NSW GOVERNMENT | Justice

NSW Government policy statement and guidelines for the establishment and implementation of closed circuit television (CCTV) in public places

A NSW Government Initiative

Any enquiries can be directed to:

Justice Strategy and Policy Division
Crime Prevention Programs Branch
NSW Department of Justice
Parramatta Justice Precinct Offices
Level 5, 160 Marsden Street
PARRAMATTA NSW 2150

Tel: (02) 8688 3277
Fax: (02) 8688 9627

The Guidelines are also available on the Internet at www.justice.nsw.gov.au

ISBN 0 7347 6702 1

Table of contents

Introduction

In 2000 an interdepartmental committee[1] developed Guidelines to establish protocols around the installation and use of CCTV in public spaces. A review of these Guidelines was prompted as a result of the case *SF v Shoalhaven City Council [2013] NSWADT 94.* The then Department of Attorney General and Justice established the CCTV Guidelines Review Group with representatives from NSW Police Force, NSW Information and Privacy Commission, Transport for NSW, Division of Local Government, Local Government NSW, City of Sydney Council, Fairfield City Council, Sutherland Shire Council, Sydney Olympic Park Authority, and Sydney Harbour Foreshore Authority.

The revised guidelines have been developed by the NSW Government to provide a policy framework and a set of underlying principles to assist agencies considering CCTV as a possible response to local community safety concerns. These Guidelines provide:

- A clear statement of the NSW Government's policy on the appropriate establishment and use of CCTV schemes.
- A set of nine principles underpinning the policy that sets out the values and conditions that should apply to the operation of CCTV schemes. These principles have been adapted from the paper *The Police and Public Area CCTV: Issues, Principles, Policy and Practice* prepared by the NSW Police Service on behalf of the Police Commissioners' Policy Advisory Group (PCPAG) and endorsed by the National Police Commissioners' Conference in 1999.
- Steps that local councils, transport authorities and other organisations should take when considering establishing and implementing a CCTV scheme.
- Issues relating to privacy and liability that need to be considered.
- A list of other sources of information or assistance that can supplement the Guidelines.
- Information on Codes of Practice, Protocols and Standard Operating Procedures that should apply to operating schemes.

[1] The 2000 Guidelines were prepared on behalf of the Premier's Council on Crime Prevention. The committee had representation from the then Departments of Local Government, Transport, Urban Affairs and Planning, NSW Attorney General, the NSW Police Service and Ministry and participation in an observer capacity of the NSW Law Reform Commission and Privacy NSW.

The Guidelines acknowledge that the application of CCTV in different settings may vary according to the particular circumstances applying to that setting. However, agencies introducing CCTV schemes should comply with the basic principles and legislation outlined below, or demonstrate clearly and openly their reasons for non-compliance.

These Guidelines are relevant to:

- Local councils as the most typical owners of CCTV schemes in public places. Local councils are democratically organised, are close and accountable to local communities, and generally have the capacity to coordinate local activities in crime prevention and the promotion of community safety. It must be recognised that ownership brings with it accountability, responsibility for securing funding, responsibility to consult with and inform the community as interested parties, and responsibility for design, management, running costs, evaluation and audit activities.
- Transport authorities, given that the definition of public places that is adopted includes railway stations, trains, buses, taxis, transport interchanges and transport-related car parks, public and Crown land. While several sections of the Guidelines, which apply to local councils, will not be as relevant to other authorities, the policy and principles underpinning the Guidelines can be used to inform program implementation in all settings.
- Private organisations that operate, or are considering operating, CCTV schemes in privately-owned spaces with high public usage, such as shopping malls or cinema complexes, entertainment precincts and those public spaces that are not included in the definition adopted, such as university and college campuses.
- Other public authorities, particularly those responsible for the management of public land.

Policy statement

CCTV can be effective in reducing crime if it is part of a broader crime prevention and community safety strategy. CCTV is not recommended as an isolated response to addressing crime in public places.

CCTV can bring benefits to the community through a reduction in crime, which can lead to enhanced perceptions of safety in a particular area. CCTV programs that have the greatest impact on crime in a local area are those implemented as one part of a suite of crime prevention measures as opposed to as a stand-alone crime prevention intervention.

