NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

Listening devices and other forms of surveillance: issues and proposals for reform

by

Rachel Simpson

Briefing Paper No 20/97

Listening devices and other forms of surveillance: issues and proposals for reform

by

Rachel Simpson

NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

Dr David Clune (9230 2484), Manager

Dr Gareth Griffith (9230 2356) Senior Research Officer, Politics and Government / Law

Ms Honor Figgis (9230 2768) Research Officer, Law

Ms Rachel Simpson (9230 3085) Research Officer, Law

Mr Stewart Smith (9230 2798) Research Officer, Environment

Ms Marie Swain (9230 2003) Research Officer, Law/Social Issues

Mr John Wilkinson (9230 2006) Research Officer, Economics

ISSN 1325-5142
ISBN 0 7310 5998 0

© 1997

Except to the extent of the uses permitted under the *Copyright Act 1968*, no part of this document may be reproduced or transmitted in any form or by any means including information storage and retrieval systems, without the prior written consent from the Librarian, New South Wales Parliamentary Library, other than by Members of the New South Wales Parliament in the course of their official duties.

Should Members or their staff require further information about this publication please contact the author.

Information about Research Publications can be found on the Internet at:
http://www.parliament.nsw.gov.au/gi/library/publicn.html

October 1997

Briefing Paper is published by the NSW Parliamentary Library

CONTENTS

EXECUTIVE SUMMARY

Surveillance involves monitoring the movements of another person. The most common types of electronic surveillance are aural surveillance ("bugging") and visual surveillance. Surveillance may be covert, where it is carried out without the notice of the subject, or overt, where the subjects are aware that the devices are in use, whether or not they are aware of the actual incidence of surveillance taking place.

Aural surveillance may be undertaken using either a) a telephone intercept or b) a listening device (pp 2-4). The use of **listening devices** is governed by the *Listening Devices Act 1984* (NSW), which prohibits the use of a listening device to record or listen to a private conversation to which the person is not a party, or to record a conversation to which the person is one of the parties. **Telephone intercepts** are governed by the Commonwealth *Telecommunications (Interception) Act 1979*, which prohibits the interception of a communication passing over a telecommunications system, either by the person or by a third person authorised by the person. Both Acts provide an exception to the prohibition when the device is used under a warrant issued by a judge upon proper application. (pp 13-15).

Visual surveillance involves the use of still cameras, closed circuit television or video cameras to observe a person. There is presently no legislation covering the use of video surveillance devices in New South Wales, unless the device doubles as a listening device. Similarly, there is no legislative prohibition on the use of **tracking devices**. A tracking device is a device which is attached to, or installed in, a moveable object for the purpose of monitoring the position of the object (pp 4-5). Another form of surveillance which is becoming increasingly prevalent is **computer surveillance**. This involves accessing or reading the storage mechanism of a computer or monitoring a person's operation of a computer. Computer surveillance *per se* is not regulated, except to the extent that the surveillance constitutes an offence under Part 6 of the *Crimes Act 1900* (NSW), which makes it an offence to engage in certain computer hacking activities (pp 5-6).

The regulation of surveillance is a achieved through a mixture of common law, specific surveillance and general privacy legislation and voluntary or involuntary codes of conduct. All forms of regulation are limited to some extent, the most important limitation being an inability to evolve at a pace consistent to that of technological development. The common law and general privacy legislation have further disadvantages because such general provisions may not be appropriate to the specific problems posed by surveillance. For example, the common law of trespass has been used to prosecute a person who trespasses while installing a surveillance device. However, an injunction preventing the publication of any material gained as a result of the trespass will only be granted where it can be proven that use of the material would be "unconscionable". The legal regulation of surveillance on all levels is examined at pages 11-20.

One of the most popular uses for surveillance is for law enforcement purposes (pp 7-8). The NSW Police Royal Commission, for example, stated in its *Final Report* that the use of electronic surveillance was the single most important factor in achieving a breakthrough in its investigations. Police interviews have also been recorded since 1991. Other uses of

surveillance include: public safety (pp 8-10); protection of private property (p 10), and protection of employers' interests (pp 10-11). Private investigators and the media also employ surveillance techniques.

The argument surrounding surveillance can be broadly divided among those who believe the public interest advantages of surveillance as a law enforcement tool outweigh any privacy argument, and those who believe that the intrusion into privacy by surveillance devices is so great that only under the most exceptional circumstances should surveillance be allowed. Although most people agree that there are circumstances where the benefits offered by surveillance justify its use, the debate evolves around exactly what those circumstances are. This question is not made easier by public perception of surveillance: despite a general view that surveillance infringes an individual's right to privacy, there are situations where the community welcomes surveillance. A long, dark pedestrian subway is one example given. The arguments for surveillance are examined at pages 21-24, and those against surveillance at pages 24-26.

There is a consensus regarding reform of the regulation of surveillance. That is that regulation of some form must extend to all types of surveillance, most particularly video surveillance and tracking devices. There is debate over the extent of the regulation, with the Royal Commission and other arguing that there are some instances where regulation is unnecessary, such as the use of overt visual surveillance in public places. There is also debate over whether that regulation should take the form of legislation, or whether a voluntary code of conduct is preferable. Such a code of conduct may be with or without legislative backing, and may be developed by the industries which it most greatly effects. Some of these recommendations for reform are examined at pages 26-29.

1.0 INTRODUCTION

The Royal Commission into the New South Wales Police Service ("the Royal Commission") found that the use of electronic surveillance was the single most important factor in achieving a breakthrough in its investigations, and was of the view that the proliferation of the drug trade and the increasing sophistication of organised crime makes electronic surveillance equally useful for conventional law enforcement agencies.[1] This view is common amongst law enforcement agencies. The New South Wales Independent Commission Against Corruption (ICAC) and the Australian Federal Police (AFP) both use electronic surveillance regularly, the AFP most often in the investigation of major drug importation cases. It is the opinion of the Royal Commission that it is essential that the Police Service, the Crime Commission, the newly formed Police Integrity Commission and the ICAC all be equipped with electronic surveillance capacity and resources, including listening devices, intercepts of telephones and other forms of telecommunications, tracking devices and video surveillance.

It is not disputed that surveillance can be extremely beneficial for law enforcement purposes. However, civil libertarians argue that surveillance, particularly video surveillance, is so intrusive into an individual's right to privacy, that use of electronic surveillance devices must be restricted to the most exceptional circumstances where it can be clearly proven that the public benefit outweighs the infringement of an individual's privacy. Amongst the reasons for this view, apart from the intrusiveness of surveillance, is a concern over "function creep" whereby, once installed, surveillance devices are used for purposes other than those initially envisaged, and the increased opportunities for fraud and other corrupt practices that technological advances in this area raise.

Presently, visual surveillance, tracking devices and other less common forms of surveillance are not specifically regulated. The only regulation is indirectly through the application of general privacy legislation or the common law. It is, therefore, not illegal to install and use a visual surveillance device as long as none of these general laws are infringed. Regardless of on which side of the debate the commentators sit, there is a consensus that all forms of electronic surveillance need to be the subject of some type of formal regulation. An interesting point was made by the New South Wales Law Reform Commission in relation to this call for regulation: regulation *per se* will have little impact on deterring criminal uses of surveillance, unless it provides for high penalties for illegal use, restriction on the sale of some items and substantial influence on enforcement.[2] Regulation without these and other measures will, therefore, only serve to legitimise already "lawful" uses of surveillance.

