

submission

Submission by Privacy NSW
to the Director General, NSW Attorney General's Department
on the

Workplace Video Surveillance Act Review



privacynsw

Issue date: October 2003

Submission made 10 October 2003 in response to invitation to comment from Director General
Attorney General's Department, 8 July 2003

Enquiries: John Gaudin
Tel: (02) 9268 5581
Our ref:A03/296
Your ref:

Mr Laurie Glanfield
Director General
Attorney General's Department
8-12 Chifley Square
SYDNEY NSW 2000

Attn: Piccolo Willoughby

Dear Mr Glanfield

Thank you for providing me with an opportunity to comment on the review of the Workplace Video Surveillance Act 1998 (WVS Act).

Privacy NSW considers that the WVS Act makes an important contribution to the protection of privacy, by imposing a degree of transparency and accountability on the way employees are monitored. At the same time we recognise the need for a more comprehensive unified approach to the regulation of surveillance as proposed in the NSW Law Reform Commission's Interim Report on Surveillance. We are also aware through numerous inquiries of possible deficiencies in the operation of the Act.

Since the commencement of the Act in January 1999, Privacy NSW has received and recorded a large number of inquiries about its operation from employers, employees and security operatives (see attachment 1). We have also provided formal and informal advice on the way the Act operates (see attachment 2). This has included comment on proposals for more comprehensive surveillance legislation as recommended in the NSW Law Reform Commission's Interim Report on Surveillance and advice on the relationship between video surveillance systems and privacy legislation.

Surveillance and Privacy Legislation

Privacy is generally taken to encompass a variety of values, which include:

- Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";
- Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
- Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and

- Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.¹

Within this framework legislation regulating video surveillance can be seen as a means for protecting territorial privacy. Some forms of surveillance result in the accumulation of large amounts of information about individuals. At the same time the very fact of surveillance alters people's behaviour and relations with each other. Setting limits on the intrusive aspects of surveillance technology raises a distinct set of issues from those which relate to protecting information privacy.

Some commentators have suggested that it is not useful to use a concept like privacy to regulate surveillance, which has become an all-pervasive aspect of a technologically oriented society.² The above framework provides an opportunity to assimilate surveillance to privacy in a way that still accords with many people's understanding of privacy, while distinguishing between the approaches required to protect against overly intrusive surveillance and the fair handling of personal information.

The commencement of the Privacy and Personal Information Protection Act 1998 (NSW) in July 2000, and of amendments to the Privacy Act 1988 (Cwth) (Privacy Act) in December 2001 resulting in coverage of the private sector, might be thought to have significantly impacted on the legal climate in which employee video surveillance takes place. This has not in fact been the case. Both pieces of legislation deal with the collection and holding of personal information by delimited classes of organisations. Whether the operation of a video surveillance system by an employer amounts to a collection or holding of personal information will depend on a range of variables, for instance:

- is the employer an agency or organisation covered by relevant information privacy principles;
- does the system operate in such a way as to capture identifiable personal information, for example are images recorded, retained and readily retrievable;
- is the operation subject to a relevant exemption, for example, the employee record exemption under section 7B(3) of the Privacy Act or the exemption relating to investigative functions under section 24 of the PPIP Act?

The answers to these questions will ensure that in any given circumstances there may be significant doubt as to whether video surveillance would be regulated by existing privacy laws. We conclude from this that the extension of privacy legislation has not displaced the need for separate legislation dealing with surveillance.

¹ Privacy International and Electronic Privacy Information Center, *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments*. 2003 Overview.

² eg David Lyons "Surveillance as Social Sorting: Computer Codes and Mobile Bodies", Chapter 1 of D Lyon ed. *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London and New York 2003 page 19.

General Surveillance Legislation

The NSW Law Reform's Commission's Interim Report on Surveillance recommended that legal provisions on workplace video surveillance be incorporated into a general surveillance Act which covers other technical means of surveillance. Privacy NSW has expressed broad support for this approach.³ General surveillance legislation would extend the distinction between overt and covert surveillance to other forms of surveillance such as listening devices, computer monitoring and tracking devices. However, in its recommendations the Law Reform Commission also recognised that the workplace constituted a special case, and that employment specific provisions should apply where surveillance was employment related (recommendation 15)

Until general surveillance legislation is implemented the regulation of workplace video surveillance remains an important issue in its own right. The significant number of complaints and inquiries we continue to receive about video surveillance indicate that the current WVS Act has not entirely resolved the issue for employers and employees.