When implementing CCTV, consideration should be given to the impact on the community, particularly in terms of resource allocation and implications for privacy. On this basis, it is recommended that the local community be consulted prior to the introduction of any proposed CCTV scheme in order to ascertain the level of support for the proposal. CCTV schemes should always be operated with respect for people's privacy and their right to conduct or engage in lawful activities.

The NSW Government encourages all agencies considering the development of CCTV schemes to use as a basis the NSW Government Policy Statement and Guidelines for the Establishment and Implementation of Closed Circuit Television (CCTV) in Public Places as well as to seek independent legal advice where appropriate.

Guiding principles

The nine principles outlined below address issues relating to privacy, fairness, public confidence and support, managerial efficiency and effectiveness, and Police involvement in public area CCTV. All of the principles represent the common elements that should constitute public policy on public area CCTV schemes.

1. Integrated approaches to crime prevention

Principle: The implementation of CCTV should be part of an integrated, multi-agency approach to crime control and community safety.

2. Scheme ownership and its responsibilities

Principle: The ownership of public area CCTV schemes must be clear and publicly known.

3. Community consultation

Principle: When considering establishing or significantly expanding a public area CCTV scheme, it is recommended that the relevant concerns of all parties affected are taken into account through an effective community consultation process.

4. Setting clear objectives

Principle: Clear scheme objectives should be set to guide the design, implementation, management and outcomes of public area CCTV. A clear statement of objectives will provide a basis for effective monitoring and evaluation of the scheme, and help to ensure that the use of CCTV is consistent with overall community safety objectives.

5. Police involvement in public area CCTV schemes

Principle: NSW Police Force should be consulted during the assessment and planning phase, including risk analysis and evaluation. The Standard Operating Procedures for the scheme should incorporate protocols covering communication and liaison between the scheme operators and the police.

6. Managing and operating CCTV schemes

Principle: CCTV schemes should be open and accountable and operate with due regard for the privacy and civil rights of individuals and the community. Continuing community support for the operation of CCTV schemes will be influenced by the confidence people have that the scheme is providing the anticipated benefits. It is therefore recommended that:

- the recording and retention of images is undertaken fairly and lawfully;
- the purpose for which the information is being obtained is known;
- the information is not used for any purpose other than that proclaimed;
- people are made aware that they may be subject to CCTV surveillance;
- the CCTV surveillance is not used for general intelligence gathering; and
- the owners of the scheme are known and accountable for its operation.

7. Evaluation

Principle: Effective evaluation of schemes is essential in order to identify whether their formal objectives are being achieved. Evaluation frameworks should be developed at the planning stage of the scheme.

8. Complaints

Principle: Publicly accountable, impartial and fair schemes should have procedures for dealing with complaints.

9. Monitoring and auditing

Principle: Audit is recommended in order to provide an account of the operation of a scheme, by testing its compliance against relevant policy, legislation and procedures, and to be used as the basis of recommendations for improved practice.

Guidelines for the establishment and implementation of CCTV in public places

The information that follows outlines steps to be taken when considering the implementation of public area CCTV as part of an integrated crime prevention strategy.

1. Issues to be considered prior to establishing a CCTV scheme

The issue of whether or not to implement a CCTV scheme is likely to arise in response to a perception or awareness that there is a crime problem in a particular public place. CCTV should not be implemented as a 'default' community safety initiative – it is important to establish the extent and nature of the problem:

- Is the problem on-going or the result of one-off public events?
- Is the perception supported by evidence and data?

A night of street disturbance following an annual sporting event, for example, is unlikely to signify a continuing community safety problem requiring the expense of installing a CCTV system. Similarly, the perception of a crime or community problem may not be supported by crime statistics. Therefore, the costs of installing a CCTV system where an actual problem is not evident will outweigh any benefits expected of the system.

The installation of CCTV should follow the completion of a comprehensive safety and security audit and should only be considered as one part of a range of crime prevention measures.

A further issue for consideration by public sector agencies is the lawfulness of the collection of personal information via CCTV.