This paper begins by examining surveillance, the different types of electronic devices available for surveillance, and the uses to which surveillance is put. It continues by looking

---

1 Royal Commission into the New South Wales Police Service, *Final Report - Volume 2: Reform*, May 1997, p. 448.

2 New South Wales Law Reform Commission *Issues Paper 12 - Surveillance*, May 1997, pp. 6-7.

at the regulation of surveillance on all levels, from international treaties to unenforceable voluntary codes of practice. The arguments for and against surveillance are canvassed, and, finally, some of the suggestions for reform put forward by the Royal Commission and other interested bodies are discussed.[3]

2.0 TYPES OF SURVEILLANCE

Surveillance involves monitoring the movements or affairs of a person or persons. The *Butterworths Concise Australian Legal Dictionary* defines surveillance generally as "watching and recording the movements of a person or premises suspected of being involved in criminal activity".[4] Surveillance may be covert or overt. **Covert surveillance** is carried out by concealed devices without the notice of the subject. **Overt surveillance**, on the other hand, is carried out in such a way as the subjects of the surveillance are made aware that devices are being used, whether or not the subject is aware of a particular incidence of surveillance.[5] Traditionally, surveillance was undertaken in person, for example by a police officer, and without the aid of any electronic equipment. However, with increasing technological developments, the use of electronic surveillance devices has become increasingly popular, particularly in the investigation of sophisticated and complex crime. The Queensland Criminal Justice Commission uses the term **electronic surveillance** to refer to 'a range of devices that are used to overtly record or monitor sounds, images, movement, signals or data'.[6] This is the term considered most appropriate for the purposes of this paper. The three most common types of electronic surveillance are aural surveillance (listening devices), visual surveillance (eg video or closed circuit television) and vehicle location systems or tracking devices.[7]

2.1 Aural surveillance

Aural surveillance, colloquially known as "bugging", can take one of two forms:

- radiating of radio frequency devices and receiver (listening devices), or

---

3 I acknowledge my heavy reliance on three recently published reports in the preparation of this paper: the New South Wales Law Reform Commission *Report 22: Surveillance*, volume II of the Royal Commission's *Final Report* and volume V of the Queensland Criminal Justice Commission's *Report on a review of police powers in Queensland* which focuses on electronic surveillance and other investigative procedures.

4 P Nygh & P Butt (eds) *Butterworths Concise Australian Legal Dictionary*, Sydney, 1997, p. 385. This definition of surveillance is limited because it only applies to surveillance by police for which a warrant has been issued, and does not allow for surveillance generally, for example surveillance in the workplace or surveillance in public places where the subjects of surveillance may or may not be suspected of committing a crime.

5 NSWLRC, n 2, pp. 6-7.

6 Criminal Justice Commission, *Report on a review of police powers in Queensland - volume V: electronic surveillance and other investigative procedures,* October 1994, p. 749.

7 Ibid.

- non-radiating devices, such as wired surveillance systems, telephone intercepts, and concealed microphones.[8]

In New South Wales, that part of aural surveillance which is characterised as utilising a **listening device** is governed by the *Listening Devices Act 1984*. Under this Act, a listening device is defined to be:

> any instrument, apparatus, equipment or device capable of being used to record or listen to a private conversation simultaneously with its taking place.[9]

The other main form of aural surveillance - **telephone intercepts**, is covered by the Federal *Telecommunications (Interception) Act 1979* (Cth). For the purposes of that act, interception of a telecommunication is defined in section 6 as:

> ... listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

The communication may be a conversation or a message, or any part of a conversation or message, and specifically includes:

- speech, music or other sounds;
- data;
- text;
- visual images, whether animated or not;
- signals, or
- any other form or any combination of forms.[10]

Interception is said to have taken place if a third party listens to or records a conversation between two or more people over a telecommunications system, or if one party to a telecommunication records a conversation without the knowledge of the other party.[11]

---

8 Legislative Assembly of Queensland Parliamentary CriminalJustice Committee, *Report on the Review of the Criminal Justice Commission's Report on a Review of Police Powers in Queensland*, *vol V: Electronic Surveillance and Other Investigative Procedures*, Report No. 28, 12 May 1995, p. 13.

9 *Listening Devices Act 984* (NSW), section 3(1), definition of 'listening device'.

10 *Telecommunications (Interception) Act 1979* (Cth), section 5(1), definition of 'communication'.

11 *Duncan v R* (1991) 5 WAR 249, in Nygh, n 4, p. 211-212.

The relationship between the two regimes is complicated and is discussed further in Part 4 - legal framework.

2.2 Visual surveillance

Electronic **visual surveillance** involves observation of a target, primarily through the use of cameras, closed circuit television or video cameras.[12] There is no definition of `visual surveillance device' in New South Wales legislation, however, section 4 of the *Drugs Misuse Act 1986* (Qld) defines a visual surveillance device to mean:

> ... any instrument, apparatus, equipment or device capable of being used to record and monitor images simultaneously with their taking place.

There is currently no legislation governing either covert or overt visual surveillance in New South Wales, unless the equipment can also be characterised as a listening device, in which case it is governed by the *Listening Devices Act 1984*. Similarly, there is no legal rule preventing the use of a camera to film a person on private property if no trespass has occurred. The *Industrial Relations Act 1996* (NSW) includes as an "industrial matter" the surveillance of employees at the workplace, although this does not operate to make it either illegal to utilise surveillance devices in the workplace.[13] For a more detailed examination of the law in regard to visual surveillance, see Part 4 - legal framework.

A more realistic description of the types of surveillance outlined above could be **audio-visual** surveillance, a combination of both aural and visual surveillance. The New South Wales Law Reform Commission (NSWLRC) believes that the distinction between the two is in many ways artificial and is, in fact, blurred. Many modern devices now record both sound and images simultaneously. Another example given by the Commission of the blurring of the distinction between the two types of surveillance is a person who is capable of lip reading, who might, in some circumstances, be able to ascertain what is being said from a video recording of a target despite the lack of audible words.[14]

2.3 Tracking devices

The Queensland Criminal Justice Commission defines a **tracking device** as a "vehicle location system magnetically attached to, or installed in vehicles or other moving things".[15] Tracking devices can be installed in cars, on persons, or attached to moveable objects such as containers, allowing the position of the object to be monitored.[16] A tracking device may

---

12 NSWLRC, n 2, p. 8.

13 *Industrial Relations Act 1996* (NSW), section 6.

14 Ibid, pp. 8-9.

15 Qld Criminal Justice Commission, n 6, p. 793.

16 NSWLRC, n 2, p. 9.

be a simple device which assists in the location or tracking of a vehicle through the generation of a recurrent radio signal, or it may be a more sophisticated device which also has listening capabilities.[17] If this is the case, the use of such a tracking device may fall under the *Listening Devices Act 1984*. The NSWLRC has identified problems for law enforcement agencies stemming from the lack of specific provisions relating to such tracking/listening devices. The problems may occur particularly in relation to the installation of the devices. An example given by the Commission is installing a device in a motor vehicle which may be seen as trespass unless the owner has consented, so any evidence gathered may be treated as illegally obtained.[18]

From 1 July 1997, all taxicabs operating in the Metropolitan transport district that are connected to a taxi radio network must be fitted with an approved vehicle tracking device.[19] For the purpose of this Regulation, an approved vehicle tracking device is "a device by which the whereabouts of a taxicab can be followed by means of the vehicle tracking system operated by the taxi radio network to which the taxicab belongs ...".

2.4 Computer surveillance

Computer surveillance involves accessing or "reading" the storage mechanism of a suspect's computer, or monitoring a person's operation of a computer.[20] It has been reported that the US Congress is poised to approve a plan whereby the FBI would have access via a "backdoor" to all information on computers with communication or encryption software distributed after 1998.[21] An additional form of computer surveillance is made possible through technology which enables the reception, reconstitution and analysis of unintentionally transmitted radiation or signals emanating from electronic equipment. This type of surveillance is known as a "Tempest attack" and can target the following electronic equipment:

- computer disk drives;
- printers;
- visual display units;
- modems;

---

17 Qld Criminal Justice Commission, n 6, p. 793.

18 NSWLRC, n2, p. 9.

19 *Passenger Transport (Taxi-Cab services) Regulation 1995* (NSW), section 7A. This provision also applies to taxi-cabs operating in the Newcastle, Wollongong, Gosford and Wyong transport districts from 1 July 1998.

20 NSWLRC, n 2, pp. 9-10.

21 D McCullagh, 'Building in Big Brother', *The Netly News*, September 1997, http://cgi.pathfinder.com/@osO2WwQAZRBVq@K3/netly/, p. 1. This proposal was passed by the US Congress House Intelligence committee on 11 September 1997, in a move that will, if passed, make it legal to own software that has data-scrambling features, but illegal to sell, import or distribute such software.

- fax machines;
- telexes;
- intercoms, and
- telephone systems.[22]

The effect of this technology is that, for example, what is on a person's computer screen can be "read" by analysing the radiation emanating from that screen. There is no legislation preventing such surveillance, with the exception of the provisions in Part 6 of the *Crimes Act 1900* (NSW) which makes it an offence to engage in certain computer hacking activities.