Definition of video surveillance

The WVS Act defines video surveillance as *surveillance by a closed-circuit television system or other electronic system for visual monitoring of activities on premises or in any other place* (WVS Act section 3). Presumably *other electronic system for visual monitoring* is capable of extending to new forms of technology which are capable of capturing visual imagery and being used for surveillance, for instance webcams, digital cameras in mobile phones, or time lapse camera systems which capture a series of still photographs rather than a video motion stream. However use of the word 'video' could be taken to imply an intention to exclude these newer systems. Any uncertainty as to the scope of the definition could be used to argue that the Act only applies to the kind of closed circuit television systems, which were the standard in 1998.

There is a need to recognise that these new forms of surveillance raise issues that were not as obvious when the WVS Act was originally passed. For example the fact that a webcam or mobile phone camera is operating in a way that amounts to employee surveillance may not be as obvious as an installed video camera. Recent publicity about the use of private mobile phone cameras in change areas and correctional facilities attests to public concern in this area.⁴ Integrated security systems featuring digital storage of images, especially when combined with facial recognition or motion sensing technology, vastly increase the potential to sort and retrieve identifiable personal information.⁵

It would be useful to review the definition of video surveillance to clarify the fact that it applies to all forms of capturing visual images that are likely to occur in a workplace.

³ Privacy NSW *Position Paper NSW Law Reform Commission Report 98 Surveillance: An Interim Report* June 2002 at <http://www.lawlink.nsw.gov.au/pc.nsf/pages/nswlrcresponse>

⁴ see for example Linda Silmalis, *Rivkin pictures prompt phone camera laws*, Sunday Telegraph 15 June 2003

⁵ Christopher Jay, *Integrated network security on the way*, Financial Review 3 October 2003.

A number of inquiries and complaints have raised the issue of surveillance systems that combine visual images with sound recording. While such systems would appear to attract the more stringent provisions of the Listening Devices Act, it would be useful to explicitly qualify the definition of video or visual surveillance to make it clear, in relation to both overt and covert surveillance that this legislation does not authorise the recording of private conversations.

Some confusion arises when systems that are not specifically intended to watch employees have the secondary effect of doing so. An example would be a series of recent proposals to place cameras in childcare centres to allow parents to keep an eye on their children.⁶ Although this can be seen to fall outside the definition of 'video surveillance of an employee by an employer in the workplace' (WVS Act section 4(1)) it could be seen to represent surveillance by proxy and involve a significant intrusion on employee privacy. Another instance is where images from cameras ostensibly installed for security purposes are used to discipline workers. It would be useful to extend the definition of video or visual surveillance to include such incidental uses.

Definition of Workplace

Section 3 defines workplace as premises, or any other place, where persons work, or any part of such premises or place. Section 5(1)(c) requires that notices informing employees that a workplace is under surveillance *are clearly visible at each entrance to that part of the workplace in which surveillance is taking place*. The qualification of the broader definition of workplace by a reference to premises creates some uncertainty as to the way the Act applies to surveillance of workers in public places and vehicles. For example does a vehicle in which an employee may be subject to surveillance require signage? Assuming signage cannot be practically implemented in public places where employees work, is it possible to operate an overt surveillance system there?

It seems logical to require some flexibility in the way the definition of overt surveillance applies to surveillance of employees that takes place outside premises, for example by using the Law Reform Commission's recommendation that there be a requirement for 'adequate notice'. However, until there is general surveillance legislation, I would recommend that 'adequate notice' not replace the current requirements for notice, signage and visibility, which should remain the criteria for defining overt surveillance in premises.

Regulation of overt surveillance

The WVS Act enforces a distinction between overt and covert surveillance but leaves overt video surveillance largely unregulated. Some commentators have questioned whether there is a reasonable basis for treating the privacy issues between these two forms as logically distinct.⁷ Uncontrolled overt surveillance can contribute to stress and a sense of powerlessness. It has the potential to be abused, for example, by

⁶ Sue Lowe, *Mummy's watching and teacher's upset*, Sydney Morning Herald 22 March 2003.