The questions that need to be asked by prospective CCTV scheme owners include:

- Is there an evidence base for the problem?
- Is the problem on-going or the result of specific public events?
- Has a comprehensive safety and security audit been undertaken?
- Does the installation of CCTV fit within a broader crime prevention strategy? If so, how?
- Are the Police supportive of the proposal?
- Is the collection lawful?

2. *Privacy and Personal Information Protection Act 1998* and *Workplace Surveillance Act 2005*

The *Privacy and Personal Information Protection Act 1998* was passed on 25 November 1998. The Act covers local governments and other public authorities as public sector agencies, and should be taken into account when considering the establishment, implementation and operation of CCTV. The requirements under the Act have implications for local council use of CCTV.

The Act defines personal information as 'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'. This definition includes the video record made by public sector agencies, as people filmed would in many cases be people whose identity is apparent or could be reasonably ascertained, e.g. people who live and/or work in the area and who are filmed on a regular basis.

Part 2 of the Act identifies 12 information protection principles with which public sector agencies collecting information must comply. Full details are provided at Appendix 1.

Of particular note is the requirement under section 8 which stipulates that the information is collected for a lawful purpose, directly related to a function or activity of that agency. This provides a legislative requirement that a local council formally consider the necessity for CCTV before installing it. A local council should be able to demonstrate that filming all people in a certain area is reasonably necessary to improve community safety and that improving community safety is a key function of the local council.

There are a number of exemptions from the privacy principles in the *Privacy and Personal Information Protection Act* that are relevant to councils who operate and install CCTV cameras in public places. In particular, the *Privacy and Personal Information Protection Regulation 2005* exempts councils from section 11 of the *PPIP Act* with respect to the collection of personal information utilising CCTV cameras installed for the purposes of filming a public place. The Regulation also permits footage to be transmitted live to the NSW Police Force, which would allow, for example, for the installation of CCTV monitors in local police stations. Councils should also be aware of the exceptions relating to disclosure of information. For example, the restrictions on disclosure of personal information in section 18 of the *PPIP Act* do not apply if the disclosure is made:

- in connection with proceedings for an offence;
- for law enforcement purposes;

- to a law enforcement agency for the purposes of ascertaining the whereabouts of an individual who has been reported missing; or
- where a subpoena or warrant authorises or requires the disclosure, or the council believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of a person.

Section 18 of the Act also allows disclosure of personal information collected by an agency in certain other circumstances as well, including if that disclosure:

- is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or the individual concerned is reasonably likely to have been aware, or
- has been made in accordance with section 10, where information of that kind is usually disclosed to that other person or body.

However, given the uncertainties about whether a person is reasonably likely to have been aware about information usually being disclosed in a particular manner, or in establishing whether a person would not object to a disclosure, it may be more difficult for councils to rely on these later exceptions. If a council has any doubt about its ability to disclose CCTV footage under these or any other exemptions in the *PPIP Act*, they should seek legal advice.

Local councils need to be aware of the potential consequences of breaching the *Privacy and Personal Information Protection Act 1998* should an exemption be used incorrectly.

Councils must also be aware of their obligations to protect the privacy of others when releasing personal information to individuals under section 14 of the *PPIP Act* or as part of a GIPA request. In these situations, it is strongly recommended that councils seek independent legal advice or contact the Information and Privacy Commission in order to ascertain their obligations.

There will also be many cases where local council employees e.g. street cleaners, garbage collectors etc., will be filmed by the CCTV system in a ‘place’ where they work. In such cases, the *Workplace Surveillance Act 2005* will apply. Section 10 of the *Workplace Surveillance Act 2005* states that:

“(1) Surveillance of an employee must not commence without prior notice in writing to the employee. **Note:** Subsection (6) provides for an exception to the notice requirement.

(2) The notice must be given at least 14 days before the surveillance commences. An employee may agree to a lesser period of notice.

(3) If surveillance of employees at work for an employer has already commenced when an employee is first employed, or is due to commence less than 14 days after an employee is first employed, the notice to that employee must be given before the employee starts work.