3.0 USES FOR SURVEILLANCE

Surveillance is used for a number of reasons. Once again there is a distinction based upon whether the surveillance is overt of covert. The most accepted use of covert surveillance is for **law enforcement** purposes. The police, the Independent Commission Against Corruption (ICAC), the New South Wales Crime Commission (NSWCC) and the recent Royal Commission into the New South Wales Police Service (the Royal Commission) all carried out covert surveillance. The Australian Federal Police (AFP), the National Crime Authority (NCA) and Australian Security Intelligence Organisation (ASIO) also carry out covert surveillance.[23] However, surveillance is being used increasingly for other purposes, and increasingly by non-government organisations, such as private security organisations and private property owners. It has been estimated that, in Victoria, more people were employed in the private security industry than were in the police forces in the 1980s.[24] There is nothing to suggest that this is untrue for New South Wales or that the trend has reversed in the 1990s.

The private security industry relies heavily on video surveillance, particularly closed circuit television, which is used in many shopping centres and malls such as Paramatta Westfield and Darling Harbour in Sydney.[25] It has been estimated that the cost of installing video surveillance cameras ranges from $2,000 for a fixed camera unit to $5,000 for a unit with pan, tilt and zoom capacities. This compares very favourably to the cost of employing a professional security guard - estimated at around $130,000 to $170,000 for a single around the clock security guard.[26] Surveillance is also becoming more common in the **workplace**.

---

22 D Price, *Fraudbusting: how to identify and deal with corporate fraud...and how to prevent it*, London, 1991, p. 123.

23 NSWLRC, n 2, p. 10.

24 R Haldane, *The People's Force: a history of the Victorian Police* (2nd ed), Melbourne 1994, p. 251.

25 The private security industry is one of the biggest proponents of video surveillance, mainly on the grounds of efficiency and deterrence. The reasons for this support are discussed more fully in Part 5.1 - Arguments for surveillance.

26 Privacy Committee of New South Wales, *Invisible Eyes: report on video surveillance in the workplace*, No 67, September 1995, p. 25.

This issue was the subject of a Privacy Committee of New South Wales report, *Invisible Eyes: report on video surveillance in the workplace*, published in September 1995, and is discussed in more detail below at 3.4 - Protection of employers' interests.

3.1 Law enforcement

The police have used listening devices as well as video cameras in licenced premises to enforce liquor licensing laws, and computer surveillance in the investigation of fraud offences and the monitoring of some paedophilia offences.[27] The New South Wales Privacy Committee 1994-95 Annual Report reported a 370% increase in the warranted use of listening devices in New South Wales by state and federal law enforcement agencies.[28] It is, however, argued that surveillance devices meet needs that other investigative techniques cannot. For example, the NSWCC's submission to the NSWLRC argued that:

> Over the years of its operation, the Commission has found that listening devices are an effective method of gathering evidence in the investigation of drug crime. Evidence of drug transactions can be difficult to obtain because typically transactions are conducted covertly, so that visual surveillance is not possible or at least difficult, offenders work in familiar groups and are extremely wary of infiltration by undercover officers or police agents, and they employ counter-surveillance techniques and communicate by means of digital telephones that can not be intercepted.[29]

Surveillance is a particularly effective **crime *detection* tool**, especially when the recording can be used in evidence in criminal trials.[30] In evaluating its effectiveness, the issue of the admissibility of illegally obtained evidence must be considered. If the surveillance was undertaken without the proper warrant, or if, in the case of unregulated surveillance, the person placing the surveillance device was trespassing, then the results of the surveillance project were illegally obtained and hence not admissible. It is also argued that surveillance is an effective **crime *prevention* tool**, particularly when used overtly in public places. This argument is discussed more fully in Part 3.2 - Public Safety.

Police interviews

The New South Wales Police Service **introduced electronic recording of interviews** with suspect persons in January 1991. There has been debate about the relative merits of covert or overt recording. The compromise which appears to the police to satisfy requirements from both sides is to covertly record an interview, having informed the suspect that he or she is being electronically recorded. It is characterised as 'covert' because, although the

---

27 NSWLRC, n 2, p. 10.

28 Privacy Committee of New South Wales *Annual Report 1993-94*, 1995, p. 33.

29 NSWLRC, n 2, pp. 14-15.

30 Ibid, p. 14.

subject has been informed that surveillance will take place, the camera is not in the interview room so the subject is unaware if and when the camera is recording.[31] The objectives of this system were identified in a report by the Attorney-General's Criminal Law Review Division, released in 1986 as:

1. to deter and/or prevent the use of unfair practices by the police prior to, during and after interviews;

2. to deter the making of unfair and false allegations of improper behaviour by police;

3. to provide an objective means of resolving disputes about the conduct and substance of police interviews, and

4. to provide the courts with a reliable account of statements made by persons accused of crime while in police custody.[32]

More than 30,000 interviews were recorded and represented in court without significant problems between up until 1994. The use of recording has resulted in an increase in guilty pleas, and there has been strong anecdotal evidence from crown prosecutors that the *voir dire* concerning the admissibility of confessional evidence are fewer and shorter.[33] All other states and the Northern Territory also employ electronic recording of interviews, although there are vast variations in the sophistication of the technology used and the number of recordings produced.[34]

3.2 Public safety

Public safety arguments have been used to justify a large number of extensions to the use of surveillance. Some examples follow. The Northern Territory government has been reported as considering whether to introduce electronic bracelets to impose a night time curfew on children. The rationale given by the territory's Minister for Correctional Services, Mr Steve Hatton, was that "...there are too many young kids wandering the streets in the middle of the night getting up to mischief or being placed at risk".[35] Similarly, alleged service station robber Fred Saad has been released on bail pending trial on the condition that he wear an electronic surveillance device in the form of a watch. The watch beeps at certain intervals, at which time the wearer must telephone a number and hold the watch face up to the receiver. A computer generated message is transmitted, allowing the wearer's

31 J R Watkins, 'Videotaping interrogations and confessions', NSW Police News, June 1994, p. 22.

32 R. Kilburn, 'Electronic recording of police suspect interviews in NSW', *NSW Police News*, June 1994, p. 24.

33 Ibid.

34 Ibid, p. 25.

35 C Ryan, 'Territory looks at electronic bracelets to keep track of children', *Sydney Morning Herald*, 10 September 1997.

whereabouts to be ascertained.[36] This form of surveillance is different from that utilised in home detention, where the offender wears what is essentially a tracking device.[37]

Local councils are using "**street surveillance**" in an attempt to prevent crime. Fourteen cameras were installed in September 1996 in the Cabramatta and Canley Vale areas, and in May 1995 video cameras were installed in the George Street cinema complex area. Up to twelve cameras have been proposed for "hot spots" around the Sydney CBD, including Circular Quay, Chinatown and Pitt Street Mall.[38] It is proposed that these cameras be linked to telephones so that people in distress could call the police. Street surveillance has the dual benefit of protecting public safety and assisting with law enforcement, however, their effectiveness as a deterrence has been questioned, with the George Street trial being labelled a "failure", as often as a "success".[39] The effectiveness of such systems depends greatly on the level of resources backing up the surveillance operation and the possible response time. It is further argued that such surveillance simply moves crime from one place to another, rather than preventing it. For greater detail on the arguments against surveillance, see Part 5.2.

Surveillance has also been used for public safety purposes where large crowds are involved and individual policing may be less effective. Most people, argues the NSWLRC, will accept some form of public surveillance, for example, at major sporting events, in return for a greater feeling of safety,[40] or in a long pedestrian subway where it has been known sexual assaults have taken place. Video surveillance is used at the Sydney Football Stadium, where the technology enables a camera to focus on individual spectators within a crowd and generate a printed image of the individual within a short space of time.[41] The question here is where to draw the line. This is a question not easily answered, in part because the community's perception of surveillance and its intrusiveness will change in different situations and under different circumstances, such as those outlined briefly above. This may be despite a general view that public surveillance infringes a person's's right to privacy. The NSWLRC gives another example, of hidden video cameras in toilets and change rooms, which, ordinarily, are seen as unequivocally unacceptable. However, there may be occasions

---

36 A Peterson, 'Home jail patrolled by watch', *Daily Telegraph*, 21 July 1997.

37 For a more detailed discussion of home detention, see H Figgis, *The Home Detention Bill 1996: Commentary and Background*, Briefing Paper No 20/96.

38 N Papadopoulos, 'Spy cameras get go-ahead to focus on city trouble spots', *Sydney Morning Herald*, 7 February 1997. In contrast, the NSWLRC reports that the trial was "adjudged a success", relying on a NSW Police Service official report into the trial: NSWLRC, n 2, p. 30.