⁷ K Foord, *Defining Privacy*, Victorian Law Reform Commission Occasional Paper 2002, pp 34-36

zooming in on individual employees or subjecting them to an unreasonable level of continuous monitoring. In the absence of privacy protection for employee records there is a capacity for misuse of stored images from video surveillance.

In March 1996 a working party on video surveillance in the workplace convened by the Department of Industrial Relations and representing employers, employees and the NSW Privacy Committee endorsed a *Code of Practice for the use of Overt Video Surveillance in the Workplace* which specified in a non-binding way a series of standards which should apply where overt surveillance systems operate in a manner which is consistent with the WVS Act (attachment 2, appendix 1). In addition to laying down the kind of provisions that the Act subsequently adopted to distinguish overt from covert surveillance, the Code seeks to restrict the hours in which surveillance should operate, retention and access to tapes and to ensure that employees have access to tapes that record their own activities.

Since responsibility for the WVS Act was transferred from the former Department of Industrial Relations to the Attorney General's portfolio, responsibility for this Code has become unclear. Privacy NSW continues to make copies available to people and organisations who have concerns about video surveillance or wish to adopt best practice for its use in the workplace. We also refer to the Code when investigating and seeking to conciliate formal complaints about overt surveillance. The Code can be seen to provide a benchmark in relation to section 6(2)(j) of the Industrial Relations Act 1996 which recognises the surveillance of employees in the workplace as an industrial matter to which that Act applies.

The Law Reform Commission's proposals for general surveillance legislation would make standards applicable to overt surveillance more generally enforceable as part of such legislation and by requiring compliance with a Code of Conduct. Assuming that such legislation will be adopted in the near future, it may be premature to suggest that the current WVS Act should be revised to the extent of incorporating provisions based on the 1996 Code. At the same time it would be appropriate to recognise that there is a level of public concern at the lack of regulation for overt surveillance and use the opportunity provided by this review to resolve the status of the 1996 Code. This might be achieved by having the Code formally endorsed by the Attorney General. Alternatively it could be incorporated by reference into the WVS Act to provide a benchmark for authorised surveillance.

Enforcement

Calls to Privacy NSW suggest that there is widespread non-compliance with the legislative requirements for notification and signage when installing video surveillance in the workplace. A smaller number of formal complaints have been received.

Non-compliance can be partly attributed to lack of knowledge of a comparatively new offence provision. It also goes to the issue of enforcement. There are obstacles for aggrieved employees who are not separately covered by privacy legislation to seek to have the Act enforced. The widespread use of video surveillance systems in other contexts for law enforcement purposes does not predispose law enforcement agencies to prosecute breaches of the WVS Act. Police enforcement of surveillance legislation only appears to take place in cases where the use of video surveillance

equipment in toilets or change rooms involves a sexual element similar to the offence of peeping and prying under section 547C of the Crimes Act, though possibly without the element of location required for that offence.⁸ The effect of this can be to confuse privacy protection with the separate issue of penalising certain forms of sexual conduct.

A lack of compliance or enforcement is not in itself grounds for concluding that the current legislation is ineffective. The existence of legislation can have an important symbolic function that is only indirectly related to the way it is enforced. It can signal where the limits exist between reasonable monitoring and intrusive surveillance. The strategy of the WWSA Act is to enforce a separation between overt and covert surveillance so that the former can be subject to legitimate negotiation between employers and employees and the latter can be subject to more intensive regulation. This object is not necessarily frustrated where conduct is for all practical purposes overt but which falls short of the legal requirements for overt surveillance. There would be more justification for concern if there was widespread evidence of abuses of covert surveillance. While there is a lack of research into the way covert surveillance authorisations have operated, Privacy NSW does not have firm evidence to suggest that information obtained through covert surveillance is widely abused.

Nevertheless it would be appropriate to consider more effective sanctions for breaches of the Act. Rather than taking the form of criminal prosecutions, these could include penalty notices similar to those issued under Chapter 7 Part 6 of the Industrial Relations Act, and a provision similar to section 13 of the Listening Devices Act 1984 which would make evidence obtained in breach of the Act inadmissible. It would also be appropriate for the regulations to give effect to section 21 of the WWS Act by providing that records provided to the Minister be kept in such a way that employees or industrial organisations could establish whether an authority had been issued once the authorised period had expired.