(4) The notice must indicate:

(a) the kind of surveillance to be carried out (camera, computer or tracking), and

(b) how the surveillance will be carried out, and

(c) when the surveillance will start, and

(d) whether the surveillance will be continuous or intermittent, and

(e) whether the surveillance will be for a specified limited period or ongoing.

(5) Notice by email constitutes notice in writing for the purposes of this section.

(6) Notice to an employee is not required under this section in the case of camera surveillance at a workplace of the employer that is not a usual workplace of the employee."

Councils must therefore ensure that they satisfy the requirements of all sections of the *Workplace Surveillance Act 2005* in relation to these employees.

Local governments and other public authorities should be aware of and consider the *Surveillance Devices Act 2007*, particularly if they are considering installing cameras on privately owned land or using cameras that have audio recording capabilities. In particular, the Act makes it an offence to install and operate an "optical surveillance device", which would include a CCTV camera, onto or into premises without the permission of the owner or occupier. Additionally, the Act generally prohibits the recording of private conversations without consent, even where the conversation occurs in public. As such, councils and other public authorities should always seek legal advice if considering installing CCTV cameras with audio recording capabilities.

3. Setting objectives for the CCTV program

Public area CCTV schemes can be used for a range of purposes. The intended purpose of any scheme should be clearly identified prior to establishing the scheme, as this will shape the model of implementation. Schemes should only be used in accordance with their established objectives and not for any other purposes. Clear objectives will also assist authorities by establishing outcome measures, which form the basis for monitoring and evaluation.

Setting the objectives of the scheme should be determined from a full analysis of the problems to be addressed, community concerns and available resources. Along with the precise objectives of the scheme, performance indicators and the processes by which it will be evaluated should be built into planning at the earliest stage possible. It will be important for goals to be set which are reasonable and achievable.

The decision to implement CCTV in a public area should be based on the considered potential of the CCTV program to realise some or all of the following objectives:

- to aid Police in the identification and apprehension of offenders
- to improve the public's general feeling of safety and security in regard to the area being monitored
- to provide accurate identification of offenders and events.

4. Community consultation

Community consultation can help to ensure schemes are designed to meet local needs. It can also facilitate strong and continuing public support, if and when, a scheme is implemented. Publicity and high quality information provide an opportunity for the community to voice any concerns which may be held about the proposed scheme.

It is recommended that local councils and other agencies undertake a thorough community consultation process prior to the purchase or installation of any CCTV related infrastructure.

Initial consultation should occur when the community is informed of the intention to investigate the use of CCTV for a nominated area. All groups likely to be affected by the proposal for CCTV should be consulted. This will include:

- residents
- users of the area
- local businesses.

While the objective behind installing CCTV is to benefit the community, there should be full disclosure of the possible costs involved, including: paying for the scheme through additional charges or rates and a potential loss of privacy. The willingness of the community to bear these costs in order to reap any potential benefit of the program should be considered.

The community should also be informed about their rights and the responsibilities of the agency proposing to install CCTV in relation to the *Privacy and Personal Information Protection Act 1998.* Of particular relevance is Section 10 of the Act which outlines obligations for public authorities regarding the provision of information to the public about the collection of personal information. Section 10 of the Act states that:

"If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:

(a) the fact that the information is being collected

(b) the purposes for which the information is being collected

(c) the intended recipients of the information

(d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided

(e) the existence of any right of access to, and correction of, the information

(f) the name and address of the agency that is collecting the information and the agency that is to hold the information."

Where consensus is reached and there is community endorsement of the CCTV program, additional consultation could be undertaken regarding operational aspects of the proposal. This might include information about:

- The proposed area to be monitored.
- The current incidence of crime.
- Community concerns.
- The objectives of the program (it is important that the community be provided with a realistic appraisal of what the program might achieve, i.e. what types of offences/behaviours are/are not likely to be deterred. CCTV should not be promoted as a panacea for crime).
- The planned duration of the program, including the period after which it will be evaluated.
- The proposed communication method between the scheme operators and Police.
- The cost and funding arrangements of the program. This includes both the installation and the ongoing costs of operating the system.