39 R Wainwright, ''Spy' cameras at end of a phone', *Sydney Morning Herald*, 11 January 1997.

40 NSWLRC, n 2, p. 15.

41 Privacy Committee of New South Wales, n 26, p. 16.

when the community would accept such an intrusion, for example after a series of bombs placed in toilets.[42]

Surveillance has been used by the Roads and Traffic Authority (RTA) to improve road safety by monitoring and controlling heavy vehicle speed and safety. Safe-T-Cams commenced operation in 1994. They work by, firstly, detecting the size of the oncoming vehicle and then taking a detailed digital image of the vehicle using an infra red flash. A computer extracts the vehicle's registration number from the second image and this, together with the time of observation of the vehicle is passed on to a central database.[43] Surveillance has also been employed to monitor toll booths, to decrease toll-evasion and improve the safety of toll collectors.

3.3 Protection of property

Surveillance is being used by both businesses and private property owners to protect their property. Most common is the use of closed circuit television or fixed cameras. Increasing numbers of house owners utilise video surveillance as a protective measure against home invaders, in addition to or instead of employing security guards. Shop owners are also using surveillance devices to prevent and monitor shoplifting and other crime, in this instance fulfilling the dual purposes of law-enforcement protection of property. In fact, in its report *Invisible Eyes: report on visual surveillance in the workplace*, the New South Wales Privacy Committee reports that the retail industry accounts for the largest investment in video surveillance equipment in Australia.[44] In most cases there is usually signage warning customers that cameras are in use. The NSWLRC gives the example of automatic teller machines which are often labelled with "Warning: you may be photographed while using this machine".[45] Other areas where surveillance is used to protect property (and control crime) are: casinos; banks; shopping centres and malls; petrol stations; building and site access; car parks; office foyers and lobbies, and elevators.[46]

3.4 Protection of employers' interests

Surveillance is used by **employers** with the major aim of protecting themselves and their businesses against security risks such as theft, fraud, vandalism and threats to the personal safety of employees.[47] Both covert and overt surveillance is used. Employers argue that they have a right to protect their own property by supervising their employees. However, privacy interests must also be recognised, such as the right of a person not to be photographed

---

42 NSWLRC, n 2, pp. 16-17.

43 Privacy Committee of New South Wales, n 28, pp. 31-32.

44 Privacy Committee of New South Wales, n 26, p. 25.

45 NSWLRC, n 2, p. 11.

46 Privacy Committee of New South Wales, n 26, p. 18.

47 Ibid, p. 24.

without consent.[48] There is concern that employers are using the information gained through video surveillance for purposes other than those for which it was originally installed, such as secretly monitoring individual work performance.[49]

The New South Wales Privacy Committee has prepared guidelines on the use of video surveillance in the workplace, *Guidelines on Overt Video Surveillance in the Workplace*, which were published in September 1995. The New South Wales Department of Industrial Relations published a *Voluntary Code of Practice for the Use of Overt Video Surveillance in the Workplace* following the recommendations of a Working Party on video Surveillance in the Workplace established in March 1996. The Attorney-General, Hon. Jeff Shaw, MLC, has proposed legislation to implement the recommendations of the Working Party. The Bill, provisionally titled *Video Surveillance in the Workplace Bill* is in the consultation stage, and has been given to the members of the Working Party and other interested parties for their consideration. It is hoped that this Bill will be introduced into parliament in late 1997. Industrial laws also limit the use of surveillance in the workplace. For example, the *Industrial Relations Act 1996* (NSW) includes in its definition of an industrial matter, "the surveillance of employees in the workplace" (section 6). While this does not prohibit the use of surveillance in the workplace, it does serve to limit surveillance by making it an issue about which employees may have a legitimate grievance.

3.5 Other uses for surveillance

Private investigators often use surveillance devices. Matrimonial disputes and alleged insurance or workers compensation frauds are common reasons for private investigators to employ surveillance. Concern has been raised that private investigators are trespassing or using listening devices without warrants in carrying out these investigations. The **media** also employ surveillance techniques. Most popular with the media are long range cameras, which allow for visual access without trespassing, as well as hidden cameras.[50]

4.0 LEGAL FRAMEWORK

The use of electronic surveillance devices in New South Wales is regulated by **common law** as well as **legislation**. Australia is also signatory to a number of **international treaties**, our obligations under which effect any regulation of listening devices. Additionally, there are a guidelines for the use of certain types of electronic surveillance which have been published by interested parties. This framework is further complicated by the application of both Federal and State legislation, the demarcation between the two sometimes raising issues of

---

48 NSWLRC, n 2, p. 16.

49 Privacy Committee of New South Wales, n 26, pp. 24, 27-34.

50 NSWLRC, n 2, p. 11. Lang Powell, the Press Council's vice-chairperson, was reported as saying that privacy complaints by public figures and private citizens had trebled to nine per cent of complaints to the council since 1994: M Kingston, 'Privacy may come out of the too-hard basket', *The Sydney Morning Herald*, 2 September 1997.

constitutional law and statutory interpretation.[51] The reason for this dual regime is the telecommunications power conferred upon the Commonwealth under section 51(v) of the Constitution, giving the Commonwealth a monopoly over "postal, telegraphic and other like services".

Any scheme attempting to regulate the use of electronic surveillance devices must seek to satisfy the conflicting goals of protecting individual privacy and protection of the public in the detection and prevention of crime. It is in order to achieve this that most regulatory schemes work to restrict the use of electronic surveillance devices to protect privacy. Or, as put by Keith Mason QC, "conscious of intrusions into privacy and potential for abuse, Parliaments have attempted to provide narrow gateways through which agencies must pass before they may lawfully use listening devices [or other forms of electronic surveillance] or enjoy their fruits."[52] In order to examine the regulation of electronic surveillance, therefore, privacy law becomes very important, particularly in relation to visual surveillance devices, which are not specifically legislated for, the use of which is therefore governed by indirect means.

4.1 Common law

"Privacy" as a separate right is not protected by the common law. Rather, privacy is afforded indirect protection by other legal rights. Nuisance, defamation and trespass all incidentally protect an individual's privacy. All these common law protections have limitations, however. For example, the tort of **nuisance** allows a landowner to protect the reasonable use and enjoyment of his or her land, or of some right over it.[53] There is, however, doubt over the capacity of nuisance to protect a person's right to privacy where the person does not have a proprietary interest (absolute ownership and the financial interest) in that land.[54] The law of defamation can only protect a person's privacy where the information published is defamatory, which occurs when the information is either a) untruthful or b) truthful but not in the public interest. Where the information is not defamatory, the fact that the information is personal or private does not affect the lawfulness of its publication.[55] It is also irrelevant to the tort of defamation how the material was obtained. Similarly, trespass only indirectly protects privacy. Where a person trespasses, or enters the land of another without that person's consent, in order to gain information such as photographs, an injunction preventing publishing of that material will only be granted where it can be proven that the use of the material would be "unconscionable". The

---

51 K Mason, 'Use of listening devices by law enforcement agencies', *The College of Law Continuing Legal Education No 95/12: Advanced Criminal Law*, p. 2.

52 Ibid, p. 1.

53 Nygh, n 4, p. 279.

54 D Yarrow, 'Developments in the Law of Privacy - Law and Policy', *The Queensland Lawyer*, Volume 17, October 1996, p. 60.

55 Ibid.

questions of freedom of speech and expression were the reasons given for this decision in *Emcorp Pty Ltd v ABC* [1988] 2 Qd R 169.[56]

4.2 Statutory provisions

Statutory provisions generally fall in one of two areas: specific surveillance legislation, and general privacy legislation. There are also other incidental statutory regulations, such as that outlined above in relation to video surveillance in the workplace (see Part 3.4 - Protection of employers' interests).

Specific surveillance legislation

1. Aural surveillance

The relevant New South Wales Act is the *Listening Devices Act 1984*. The main Federal Act to deal with surveillance is the *Telecommunications (Interception) Act 1979* (Cth). Additionally, there are a number of other federal acts with parts relevant to the regulation of surveillance. These are:

- *Australian Federal Police Act 1979* (Part II Division 2 - serious federal offences)
- *Australian Security Intelligence Organisation Act 1979* (section 26 - security matters)
- *Customs Act 1901* (Part XII Division 1A - narcotics offences).

The ***Telecommunications (Interception) Act 1979*** (the Interception Act) prohibits the interception of a communication passing over a telecommunications system. The prohibition is contained in section 7(1):

> A person shall not:
>
> a) intercept;
> b) authorise, suffer or permit another person to intercept; or
> c) do any act or thing that will enable him or another person to intercept;
>
> a communication passing over a telecommunications system.