I trust that these matters will assist your review. To discuss any of these issues further, please contact John Gaudin on 9268 5581

Yours sincerely

John Dickie
ACTING PRIVACY COMMISSIONER

⁸ See the conviction of Alan Harper in the Liverpool Magistrates Court on 16 May 2001, and the conviction of ACI Glass Packaging in Penrith Local Court on 12 July 2001

Attachment 1

Employment Visual Surveillance Complaints and inquiries received by Privacy NSW

Phone inquiries to Privacy NSW about Video Surveillance in employment

<i>Year</i>	<i>Total Inquiries</i>
1999-2000	108
2000-1	73
2001-2	95
2002-3	65

Where did calls come from? 2002-2003

<i>Individuals & advocacy groups</i>	<i>43</i>
State and local government	6
Non-government	16
Total	65

Written complaints and advice

	<i>Complaints</i>	<i>Requests for advice</i>
1999	3	6
2000	0	0
2001	1	2
2002	3	3

A Guide to the Workplace Video Surveillance Act 1998 (NSW)

Privacy NSW

February 2002

CONTENTS

The Workplace Video Surveillance Act 1998

Coverage of the Act

- Covert or overt video surveillance?**
- Overt video surveillance - employers' obligations**
- Is the surveillance occurring in a workplace?**
- Is the employer carrying out the surveillance?**

Employers' Obligations

- When can an employer use covert video surveillance in the workplace?**
- What are the obligations on the nominated licensed security operator?**
- How does an employer obtain a covert surveillance authority?**

Employees' Rights

- Can employees ask the magistrate to stop the authority?**
- What happens if an employer unlawfully places employees under video surveillance?**
- Do employees have any other options if they are unhappy about surveillance in their workplace?**

The Role of the Privacy Commissioner

- Where can I get more information, or make a complaint about covert or overt video surveillance?**

Appendix 1 - Overt Surveillance Code The Workplace Video Surveillance Act 1998

The Workplace Video Surveillance Act 1998 attempts to balance the rights of employees and employers in relation to workplace video surveillance. Under the Act employees have their privacy in the workplace protected to some degree while employers are given the right to use video surveillance to prevent theft and other illegal activities occurring on their premises.

This document is intended as a guide only. It is not a substitute for legal advice.

Coverage of the Act

The Act is limited in its application in a number of ways. It applies only to covert video surveillance of employees (not contractors) by an employer within a workplace. The Act is not intended to cover covert surveillance by law enforcement agencies Section 7(2).

The extent of some of these limitations is outlined below.

Covert or overt video surveillance?

The Act is directed at covert video surveillance or surveillance by hidden cameras. However, even cameras that are clearly visible may be considered hidden in a number of cases. The Act applies a three part test to decide whether or not a camera is 'covert'. If any one of the three elements is missing then the cameras are considered to be covert. The three questions to ask are:

- Can the cameras or their housing (eg. black plastic domes) be clearly seen Section 4(1)(b)?
- Are there signs present at every entrance to the workplace informing people that they will be under video surveillance Section 4(1)(c)?
- Have all employees been notified in writing of the purpose and coverage of the video surveillance at least 14 days prior to the installation of the cameras Section 4(1)(a)?

If the answer to all of the above questions is "yes" then the video surveillance is not affected by the Act. The surveillance is considered to be 'overt' and should be conducted in accordance with the Department of Industrial Relations' *Code of Practice for the use of Overt Video Surveillance in the Workplace* (see Appendix 1).

However if any one of the three questions on page 1 is answered with a "no" then the Act probably applies, and a covert surveillance permit is necessary. However see s.4(2), which allows an exception to this rule; video surveillance will not be considered 'covert' if the surveillance is used for a purpose other than the surveillance of employees, and the employees have agreed to such a use. For example, staff may agree to the use of security cameras to protect staff or premises.

Overt video surveillance - employers' obligations

As noted above, overt video surveillance should be conducted in accordance with the Department of Industrial Relations' *Code of Practice for the use of Overt Video Surveillance in the Workplace* (see Appendix 1).