- Any environmental alterations required for the functioning of the program (i.e. removal or alterations to trees, vegetation or structures).
- The avenue through which complaints about the operation of the program may be lodged.

Local councils should include information about the proposed scheme along with an outline of how they propose to meet their responsibilities under the *PPIP Act* in their Privacy Management Plans. Consideration should also be given to appointing a Privacy Contact Officer to handle any issues relating to breaches of privacy generally, including those that may arise from the installation of a CCTV system.

Section 11 of the *Privacy and Personal Information Protection Act 1998* requires that the collection of information does not intrude to an unreasonable extent on the personal affairs of an individual. For this reason, all efforts should be taken to avoid including private property within the camera view of the monitored area. However, this may be difficult in all instances, e.g. when residences are located above commercial premises in the areas to be monitored. In such cases, local councils should write to residents involved, give them the opportunity to voice concerns, and then act on those concerns, or provide information to residents about why their concerns cannot be addressed. Currently, the *Privacy and Personal Information Protection Regulation* provides an exemption for councils in relation to section 11 of the Act as long as their CCTV cameras are positioned so that no other land is filmed (unless it is not reasonably practicable to avoid filming the other land when filming the public space). However, this exemption only applies to councils and any other authority or agency must still comply with the requirement that collection does not intrude to an unreasonable extent on the personal affairs of an individual.

Anyone who, without lawful excuse or consent, affects a person's amenity in his or her property is likely to be legally liable in nuisance. In the case of *Raciti v Hughes* (unreported, Supreme Court of NSW Equity Division, No. 3667 of 1995), the Court found that it may be a nuisance at common law to continuously film a property. In this case, the complainant was granted an injunction to have the camera moved. Nuisance attaches to any right in property and would presumably cover a lease.

5. Roles and responsibilities of key agencies

In developing a CCTV strategy, it is recommended that a Code of Practice and associated Protocols are established which define the nature and level of involvement of each agency in the management and operation of the scheme. The discrete roles and responsibilities of owner/managers and the Police must be made explicit.

6. Options for police access to CCTV monitoring equipment

CCTV is primarily used for the detection, apprehension and conviction of offenders and is therefore most effective after the fact, with recorded footage being provided to the relevant Local Area Command (LAC) to aid in their investigations.

However, it is essential that there should not be any inappropriate sharing or exchange of information (under section 62(1) of the *Privacy and Personal Information Protection Act 1998,* it is an offence to informally exchange personal information collected in an official capacity). Strict procedures should therefore be established to ensure that this is enforced.

Police involvement in the operational aspects of any CCTV strategy must be discussed with the relevant Local Area Commander or their delegate. Where it is requested, it is possible for direct telephone facilities and monitoring equipment to be provided at a nominated location in the local police station, to ensure instant communication and monitoring of identified events. In this scenario, control of the monitoring equipment resides with the local council's monitor operator, even though Police are able to access images as required. Police would not be required to monitor the equipment on an ongoing basis.

Some systems are designed to allow the Control Centre operator to transfer operational control of the monitor to Police. Such transfer of control should only occur in clearly defined and emergency situations. Clear instructions regarding the circumstances under which transfer of control should occur, and procedures for the transfer of control, should be included in Protocols and Standard Operating Procedures.

An additional possibility is for monitor operators to report identified incidents to local Police via normal telephone facilities.

The most appropriate option will depend on local circumstances, the parameters of the scheme and negotiations between the scheme owners and Police. The option chosen by Police will require endorsement by the owner and the relevant NSW Police Force Region Commander.

In each option outlined, when operators identify an incident on screen they report the incident to the arranged Police contact. These Police Officers then assess what level of Police response is required to the incident and organise the response accordingly.

7. Install and/or trial a CCTV system

Implementing a CCTV program involves a substantial outlay of resources and local councils may wish to consider leasing CCTV services rather than making a capital investment in their installation.