There are a number of exceptions to this prohibition, which are contained in section 7(2) of the Interception Act, most important being that in section 7(2)(b) which provides that the prohibition does not apply in relation to "the interception of a communication under a warrant". Those bodies able to apply for a warrant include: the AFP, the NCA, and participating State law enforcement agencies, including, in New South Wales, the New

---

56 Ibid. This is the approach adopted by the Australian Press Council, whose policy is that news be 'gathered with respect for the privacy and sensibilities of individuals [but] that the right to privacy should not prevent publication of matters of public record or obvious or significant public interest': see M Kingston, n 50.

South Wales Crime Commission, the New South Wales Police Force, ICAC and, the Police integrity Commission.[57] A further prohibition is imposed by section 63: if a communication obtained in contravention of section 7(1) is: communicated to another; made use of; made a recording of, or given in evidence in a proceeding, a penalty of up to $5,000 or two years' imprisonment may be imposed. This is despite the fact that the communication was otherwise lawfully obtained.[58]

The primary object of the Interception Act, according to the 1995/96 Annual Report into its operation, is "to protect the privacy of individuals who use the telecommunications system by making it an offence to intercept communications passing over that system other than in accordance with the provisions of the Act."[59] This reflects the policy underlying the Act, which is in order to achieve a balance between the competing pressures of law enforcement and the right to privacy, interception should only be used in relation to criminal prosecutions for serious offences.[60] However, the NSW Police Royal Commission is of the view that because a significant number of offences defined as serious at the state level do not achieve this status for the purposes of the Interception Act because the minimum sentence is less than seven years imprisonment or the offence is not specifically referred to in the definitions of the Interception Act, the Act's potential application is reduced.[61]

Section 5 of the ***Listening Devices Act 1984*** (the LDA) contains the prohibition:

> A person shall not use, or cause to be used, a listening device:
>
> (a) to record or listen to a private conversation to which the person is not a party, or
>
> (b) to record a private conversation to which the person is a party.[62]

The main exception to this prohibition relates to the use of a listening device under a warrant granted pursuant to Part 4 of the LDA. A warrant may be issued by a judge upon application that the person applying suspects or believes that a prescribed offence has been, or is likely to be committed and that for the purpose of investigating that offence the use of a listening

---

57 While operational, the right was also afforded to the Royal Commission into the New South Wales Police force.

58 A Collier, 'When does unauthorised listening become interception?', *Law Institute Journal*, January-February 1994, p. 59. This article is particularly useful because it very clearly outlines what constitutes interception for the proposes of the Interception Act.

59 *Telecommunications (Interception) Act 1979: Report for the year ending 30 June 1996*, AGPS, Canberra 1996, p. 4.

60 Royal Commission, n 1, pp. 450-451.

61 Ibid, p. 451.

62 *Listening Devices Act 1984* (NSW), section 5(1).

device is necessary.[63] A prescribed offence is defined in sec 15 generally as an offence that is punishable on indictment or is of a class of offence prescribed for the purposes of Part 4. This second class of offence could greatly widen the scope of the Act by including many, less serious offences as those which may qualify for issue of a warrant. Not only is use of a listening device without a warrant unlawful and it therefore carries a penalty, but any evidence obtained through such use is usually excluded as unlawfully obtained evidence. In 1995, 1341 warrants for listening devices were south in New South Wales. No applications were refused.[64] Of the 758 applications for warrants under the Interception Act in 1995/96, only 11 were refused.[65]

Where there is an overlap between the LDA and the Interception Act, the High Court decided in *Miller*[66] that the Interception Act will prevail. When determining which Act will apply in any given situation, the principal criterion seems to be whether the relevant communication is being carried over or passed by a telecommunications system. If the communication is not in electromagnetic form, it is not part of a telecommunications system as defined by the Interception Act and it is not that act which is applied. For example, once the communication is in the form of audible speech, it becomes subject to the LDA, not the Interception Act.[67] When these principles are applied to non-voice communication, there is an argument that until the communication obtains the character of stored information it is still being "carried" over a telecommunications system. It is only once the communication ceases to be carried or passed over the transmission system that the Interception Act ceases to apply, as the communication is no longer capable of being intercepted. Other protections such as computer trespass (hacking) or unauthorised access to data are applied instead.[68]

2. Visual surveillance

There is currently no specific legislation governing the use of video surveillance. Audiovisual surveillance is also not regulated, except to the extent that it is regulated as a listening

---

63 Ibid, section 16(1).

64 Privacy Commission of New South Wales, *Submission to the New South Wales Law Reform Commission's Issues Paper 12 "Surveillance"*, August 1997, p. 17. This figure does not include warrants issued for phone taps in New South Wales under the Interception Act. The Commission continues by comparing the number of warrants issued in the United States to the number in New South Wales. The combined total for listening devices and wire taps in the United States in 1995 was 1058. The Commission made the further comparison that if New South Wales issued listening devices at the same rate per population as the United States, only 26 application would have been made in 1995.

65 *Interception Act Annual Report 1995/96*, p. 14. The number of warrants issued in 1994/95 was 692. The Report attributes the increase to "factors such as greater emphasis placed upon interception as an efficient and effective evidence gathering process".

66 *Miller v Miller* (1979) 141 CLR 269.

67 Collier, n 58, p. 63.

68 Ibid.

device. The Australian Law Reform Commission, in its 1983 report *Privacy*[69], recommended that the same rules apply to both aural and visual surveillance, which would have the effect that the use of video surveillance devices to observe people who would otherwise expect to be reasonably free of such surveillance would be illegal.[70] The only legislative prohibition of visual surveillance is found in the *Australian Security Intelligence Organisation Act 1979* (Cth). Section 22 defines a listening device to include equipment capable of recording images, which could include a video or other camera. However, the application of this Act is limited to special circumstances relating to the work of the Australian Security Intelligence Organisation.[71] In New South Wales, section 65 of the *Casino Control Act 1995* (NSW) makes it a condition of a casino license being granted that the New South Wales Casino Control Authority approve plans including those for the monitoring of casino operations, including the operation of closed circuit television cameras.

In relation to other users of visual surveillance devices, general laws therefore apply, such as that common law discussed in Part 4.1 above. Additionally, the *Search Warrants Act 1985* (NSW) permits private premises to be entered for the purpose of executing a properly authorised search warrant, and the LDA impliedly authorises entry of a premise to install a listening device. However, neither act deals with the installation of a video camera, except where it doubles as a listening device. The Royal Commission argued that as long as entry to a property is gained lawfully then there may be nothing illegal about using that entry to install a video surveillance device.[72] However, because the action is not specifically authorised, law enforcement agencies run the risk of the evidence being excluded because it was illegally obtained, under Part 3.11 of the *Evidence Act 1995* (NSW).

3. Tracking devices

The use of tracking devices is another area not specifically covered by legislation. Warrants have been sought and granted under the LDA for the use of listening devices with tracking capacities, but where the principal purpose of the device is aural surveillance. The installation of a tracking device usually involves some type of unauthorised and therefore illegal access, which provides the only avenue for legal recourse, using general laws as discussed in relation to video surveillance above. The Royal Commission recommends that a warrant scheme be established for the use and installation of tracking devices, similar to the scheme operating for listening devices.[73]

Privacy legislation

69 Report No. 22, 1983, vol 2, para 1183.

70 Privacy Committee of New South Wales, n 26, p. 67.

71 NSWLRC, n 2, p. 35.

72 Royal Commission, n 1, pp. 457-458.

73 Ibid, p. 459.

Privacy *per se* is not protected by the common law in Australia. See Part 4.1 for more detail on the ways in which privacy is indirectly protected by the common law. The Commonwealth ***Privacy Act 1988*** provides some protection from invasions of privacy by Commonwealth Government agencies by regulating the handling of personal information collected by those agencies. It imposes a duty on government agencies to comply with 11 privacy principles, developed from those contained in the Organisation for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of personal Data* (see Part 4.4 for more detail on these guidelines). These principles are contained in section 14 of the *Privacy Act 1988* (Cth) and relate to:

1. Manner and purpose of collection of personal information
2. Solicitation of personal information from individual concerned
3. Solicitation of personal information generally
4. Storage and security of personal information
5. Information relating to records kept by record-keeper
6. Access to records containing personal information
7. Alteration of records containing personal information
8. Record-keeper to check accuracy etc. of personal information before use
9. Personal information to be used only for relevant purposes
10. Limits on use of personal information
11. Limits on disclosure of personal information