The broad definition of covert surveillance means that any employer who uses video cameras on a day to day basis in a workplace will need to ensure that signs are placed at every entrance to the workplace and that all employees are notified in writing about the surveillance. Employers will also need to ensure that all cameras are clearly visible. Failure to do these things can be a breach of the Act and expose an employer to a criminal charge.

Is the surveillance occurring in a workplace?

The Act defines workplace as "premises, or any other place, where persons work, or any part of such premises or place" Section 3. This clearly covers many places that would not normally be thought of as a workplace, for example shops (shop employees), public streets (council employees such as street cleaners), inside many vehicles (eg delivery drivers, taxis, couriers, bus drivers and inspectors), and outside buildings (security guards and maintenance personnel).

In other words most places where an employer places a camera will probably be a workplace for at least some employees and so all employers should be aware of the requirements of the Act.

Is the employer carrying out the surveillance?

The Act covers cases where the employer actually carries out the surveillance and also cases where the employer "causes" covert surveillance to be carried out in the workplace Section 7(1). This would clearly cover cases where an employer carried out the surveillance or paid a

person to carry out the surveillance. It is not so clear whether the Act would cover cases where an employer merely allowed a third party, such as the media, to film an employee covertly.

However, given that the Act is designed to prevent covert surveillance of employees except in a limited number of clearly defined situations, it is possible that allowing a third party to film will be seen as causing the surveillance to take place. Employers should be aware of section 33 of the Interpretation Act 1987 which directs courts to interpret ambiguous sections in a way that is consistent with the purposes of the Act. In this case the purpose of the Act is to prevent unauthorised covert surveillance in the workplace..

Employers' Obligations

When can an employer use covert video surveillance in the workplace?

If an employer wishes to use covert video surveillance there are a number of requirements that must be observed:

- it must be used only to detect whether an employee is engaged in an unlawful activity in the workplace Section 7(1)(a). It is not allowed to be used to check whether an employee is present or is doing his or her job properly, or for other monitoring purposes;
- the employer must obtain a covert surveillance authority from a Magistrate approving the covert surveillance Section 7(1)(b);
- the surveillance must be carried out in accordance with the terms of the covert surveillance authority Section 18;
- the surveillance must not continue for more than 30 days Section 16;
- the covert surveillance must not take place in a change room, toilet, shower or bathing facility Section 9(3)(b); and
- the surveillance must be overseen by a nominated licensed security operator Section 9(2)(a). Licensed security operator is defined at s.3 to be "a person holding a Class 1 licence issued under the Security (Protection) Industry Act 1985 or a licence of a corresponding kind issued under any Act that replaces that Act". The Security (Protection) Industry Act 1985 has since been replaced by the Security Industry Act 1997. Under s.11(1) of that Act, a Class 1A licence authorises the licensee to "patrol, guard, watch or protect property ... ". The requirements for obtaining and operating under such a licence are set out in that Act; for example, holders of Class 1A licences must be employed by a person holding a 'master licence' issued under that Act. .

Employers are strongly advised to contract a licensed security operator to set up and conduct any covert video surveillance.

After the covert surveillance has taken place employers have a number of further obligations:

- the employer must not use the recording for an irrelevant purpose (that is one unrelated to legal action, disciplinary action or amending security procedures as a result of the illegal activity) Section 8;
- the employer must ensure that any recordings within his or her control are protected against loss, unauthorised access or use. (One precaution that could be taken is for an employer to erase all recordings as soon as they cease to be of use in relation to disciplinary or legal action);
- the employer also has a duty to report back in writing to the Magistrate issuing the authority, within 30 days of its expiry, the results of the surveillance Section 23; and
- if the employer proposes to take any detrimental action against an employee as a result of the covert surveillance, then that employer should provide the employee or the employee's lawyer with reasonable access to the recording Section 17(1)(d).

What are the obligations on the nominated licensed security operator?