A trial period for the scheme will allow any problems to be identified early and corrected. It will also allow initial assessment of the effectiveness of the scheme and whether or not it is meeting its objectives, whether objectives are realistic and whether any adjustments to the scheme need to be made, or indeed, whether the scheme should continue at all. The scheme should be monitored carefully and its implementation reviewed throughout this period. This review process should be undertaken in conjunction with any Community Safety Committee and/or CCTV Committee, and the NSW Police Force.

If the scheme is to be maintained, monitoring should continue with set review times built into the ongoing scheme.

8. Location of cameras

Effective location of cameras will be critical to the success of the program. Camera location should also be guided by the specific objectives of the program and purpose of the CCTV system. It is suggested that selection of camera locations should be made in consultation with key stakeholders including local Police.

9. Liability issues

Local councils should be aware of the potential for increased liability, which may be incurred when considering the installation of CCTV. By taking on the responsibility of ensuring public safety within the monitored area, a local council may be found liable should a person be injured in some way. This is especially so where camera equipment is not working, is not supervised or is pointing in the wrong direction.

It is strongly recommended that local councils seek independent legal advice on this issue prior to installing CCTV equipment.

10. Staffing of the control centre

The Control Centre is to be staffed by either contracted security personnel or local council employees and is to meet the requirements of the *Security Industry Act 1997*. Under the terms of the Act, all personnel employed in the Control Centre are required to be licensed security operators. Personnel assigned to the Centre must be trained and qualified in the use of surveillance equipment and the responsibilities required.

A local council, when defining the contractual terms for the party engaged to conduct the CCTV monitoring, should make that party aware of the requirements of the *Security Industry Act 1997*.

It is recommended that a set of Standard Operating Procedures are developed for Control Centre monitoring staff. The Standard Operating Procedures must reflect the requirements of section 12 of the *Privacy and Personal Information Protection Act 1998.*

It is further recommended that Control Centre staff are required to sign an undertaking to comply with the Standard Operating Procedures and confidentiality agreement and that they are subject to disciplinary action should they breach that undertaking.

11. Control and operation of cameras

Monitor operators must act with the utmost probity.

The tracking or zooming in on any member of the public should never be done in a gratuitous or unreasonable manner. All operators should be made aware, as a matter of course, that their camera operation may be audited and that they may be called upon to explain their interest in a member of the public.

Generally, operators will not allow cameras to view into private residences. Private residences may come into view as part of a wide angle or long shot or as a camera is panning past them.

An operator may allow a private residence to remain in view when there are reasonable grounds for so doing, that is, for the purpose of identifying individuals or actions when there is a reasonable suspicion that a serious offence is in progress or is about to occur.

12. Erection of signs

Signs informing the public of the existence of CCTV cameras must be erected. There is currently no one sign that is universally accepted – different signs have been developed by organisations using CCTV, including local councils.

In deciding the design and location of signs, it is strongly recommended that councils consider Australian Standard – *Development, testing and implementation of information and safety symbols and symbolic signs* – AS 2342 – 1992. This publication is available from Standards Australia, telephone 1300 654 646.

The information provided on the signs should comply with section 10 of the *Privacy and Personal Information Protection Act 1998* and include at a minimum:

- the contact details for the ownership of the scheme
- the purpose of the scheme, and
- hours of operation (e.g. when the area is monitored – continuous or random).

13. Complaints

The *Privacy and Personal Information Protection Act 1998* authorises the Office of the Privacy Commissioner to receive and investigate complaints about alleged violations of privacy. Any information distributed about the scheme should advise members of the community that they can lodge a complaint to the NSW Information and Privacy

Commission under section 45 of the *Privacy and Personal Information Protection Act 1998*. Local councils should also cooperate with the investigation of any complaint by the NSW Information and Privacy Commission.

Part 5 of the *Privacy and Personal Information Protection Act 1998* requires that wherever a complaint indicates that an information protection principle has been breached, a local council must conduct an internal review as outlined in that Part of the Act. This process is subsequently reviewable by the Administrative Decisions Tribunal.

Complaints which do not indicate a breach of the *Privacy and Personal Information Protection Act 1998* can be handled in the manner set out below.

Local councils should already have a complaints handling mechanism in place as outlined in the Department of Local Government's *Practice Note No.9 Complaints Management in Councils (August 1994)*. This mechanism, which provides for the following three levels of review, should also be used to deal with any complaints about the CCTV system.