The *Privacy Act 1988* also regulates the use of tax file numbers and information collected by private credit reporting agencies. This is the extent to which the Act applies to the private sector. Adherence to the Act is monitored by the Commonwealth Privacy Commissioner. However, legislation that merely regulates the collection of information is insufficient to regulate surveillance, as there is not necessarily a connection between surveillance and the collection of information. Surveillance is considered by many intrusive in itself, regardless of any information-collecting purpose, so simply regulating the use of information collected by surveillance is not likely to be considered an adequate protection of privacy.[74]

There is no legislative equivalent to the *Privacy Act 1988* in New South Wales, although from time to time there have been calls for such legislation. Privacy and Data Protection Bills were introduced into Parliament in 1994, 1995 and 1996, but none have been passed. More recently, at a conference on privacy laws in February 1997, the New South Wales Attorney-General announced that privacy protection legislation will be introduced in New South Wales. That legislation is in the process of being drafted. The proposed legislation, as foreshadowed by the Attorney-General, will enshrine data protection principles in legislation (such as those contained in the *Privacy Act 1988* (Cth)). The proposed scheme will allow for codes of practice to be made in consultation with the relevant industries, and backed by regulation, which are foreseen as extending to both the public sector and private agencies. The legislation will also create a statutory office of NSW Privacy Commissioner, who will be empowered to investigate and attempt to resolve complaints concerning breaches of the data protection principles. Under the proposed scheme, if a complaint can

74 NSWLRC, n 2, p. 13.

not be resolved, the complainant will have the right to seek damages for any loss suffered, by bringing a claim before the District Court.[75]

The *Privacy Committee Act 1975* (NSW) established the NSW Privacy Committee, whose function it is to research and investigate complaints of intrusions into privacy, and report on the desirability of legislative changes or administrative action to protect the privacy of individuals. The Committee was responsible for the recent report *Invisible Eyes: report on video surveillance in the workplace* (September 1995), and, together with the New South Wales Police Force and the New South Wales Crime Commission, was one of the major contributors to research by the NSWLRC for their 1997 report on surveillance. The Privacy Committee has no powers of adjudication, other than to name people in an annual report.[76]

4.3 International obligations

Australia's international obligations in respect of individual privacy impact on electronic surveillance. Any legislation passed which deals with any of the principles in the covenants and guidelines to which Australia is a signatory must take into account those principles. The main sources for Australia's international obligations in relation to privacy and electronic surveillance are outlined below.

International Covenant on Civil and Political Rights

Australia became a signatory to the Covenant on 18 December 1972, and ratified it on 13 August 1980. While ratification does not automatically incorporate the Covenant into Australian law, it means that the Australian government recognises the standards contained therein. The NSWLRC stated in its report on surveillance that "the Commission considers that its recommendations should, as far as possible, ne consistent with those standards recognised by the Australian Government".[77] Most relevant to the question of electronic surveillance is Article 17:

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.

---

75 J Shaw, Attorney-General, *Speech to The New Privacy Laws: A Symposium on Preparing Privacy Laws for the 21st Century*, Wednesday 19 February 1997. For a more detailed discussion of data protection and privacy, see V Mullen, 'The Individual's Right to Privacy: Protection of Personal Information in New South Wales', *Briefing Paper No 014/95*, and G Griffith, 'Privacy and Data Protection Law Reform: Some Relevant Issues', *Briefing Paper No 15/96*, published by the Parliamentary Library Research Service.

76 Yarrow, n 54, p. 62.

77 NSWLRC, n 2, pp. 20-21.

In September 1991, Australia ratified the *First Optional Protocol to the International Covenant on Civil and Political Rights*. This Protocol allows Australian complainants who have exhausted all legal recourse in Australia to take to the United Nations Human Rights Committee alleged violations of the rights contained in the ICCPR. As surveillance can violate the privacy of individuals, it is conceivable that the Protocol could be employed to challenge any arbitrary interference with an individual's right to privacy caused by surveillance.[78]

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Information

Australia adopted the 1981 OECD Guidelines in 1984. These Guidelines include basic privacy principles and set out various principles that are intended to guide the collection, storage and use of personal guidelines. These principles include: the collection limitation principle; the data quality principle; the purpose specification principle; the use limitation principle; the security safeguards principle; the openness principle; the individual participation principle and the accountability principle.[79] These principles were taken into account when formulating section 14 of the *Privacy Act 1988* (Cth): Information Privacy Principles.[80]

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[81]

This European Community Directive (No 95/46/EC of 1995) requires privacy laws binding on both the public and private sectors. The Directive is not binding in any way on Australia. However, by threatening to ban the export of personal data to non-European countries without adequate data protection legislation from July 1998, it provides an incentive for such legislation to be introduced.[82] If such legislation was not introduced, the NSWLRC

78 Ibid, p. 21.

79 'OECD Guidelines', http://inter.gov.nb.ca/edt/infohigh/privacy/5-1.htm

80 NSWLRC, n 2, p. 22.

81 For a more thorough discussion of content of the European Directive, see G Griffith, 'Privacy and Data Law Reform: Some Relevant Issues', *Briefing Paper No 15/96*, Part 3.

82 Yarrow, n 54, p. 63. Australia is not the only country who's trade has been put at risk by the European directive. New Zealand, Hong Kong, Taiwan and South Korea had, by March 1997, passed privacy laws bringing them in line with European Community standards. Japan and Canada were also considering such laws. See C Merritt, 'Australia now offside with Europe on privacy laws', *Australian Financial Review*, 27 march 1997.

argues that Australian businesses wishing to trade with European countries would have to set up their own contractual privacy protection systems with their trading partners.[83]

4.4 Guidelines/Codes of Practice

There have been a number of guidelines and codes of practice published relating to the use of electronic surveillance devices. Those most relevant to New South Wales are:

- New South Wales Privacy Committee *Guidelines on Overt Video Surveillance in the Workplace* (September 1995)
- New South Wales Police Service *Guidelines for Investigation of Potential for, and Implantation of, CCTV by Local Councils* (May 1996)
- New South Wales Department of Industrial Relations *Code of Practice for the use of Overt Video Surveillance in the Workplace* (preliminary version, December 1996)
- Commonwealth Privacy Commissioner *Guidelines on Covert Optical Surveillance in Commonwealth Administration* (1992).

The Federal Privacy Commissioner, Ms Moira Scollay, announced in August 1997 a voluntary scheme which would detail privacy protection standards to be met by businesses. It would include a voluntary code, overseen by an independent administrator with powers to act against companies which breach the code.[84] Under the scheme, the administrator would have the power to make companies pay compensation to people affected by the misuse of personal information, including an amount for stress.[85] Another recent development is the *Telecommunications Act 1997* (Cth), assented to in April 1997, which provides for regulating privacy, including surveillance, through a scheme of industry codes and industry standards.[86]

---

83 NSWLRC, n 2, p. 22. In fact, the Federal Attorney-General, Mr Daryl Williams, supported this approach to privacy regulation, calling for "industry to develop a unified set of privacy principles...". See also H van Leeuwen, 'Lack of privacy safeguards won't 'affect EU trade'', *The Australian Financial Review*, 23 May 1997.

84 The regime of Codes of Practices supervised by the Privacy Commissioner and subject to statutory backing was mooted by the Federal Attorney-General in his Discussion Paper on privacy, issued in September 1996, and is consistent with the schemes adopted by New Zealand, Hong Kong, Taiwan and the European Union. See N Scott Despoja, 'Personal and Private', *The Alternative Law Journal*, Vol 22, No 4, August 1997, p. 166.

85 B Lagan, 'Plan for a privacy code with teeth', *The Sydney Morning Herald, 19 August, 1997.*

86 Sections 112-135 (section 113 in particular).

5.0 ARGUMENTS FOR AND AGAINST SURVEILLANCE

It is the view of the NSW Police Royal Commission that, ultimately, the question of surveillance or no surveillance is one of weighing the broader public interests in effective law enforcement, corruption prevention and preservation of the safety of the community against the individual interest in privacy.[87] The New South Wales Privacy Committee acknowledged this tension, expressing concern however, that the interests of law enforcement bodies have tended to receive greater priority than the privacy interests of individuals, leading to a "need to restore the balance and renew the commitment to protecting individual freedoms and rights."[88] The Committee noted further that "the development of technology has greatly favoured those engaging in surveillance to the detriment of those that are its victims."[89] The arguments for and against surveillance are discussed below.