Apart from placing obligations on the employer, the Act and Regulation also place a number of obligations on the nominated licensed security operator. These can be summarised as follows:

- the security operator can supply to the employer only those parts of the tape that are relevant in proving that the employee was engaged in an illegal activity Section 17(1)(b);
- the operator is not allowed to give the tapes to any other person Section 17(1)(a);
- the security operator must ensure that any recordings within his or her control are protected against loss, unauthorised access or use Section ; and
- the operator must erase or destroy, within 3 months, all parts of the tape that are not required for evidentiary purposes Section 17(1)(c).

How does an employer obtain a covert surveillance authority?

When an employer wishes to obtain a covert surveillance authority, either they or their nominated security operator needs to complete Form 1 (found in the Workplace Video Surveillance Regulation 1999) and apply to a Magistrate.

The form needs to address several matters, including:

- why the employer believes that one or more employees are engaged in an illegal activity within the workplace Section 10(2)(a);
- other managerial or investigative techniques that have been tried to detect the activity Section 10(2)(b);
- who and what will be seen by the cameras Section 10(2)(c);
- when the surveillance is planned to take place Section 10(2)(d); and
- the names of the licensed security operatives who will oversee the surveillance Section 10(3).

If the application to the Magistrate is made by the nominated security operative then that person will also need to provide evidence that the employer has authorised them to undertake the surveillance Section 10(2)(e).

In all cases the evidence supporting the application will need to be given to the Magistrate under oath or affirmation or in the form of an affidavit Section 10(4). Providing misleading or false information in relation to an application can lead to a serious penalty being imposed Section 11.

The Magistrate must then weigh up the evidence provided by the employer against the privacy expectations of employees and other people who may be filmed Section 14 and reach a decision whether to issue the authority or not. Employers have a right to appeal the decision Section 25 and have it reviewed by a judicial member of the Industrial Relations Commission.

Employees' Rights

Can employees ask the Magistrate to stop the authority?

Yes. But most employees will not know that the authority has been asked for or granted. If they do find out and want it stopped, they must apply to the Magistrate within 30 days of the authority being issued although there is provision for this time to be extended if applicable.

What happens if an employer unlawfully places employees under video surveillance?

If an employer covertly films employees without a covert surveillance permit Section 7, or if the employer or nominated licensed security operator breach the terms of the covert surveillance authority Section 18, then they may be committing a criminal offence. If employees believe this to be the case then they should contact the Police.

Do employees have any other options if they are unhappy about surveillance in their workplace?

Section 6(2)(j) of the Industrial Relations Act 1996 makes any surveillance of employees an industrial issue under that Act. As such employees may want to seek the intervention of their Union in disputes about workplace surveillance. The Industrial Relations Commission of NSW is empowered to make determinations in this area if necessary. Concerns about workplace surveillance can also be raised with the Privacy Commissioner of NSW.

The Role of the Privacy Commissioner

Privacy NSW is the office of the NSW Privacy Commissioner. Privacy NSW was established in 1999 when parts of the *Privacy and Personal Information Protection Act 1998* came into effect. The role of Privacy NSW is to educate people about privacy issues and ensure that the people of NSW have their privacy rights respected.

Privacy NSW also has the power to receive, investigate and conciliate complaints about privacy related matters. However the Privacy Commissioner has no power to make binding orders on any party.

Where can I get more information, or make a complaint about covert or overt video surveillance?

If you wish to obtain further advice on the Act or if you wish to make a complaint about any workplace surveillance issue then you should contact Privacy NSW.

Phone: **(02) 9268 5588**

Fax: **(02) 9268 5501**

Mail: **PO Box A2122
Sydney South NSW 1235**

e-mail **privacy_nsw@agd.nsw.gov.au**

(Please note that Privacy NSW does not receive complaints by e-mail)

The Privacy Commissioner also has a website that contains useful information about privacy, this can be accessed at:

www.lawlink.nsw.gov.au/pc

Appendix 1 - Overt Surveillance Code
NSW Department of Industrial Relations
Code of Practice for the use of Overt Video Surveillance in the Workplace

This Code establishes principles and standards of behaviour for employers and employees in New South Wales about the use of non-covert video surveillance cameras in the workplace.

