, Listening Devices: Aspects of Legislation in Australian States and Territories (Law Reform Discussion Paper 1, 1994)

NETTHEIM G, "Open Justice Versus Justice" (1985) 9 Adelaide Law Review 488

NEW SOUTH WALES, ATTORNEY GENERAL, Report Pursuant to Section 23 of the Listening Devices Act 1984 for the year ended 31st December 1998 (AGPS, Sydney, 1999)

NEW SOUTH WALES, LAW REFORM COMMISSION, Evidence (Report 56, 1988)

NEW SOUTH WALES, LAW REFORM COMMISSION, Review of the Anti-Discrimination Act 1977 (NSW) (Report 92, 1999)

NEW SOUTH WALES, LAW REFORM COMMISSION, Surveillance (Issue Paper 12, 1997)

NEW SOUTH WALES, LAW REFORM COMMISSION, The Right to Silence (Report 95, 2000)

NEW SOUTH WALES, OFFICE OF THE DIRECTOR OF PUBLIC PROSECUTIONS, Prosecution Guidelines: Issued December 1995 (Sydney, 1995)

NEW SOUTH WALES, Parliamentary Debates (Hansard) Legislative Assembly, 17 May 1984

NEW SOUTH WALES, Parliamentary Debates (Hansard) Legislative Council, 29 April 1998, the Hon J W Shaw, Attorney General, Second Reading Speech

NEW SOUTH WALES, PRIVACY COMMITTEE, "Invisible Eyes: Report on Video Surveillance in the Workplace" (Report 67, 1995)

NEW SOUTH WALES, PRIVACY COMMITTEE, Annual Report 1982-1983 (Sydney, 1983)

NEW SOUTH WALES, PRIVACY COMMITTEE, Privacy Protection: Guidelines or Legislation? (Sydney, 1980)

NEW SOUTH WALES, ROYAL COMMISSION INTO THE NEW SOUTH WALES POLICE SERVICE, Final Report Vol 2: Reform (Sydney, 1997)

NEW ZEALAND, LAW COMMISSION, Juries in Criminal Trials (Preliminary Paper 37, Vol 2, 1999)

NIETO M, Public Video Surveillance: is it an Effective Crime Prevention Tool? (California Research Bureau, California State Library, Sacramento, 1997)

NORRIS C and ARMSTRONG G, The Maximum Surveillance Society: the Rise of CCTV (Berg, Oxford, 1999)

O'CONNOR K, "Why a National Law to Protect the Privacy of Australians?" (1998) 48(2) Telecommunication Journal of Australia 21

ONIONS C T (ed), Oxford Dictionary of English Etymology (Oxford, 1978)

PERRY R A and DILLON K W, Annual Report of the Public Interest Monitor delivered pursuant to the Police Powers and Responsibilities Act and the Crime Commission Act (Queensland, 1998)

PERRY R A and SPRINGER B, Second Annual Report of the Public Interest Monitor delivered pursuant to the Police Powers and Responsibilities Act and the Crime Commission Act (Queensland, 1999)

PEYSER M and RHODES S, "When E-mail is Oops-Mail" The Bulletin (17 October 1995)

PHILLIPS B, "Privacy in a 'Surveillance Society'" (1997) 46 University of New Brunswick Law Journal 127

RETAIL TRADERS' ASSOCIATION OF NEW SOUTH WALES, Shopwatch: an Advisory Code of Practice for the Use of Video Surveillance Equipment in Retail Stores

Review of Press Self-Regulation (Dept of National Heritage, Cm 2135, London, HMSO)

RICHARDSON M A, LUCKRAFT I C, PICTON R S, RODGERS A L and POWELL R F, Surveillance and Target Acquisition Systems (Brassey's, London, 1997)

ROONEY M J, "Liability of a Premises Owner for the Provision of Security: the Massachusetts Experience" (1995) 29(51) Suffolk University Law Review 51

ROSEN J, "The Eroded Self" New York Times Magazine (30 April 2000)

ROSEN J, The Unwanted Gaze: The Destruction of Privacy in America (Random House, New York, 2000)

SCHARRER J R, "Covert Electronic Surveillance of Public Rest Rooms: Privacy in the Common Area?" (1989) 6 Cooley Law Review 483

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

SHARPE S, "Electronic Eavesdropping: A chance for accountability?" (1996) 146 New Law Journal 1088

SIVARAJASINGAM V and SHEPHERD J P, "Effect of closed circuit television on urban violence" (1999) 16 Journal of Accident and Emergency Medicine 255

STEEVES V, "Privacy in the Workplace: A Moral and Legal Right" (1997) 2(8) Privacy Files 2

UNITED KINGDOM, HOUSE OF LORDS SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY, Digital Images as Evidence (Fifth Report, 1997-98, HL 64)

UNITED STATES, GENERAL ACCOUNTING OFFICE, Identity Fraud (Report No GGD 98-100BR, 1998)

WACKS R, "Reconciling privacy and free speech" (1999) 4(4) Media and Arts Law Review 261

WARREN S D and BRANDEIS L D, "The Right to Privacy" (1890) 4 Harvard Law Review 193 at 195

WESTERN AUSTRALIA, Parliamentary Debates (Hansard) Legislative Assembly, 21 October 1997

WESTIN A, "Monitoring and New Office Systems" Part II of "Employee Privacy, Monitoring and New Technology" Chapter 6 of Arbitration 1988: Proceedings of the Forty-First Annual Meeting of the National Academy of Arbitration (Bureau of National Affairs, Washington, DC, 1989)

WESTIN A, "Privacy in the Workplace: How Well Does American Law Reflect American Values" (1996) 72 Chicago-Kent Law Review 271

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

WORKING PARTY ON VIDEO SURVEILLANCE IN THE WORKPLACE, Report to the Hon J W Shaw QC MLC Attorney General and Minister for Industrial Relations (NSW Department of Industrial Relations, Sydney, December 1996)

YOST G, Spy-Tech (Harrap, London, 1985)

ZABEL M L, "A High-Tech Assault on the 'Castle': Warrantless Thermal Surveillance of Private Residences and the Fourth Amendment" (1995) 90 Northwestern University Law Review 267

INDEX