5.1 Arguments for surveillance

The most common justification for, and argument in favour of, surveillance is the role it plays in law enforcement. The Royal Commission found that the use of electronic surveillance was the single most important factor in achieving a breakthrough in its investigations. The ICAC and the AFP both use electronic surveillance regularly, the AFP utilising surveillance most often in major drug importation cases. It is the Royal Commission's judgement that it is essential that the Police Service, the Crime Commission, the Police Integrity Commission and ICAC all be equipped with adequate resources and electronic surveillance capacity. These resources include listening devices, intercepts of telephones and other forms of telecommunications, tracking devices and video surveillance.[90] In support of this position, the Commission identified the following factors to be considered when balancing the conflicting objectives of law enforcement and privacy:

- law-abiding citizens have nothing to fear from surveillance;
- those involved in serious crime have no legitimate claim to plan or engage in their criminal activities in privacy, and
- safeguards can be provided through:
  - a suitable legislative prescription of the circumstances in which video surveillance is allowed;
  - the need for a court approved warrant before targeted individual surveillance extending to conversations is allowed, and

---

87 Royal Commission, n 1, p. 450.

88 Privacy Committee of New South Wales, n 64, p. 1.

89 Ibid.

90 Royal Commission, n 1, p. 449.

- a statutory regime as to the use, storage and destruction of all electronically gathered product, to ensure that it is used only for legitimate purposes of law enforcement, and
- oversight by the State or Federal Ombudsman in accordance with existing arrangements, of compliance with the relevant legislation.[91]

The Royal Commission stated that "the advantages of ... surveillance are so obvious they barely need statement". The Commission is not alone in its assessment of the value of surveillance to law enforcement agencies. The Commission's arguments have been used simply because its Report clearly and succinctly summarises the position taken by many. In March 1994 Jeff Barrett released his report titled *Review of Long Term Cost Effectiveness of Telecommunications Interception*, prepared by the Federal Department of Finance. Although prepared specifically in relation to the federal telecommunication interception regime, the conclusions drawn by that report are valid for other forms of surveillance also. Generally, the Report found that "telecommunications interception is a very effective part of an integrated framework of surveillance, it being both cost effective and generally effective", although "more privacy focussed inspections and greater transparency through notification procedures and additional reporting would further enhance privacy".[92] This view is consistent with those of the Royal Commission and New South Wales Privacy Commission discussed above. Other law enforcement bodies (particularly, in this state, the NSW Police Service and the NSW Crime Commission) also all greatly value the assistance given to them by surveillance.

The private security industry is another strong supporter of the use of electronic surveillance, arguing that it is a very efficient, and is in fact less intrusive to innocent individuals than other forms of policing, such as a large physical presence of security guards.[93] As noted above, the cost of installing and maintaining a security camera is far less than that of employing a round-the-clock security guard. It is further argued that surveillance, particularly overt visual surveillance, acts a deterrent to potential criminals, making them "think twice before committing a crime".[94]

The advantages identified by the Commission are not only in the area of law enforcement, but are also concerned with the reduction of police corruption and the safety of both police and the public. These advantages include:

---

91 Ibid.

92 Legislative Assembly of Queensland Parliamentary Criminal justice Committee, *A review of the Criminal Justice Commission's report on Telecommunications Interception and Criminal Investigation in Queensland*, Report No. 29, 18 May 1995, p. 3.

93 J Hume & J Adams, 'Successful public surveillance: controlling crime without social control', *Security Australia*, March 1996, pp. 20-22.

94 J Adams, 'Privacy: security surveillance versus civil rights', *Security Australia*, May 1996, p. 24.

- obtaining evidence that provides a compelling, incontrovertible and contemporaneous record of criminal activity;
- the removal of an incentive to engage in process corruption;
- the opportunity to effect an arrest while a crime is in the planning stage thereby lessening the risk to lives and property;
- the provision of greater security for money in the possession of undercover operatives;
- the reduction of the possible harm to police, undercover operatives and informants arising out of the opportunity surveillance provides to obtain a forewarning of any planned reprisals and to know in advance the planned movements and activities of the targets;
- the reduction in the need to close personal contact with criminals;
- overall efficiencies in the investigation of corruption offences and other forms of criminality that are covert, sophisticated and difficult to detect by conventional methods, particularly where those involved are aware of policing methods, are conscious of visual surveillance and employ counter-surveillance techniques;
- a higher plea rate in cases which, by reason of unequivocal surveillance product, are indefensible, and do not depend on disputed evidence or civilian eyewitnesses who are untrained as observers and historians of fact, and
- the provision of a record to establish or rebut complaints against police.[95]

In relation to specific forms of surveillance, the Royal Commission believes that tracking devices and video surveillance have particular advantages for law enforcement:

- tracking devices can prevent the theft or loss of drugs, drug buy money and chemicals;
- tracking devices can provide greater personal security in the case of extortion investigations;
- tracking devices may support police in terrorist and siege situations;
- tracking devices are valuable in assisting surveillance;
- video surveillance provides cogent and compelling evidence not otherwise available of clandestine criminal activity;

---

95 Royal Commission, n 1, pp. 448-449.

- video surveillance supplements listening devices by identifying visually the parties to a conversation; (see also NSW Police News, June 1994, p. 24)

- video surveillance records activities involved, for example, in the manufacture, packaging and supply of drugs, which might otherwise be incapable of observation; and

- video surveillance rebuts false allegations of improper conduct by police, and of entrapment.

5.2 Arguments against surveillance

Privacy

The primary argument against surveillance is that it infringes individuals' privacy. "Privacy" has proven notoriously difficult to define. The Federal *Privacy Act 1988* deliberately avoids a definition of "privacy", and instead establishes the information privacy principles which were outlined in Part 4.2 - Statutory Provisions, above. The NSWLRC defined "privacy" in its Report, *Surveillance*, as "involving keeping oneself and one's affairs removed from public view or knowledge even if the information so protected is itself not intrinsically sensitive".[96] Both these approaches illustrate the developments in understanding of what constitutes privacy since American Judge Cooley's famous definition in 1888, simply as the right "to be left alone".[97]

MasterCard International undertook a survey of attitudes of the Australian public to privacy in May and July 1996. The findings were released in a report called *Privacy and Payments*. A summary of the findings follow:

- 41% of Australiana are "very concerned" and 46% are "concerned" about issues of privacy generally;

- 83% of people were concerned about organisations having access to information relating to their everyday banking transactions, 79% about access to information relating to major financial purchases (such as a car), 73% about access to information relating to income and 70% about access to their medical history;

- the biggest perceived threat to privacy came from government agencies having computer access to networks containing personal information (80%). Credit rating agencies presented the next greatest perceived threat (74%), followed by video surveillance (59%);

---

96 NSWLRC, n 2, p. 13.

97 Ibid, pp. 12-13.

- 63% of mail order companies were perceived to be untrustworthy. This compares to 33% of retail stores, 29% of telephone companies and 28 of credit card operators;

- the activity of the greatest concern to people was telephone tapping, with 77% of people being very concerned. 57% were very concerned about different government agencies sharing personal information and 55% were very concerned about different financial agencies sharing personal information;

- 85% of people thought it very important that they be advised as to who had access to data about them. 84% believed it to be very important that they be advised how that data may be used and 72% believed it to be very important that their permission was asked before data about them was stored, and

- 71% of people believed that information stored on a central computer database was unsafe or not at all safe. The safest method of storage was perceived to be a computer not linked to a central database (only 30% believed it to be unsafe or not at all safe).[98]

The privacy argument was summed up by the NSWLRC as this: "in the absence of wrongdoing, many would endorse the view that they have the right to be let alone, and that such a right is infringed by indiscriminate surveillance".[99]

Other arguments against surveillance

Those opposed to surveillance raise other issues apart from the privacy issue. **Trespass** may be involved in the surveillance, for example when entering onto private property in order to install an electronic surveillance device. **Damage** to private property may also occur as a result of installing or retrieving the device. Incidental **theft** is also an issue, for example, the effective theft of electrical power to maintain the device. In some situations, the device may **hamper** the effective operation of the host device, such as a computer system. It is argued that surveillance can also infringe other **private rights**. An example given by the NSWLRC is unauthorised video images of a celebrity wedding which may breach an agreement to provide the exclusive rights to the coverage of the event to a third party.[100]

---

98 MasterCard International, *Privacy and Payments, A study of attitudes of the Australian public to privacy - summary and findings*, 1996, pp. 11- 16.