The Code was considered by the Working Party on Video Surveillance in the Workplace which was established in March 1996 by the Attorney General and Minister for Industrial Relations, The Hon. J.W. Shaw AC MLC. The following members of the Working Party adopted this Code : The Labour Council of NSW; The Australian Liquor, Hospitality & Miscellaneous Workers Union; Miscellaneous Workers Division; The Australian Chamber of Manufactures - NSW Branch; the Retail Traders Association of NSW; The Australian Liquor, Hospitality & Miscellaneous Workers Union - Liquor and Hospitality Division; the Registered Clubs Association of NSW and the National Union of Workers.

What is overt video surveillance?

The use of video cameras in the workplace should be regarded as overt video surveillance if :

- a) employees have been notified in writing at a reasonable period of time before the video cameras are used;
- b) the video cameras are clearly visible to a person in the area which is under surveillance; and
- c) there are signs which are visible to both employees and visitors such as customers, which notify those persons that they may be under surveillance in an area.

Overt video surveillance should not be used in certain areas

Overt video cameras should not be installed or used in toilets, showers, change rooms or locker rooms which are located within a workplace.

Employees should be notified before the use of overt video surveillance

At a reasonable period of time before the use of overt surveillance, notice should be given to employees in the following ways:

- a) written notices, together with at least one copy of this Code, should be displayed in conspicuous places within the workplace where notice to employees are customarily posted, and
- b) written notices should be given to each individual employees working in the area intended to be under surveillance

This prior notice to employees should contain the following information:

- a) the area(s) in which the surveillance is to be conducted;
- b) the specific purpose(s) for the surveillance; and
- c) the person(s) or designated position(s) within the organisation who is/are responsible for the conduct of the surveillance.

Employers should consult their employees before installing and using overt video surveillance equipment

Employers should consult with employees and/or their representatives if they are planning to install video surveillance equipment. This consultative process should give individual employees the opportunity to comment on :

- a) the purposes(s) for the installation of surveillance equipment;
- b) the nature and capacities of the equipment being installed;
- c) the hours in which cameras will be operated (this requirement is only necessary if the purpose of the surveillance is to protect employee safety and security or otherwise to redress occupational health and safety risks);
- d) the circumstances in which the video tape recordings will be used;
- e) the mechanisms for ongoing consultation regarding the use of video surveillance equipment; and
- f) how any disputes arising from the use of video surveillance will be settled.

All employees who are affected by overt video surveillance should be provided with a written statement of employer policies, procedures, and purposes of the surveillance. They should also be made aware of and given access to a copy of this Code.

Signs should be displayed

Conspicuous signs should be displayed while an overt video surveillance operation is being conducted. These signs should inform employees and members of the public that:

"This area is under video surveillance".

This information should be in a language(s) which all employees can understand having regard to the composition of the workforce.

The location and hours of use of surveillance cameras should be restricted

Video cameras should only be installed in areas and be operated during the hours which have been the subject of prior consultation in accordance with this Code (see section 4 above).

Overt video surveillance should be used in an ethical manner

Surveillance cameras should be operated ethically. Cameras should not be used to zoom in on individuals or pry on a person's activities without cause. Employers should take responsibility to ensure that appropriate disciplinary action is taken if camera operators are found to be conducting surveillance in an inappropriate or unethical manner.

Access to video tapes should be restricted

Access to video tapes by persons other than those whose actions are recorded on those tapes should be restricted to individuals who are nominated personnel on the security staff and/or individuals in senior management. These individuals should only use the tapes for the original purpose of the surveillance operation. Instances of access to the tapes by persons other than the nominated individuals, including the purpose of such access, should be documented. Individual employees should be entitled to access tapes which record their actions in the workplace.

The retention of tapes should be restricted

Tapes may be kept for a reasonable predetermined time, for example seven days, after which time they should be erased or destroyed. The reasonable predetermined time may be extended subject to consultation with employees.

External access to tapes should be restricted

Parties external to the workplace should not have access to tape recordings unless that access is authorised by law, by this Code, or is necessary for the purposes of legal proceedings. The employer's or employees' agents for the purposes of the conduct of video surveillance are exempt from this provision.

Employees should have a right to view tapes

If an incident is viewed and as a result, an employee is the subject of a warning, or any form of disciplinary proceedings (including legal action), a videotape of the incident or incidents should be made available to the employee or the employee's representative within fourteen days of the warning, commencement of disciplinary proceedings, or legal action.