First level – while any council staff member may be able to receive a complaint about the CCTV system, it is strongly recommended that complaints of this nature be dealt with by a designated CCTV complaints officer. If complaints relate to issues of privacy, they should be handled by staff that are aware of and sensitive to privacy issues in relation to the use of CCTV.

Second level – if the complainant is dissatisfied following the first level response the complaint should be investigated by a more senior officer and the results of the investigation reported to the complainant.

Third level – where the complaint cannot be resolved within the council, the complainant should be referred to an outside agency to seek resolution. The Information and Privacy Commission is authorised under the *Privacy and Personal Information Protection Act 1998* to receive, investigate and resolve through conciliation, complaints about alleged violations of privacy. The Ombudsman investigates complaints about the conduct of public authorities, and will always consider for investigation complaints which cannot be resolved within the public authority, as well as failure by a public authority to deal satisfactorily with a complaint.

14. Monitoring, evaluation and auditing

It is essential that the community have confidence in the operation of CCTV technology. Local councils and other public authorities should regularly audit compliance with the *PPIP Act*. In addition to audits, all logs of Control Centre activity should be regularly scrutinised by the owners of the scheme.

Local councils should arrange for an independent audit to be carried out every 12 months.

The NSW Information and Privacy Commission may request to undertake spot audits from time to time and local councils should comply with such requests.

Local councils should also inform the public about how they can obtain access to the results of any audits. The results of audits should be included in formal evaluation reports.

Copies of completed audits should be submitted to the Privacy Commissioner by emailing them to ipcinfo@ipc.nsw.gov.au.

15. Code of practice, protocols and standard operating procedures

A detailed code of practice that covers all aspects of the management of the operations of a public area CCTV scheme should be developed. Such a code would include reference to all the following matters:

- scheme objectives and principles of operation
- parameters of the scheme including geographical boundaries, number and location of cameras, system description, method of operation
- scheme ownership, partners to the scheme including suppliers of equipment and Police and their respective responsibilities, management of the scheme, control and operation of cameras, accountability, monitoring and evaluation mechanisms, and avenues for complaints
- signage, publicity and information about schemes
- rules defining access to scheme control rooms and monitors so that only those with a lawful and legitimate reason may operate or view the equipment in a control room
- adequate standards for the recruitment, integrity and training of control room staff
- lawful, fair, safe and secure procedures defining recording and storage practices, image retention times, image re-use and image copying
- information being recorded which is adequate, accurate, and relevant
- rules on how recorded images are accessed for evidentiary purposes which satisfy continuity of evidence

- provision for the implementation of disciplinary and/or other procedures where protocols are breached.

The Code of Practice should underpin the management and operations of the scheme and be supplemented by Protocols or Procedures and appropriate Standard Operating Procedures for participating agency staff to guide the day-to-day operation of the scheme.

Again, section 12 of the *Privacy and Personal Information Protection Act 1998* lays out a number of requirements relating to security of information collected and held. Standard Operating Procedures should comply with these requirements and these should be built into formal agreements, such as Memorandums of Understanding, between local councils and the NSW Police Force.

16. Technical specifications

Given the ever evolving technological advancements in the CCTV sphere, it is strongly suggested that scheme owners seek expert advice on issues relating to technical requirements and specifications that best suit their proposed usage and local area.

List of resource information

Acts

- *Privacy and Personal Information Protection Act 1998* (NSW) (No. 133 of 1998)
- *Security Industry Act 1997* (NSW) (No. 157 of 1997)
- *Workplace Surveillance Act 2005* (NSW) (No. 47 of 2005)
- *Local Government Act 1993* (NSW) (No. 30 of 1993)
- *Local Government (Tendering) Regulation* (NSW) (No. 464 of 1999)

Standards

- Australian Standard AS 4806.1 – 2006, *Closed circuit television (CCTV), Part 1: Management and operation*
- Australian Standard AS 4806.2 – 2006, *Closed circuit television (CCTV), Part 2: Application guidelines*
- Australian Standard AS 4806.3 – 2006, *Closed circuit television (CCTV), Part 3: PAL signal timings and levels*