99 NSWLRC, n 2, p. 33. This point is made in particular reference to street surveillance, but could be applied to any form of unregulated, indiscriminate surveillance. The warrant system that operates for listening devices and telephone interception does, to a large extent, overcome this concern.

100 Ibid, p. 14.

Chris Puplick, chairman of the New South Wales Privacy Committee argues that street video surveillance only operates to **displace** crime, rather than curing or preventing it,[101] so the invasion of an individual's privacy can not be justified on these grounds. It is further argued that this type of surveillance not only monitors illegal behaviour but also "undesirable" behaviour which is distinct from illegal behaviour. This may lead to what is known generally as "function creep", which refers to a surveillance device being used for a purpose other than that for which it was originally installed. An example is the potential use of surveillance to keep certain kinds of people, or people displaying certain kinds of behaviour, out of certain areas.[102] Thus, surveillance can be used as a social control mechanism, targeting behaviour which is legal but undesirable. There is concern over tapes from recorders and cameras and the uses to which the information is being put. Some of these "extra" uses include: marketing or market research; advertising; identifying behavioural trends, commercial entertainment; voyeurism, and blackmail.[103] The NSWLRC characterised this concern in the following manner: "that some act, quite possibly harmless and best forgotten, once captured by the surveillance camera has the potential to become a source of humiliation, even blackmail."[104]

As those in favour of surveillance argue that surveillance can reduce the level of police corruption because dealings between police and criminals are recorded, those opposed to surveillance argue that new technology allows greater scope for police corruption. The New South Wales Privacy Committee in its submission to the NSWLRC argued that, while the majority of police would not abuse electronic surveillance technology, ... "the greater power given to corrupt officers then the greater the potential harm. Any new powers, whether legal powers or access to new technologies, must be carefully scrutinised. Any grant needs to be countered with checks and balances to protect against abuse".[105]

6.0 SUGGESTIONS FOR REFORM

There is a general consensus among those with particular interest in electronic surveillance that regulation must extend to visual and other forms of surveillance, instead of being confined to aural surveillance. It is a matter of opinion exactly what form that regulation will take. There are also calls for amendments to be made to the LDA to make it more applicable to modern technology and changing police procedures. In fact, it would be sensible for a complete overhaul of the relevant legislation be undertaken to answer all the concerns. It is

---

101 In response, the private security industry argues that "criminal displacement theory is the driving force behind police patrols, security officers, fences and alarm systems", and is, in fact, the aim of most types of electronic and physical security. Rather than failing, therefore, displacement is proof of the success and efficiency of surveillance: J Adams, n 94, p. 26.

102 N Waters, 'Street surveillance and privacy', *Privacy Law and Policy Reporter*, vol 3, Number 3, June 1996, p. 50.

103 Ibid, p. 49.

104 NSWLRC, n 2, p. 32.

105 Privacy Committee of New South Wales, n 64, p. 2.

the opinion of the Royal Commission that deficiencies in legislation can have the following results:

- the capacity of law enforcement to deal with serious crime is reduced
- process corruption may be encouraged
- detection and investigation of corruption on the behalf of police and other public officials is hindered.[106]

Visual surveillance

The Royal Commission recommends that the use, for security reasons, of simple visual surveillance devices by owners or occupiers of shops, commercial premises and the workplace be permitted without the need for a warrant. The Commission is of the opinion that no legislation is needed in this area. Similarly, the Commission supports the general use of visual surveillance without the need for a warrant in public places, places open to lawful access by the public or able to be lawfully viewed from a public place.[107] The Commission did not specify that this surveillance must be overt, however, it can be assumed that the use of such simple visual surveillance devices would necessarily be overt.

Additionally, the Royal Commission recommends that a system of judicial warrants be created "providing lawful authority for the use of video devices and entry into premises to permit their use along similar lines to the scheme created by the LD Act".[108] Such a scheme would regulate the use of covert visual surveillance by law enforcement agencies, allowing any evidence gained as a result of its use to be admissible in legal proceedings. The Queensland Parliamentary Criminal Justice Committee also recommends that there be a system of warrants issued by a Supreme Court judge allowing entry onto private property for the purpose of installing a visual surveillance device. However, the Committee further recommends that such a warrant not be necessary if entry onto the property is with the consent of the owners or lawful occupiers of the property.[109]

If such a scheme is to be provided for by legislation, there are two obvious options: 1) create a new Act or 2) amend and add to the existing LDA. Any new Act would no doubt be modelled on an LDA type regime. Alternatively, it has been suggested that the LDA be amended to include:

- a definition of covert video surveillance

---

106 Royal Commission, n 1, p. 449. For the Commission's detailed recommendations of amendments to the LDA, see paragraph 7.99 of the *Final Report*.

107 Royal Commission, n 1, p. 458.

108 Ibid, pp. 457-458.

109 Queensland Parliamentary Criminal Justice Committee, n 8, 92, p. 72.

- a prohibition of certain uses of covert video surveillance
- a system of prior judicial authorisation
- a prohibition on certain uses of resultant video tapes.[110]

Others argue that codes of practice are sufficient, and are in fact preferable to a legislated scheme as a code allows for greater flexibility, and increased capacity to deal with technological developments.[111] A code of practice may be either voluntary or legislated, which allows for prosecution of those who do not comply. The NSWLRC pointed out one major advantage of enforced self-regulation: those who are regulated make the rules themselves using their intimate knowledge of the environment in which they function. These rules are enforceable once they are sanctioned and given power by a Parliament. The NSWLRC suggests that the standards upon which any code of practice is based be contained in legislation. Although the code is designed by its users, accountability would be provided through certain non-negotiable standards and by the oversight of the regulator. Thus the requirements of an appropriate and applicable scheme and independent regulation are satisfied.[112] For a further discussion of existing and proposed codes of practice, see Part 4.4 - Guidelines and Codes of Practice, above.

Tracking devices and other forms of surveillance

The Royal Commission recommended that a system of warrants be created authorising the use and installation of tracking devices similar to the scheme that operates for listening devices. The Queensland Parliamentary Criminal Justice Committee went one step further, recommending a two-tiered system:

1. where the tracking device is of a basic type which emits a signal to assist in locating and tracking a vehicle and is simply attached to the outside of a vehicle on public property, the device may be used upon authorisation in writing from a police officer of the rang of Inspector or higher, without the need for a warrant, and

2. where the installation of the device involves entry into a vehicle or entry onto private property, or where the device is of the type that stores data or has listening device

---

110 The working party on video surveillance in the workplace, *Report to the Hon JW Shaw QC MLC Attorney General and Minister for Industrial Relations*, NSW Department of Industrial Relations, December 1996, pp. 2-5. Note that these recommendations were made specifically in relation to video surveillance in the workplace. They are, however, also applicable to video surveillance generally.

111 The security industry holds this view, although is aware of the problems of a voluntary code, particularly the potential for abuse and lack of recourse if such abuse occurred: see Adams, n 94, p. 34.

112 NSWLRC, n 2, p. 40.

> capacity, a warrant issued by a judge of the Supreme Court is necessary before use.[113]

Obviously, any code of practice system such as that outlined in relation to visual surveillance, above, can also apply to the use of tracking devices and, indeed, any other form of surveillance, providing the general principles are applicable.

7.0 CONCLUSIONS

There is a strong divide between those who support surveillance and those who oppose it, although most can appreciate the benefits surveillance offers for law enforcement agencies. Not surprisingly, the most ardent supporters of surveillance are those who have an interest in law enforcement processes, and those who most strongly oppose surveillance are those whose focus is on individual privacy rights. It is therefore for different reasons that there is a consensus on the need for regulation of visual and other forms of electronic surveillance: whether to control or liberate surveillance. Whether this takes the form of amendments to the LDA or the introduction of additional legislation seems largely irrelevant, as long as any regime regulating surveillance is flexible enough to adapt to technological changes, such as in the area of computer data surveillance and tracking devices which may not fit the typical models of surveillance. The issues surrounding surveillance are intricately related to issues of privacy. Privacy principles as contained in the international covenants have been adopted by the Australian Government and must therefore be kept in mind when making any changes to laws affecting surveillance.

---

113 Queensland Parliamentary Criminal Justice Committee, n 8, 92, p. 75.