- Australian Standard AS 4806.4 – 2008, *Closed circuit television (CCTV), Part 4: Remote video*
- Australian Standard AS 2342 - 1992, *Development, testing, and implementation of information and safety symbols and symbolic signs*
- Australian Standard AS 4269 - 1995, *Complaints Handling*

Resources

- NSW ATTORNEY GENERAL'S DEPARTMENT, *Crime Prevention Resource Manual*, 1998
- NSW DEPARTMENT OF LOCAL GOVERNMENT, *Competitive Tendering Guidelines*, January 1997
- NSW DEPARTMENT OF LOCAL GOVERNMENT, *Practice Note No. 9, Complaints Management in Councils*, August 1994
- PRIVACY NSW, A Guide to the Information Protection Principles, 2000
- *Raciti v Hughes* (unreported, Supreme Court of NSW Equity Division, No. 3667 of 1995)

Appendix 1

Privacy and Personal Information Protection Act, 1998

Part 2 – Information protection principles

Division 1 – Principles

8. Collection of personal information for lawful purposes

(1) A public sector agency must not collect personal information unless:

(a) the information is collected for a lawful purpose which is directly related to a function or activity of the agency, and

(b) the collection of the information is reasonably necessary for that purpose.

(2) A public sector agency must not collect personal information by any unlawful means.

9. Collection of personal information directly from individual

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:

(a) the individual has authorised collection of the information from someone else, or

(b) in the case of information relating to a person who is under the age of 16 years the information has been provided by a parent or guardian of the person.

10. Requirements when collecting personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:

(a) the fact that the information is being collected

(b) the purposes for which the information is being collected

(c) the intended recipients of the information

(d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided

(e) the existence of any right of access to, and correction of, the information

(f) the name and address of the agency which is collecting the information and the agency which is to hold the information.

11. Other requirements relating to collection of personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

(a) the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete, and

(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

12. Retention and security of personal information

A public sector agency which holds personal information must ensure:

(a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and

(c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

(d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

13. **Information about personal information held by agencies**

A public sector agency which holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the agency holds personal information, and

(b) whether the agency holds personal information relating to that person, and

(c) if the agency holds personal information relating to that person:

(i) the nature of that information, and

(ii) the main purposes for which the information is used, and

(iii) that person's entitlement to gain access to the information.

14. Access to personal information held by agencies

A public sector agency which holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

15. Alteration of personal information

(1) A public sector agency which holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:

(a) is accurate, and

(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

(2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the public sector agency.

16. Agency must check accuracy of personal information before use

A public sector agency which holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

17. Limits on use of personal information

A public sector agency which holds personal information must not use the information for a purpose other than that for which it was collected unless:

(a) the individual to whom the information relates has consented to the use of the information for that other purpose, or

(b) the other purpose for which the information is used is directly related to the purpose for which the information was collected, or

(c) the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

18. Limits on disclosure of personal information

(1) A public sector agency which holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

(a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or

(b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or

(c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

(2) If personal information is disclosed in accordance with subsection (1) to a person or body which is a public sector agency, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

19. Special restrictions on disclosure of personal information

(1) A public sector agency must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

(2) A public sector agency which holds personal information must not disclose the information to any person or body who is in a jurisdiction outside New South Wales unless:

(a) a relevant privacy law which applies to the personal information concerned is in force in that jurisdiction, or

(b) the disclosure is permitted under a privacy code of practice.

(3) For the purposes of subsection (2), a "relevant privacy law" means a law which is determined by the Privacy Commissioner, by notice published in the Gazette, to be a privacy law for the jurisdiction concerned.

(4) The Privacy Commissioner is, within the year following the commencement of this section, to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales.

(5) Subsection (2) does not apply:

(a) until after the first anniversary of the commencement of this section, or

(b) until a code referred to in subsection (4) is made, whichever is the later.

The Guidelines are also available on the Internet at www.justice.nsw.gov.au

ISBN 0 7347 6702 1