

# submission

Privacy NSW submission on the  
NSW Law Reform Commission Report 98

## Surveillance: An Interim Report



privacynsw

*Issue date: 24 June 2002*

## **CONTENTS**

<b>1. Executive Summary</b>	<b>3</b>
<b>2. Submission lodged 24 June 2002</b>	<b>5</b>
General comments	5
Overt surveillance	6
Covert surveillance	19
Other comments	28
Conclusion	28

## Executive Summary

Privacy NSW strongly supports the over-arching recommendations of the Law Reform Commission Report 98 Surveillance: An Interim Report ("LRC Report") in relation to the development of a comprehensive Surveillance Act which is technology-neutral in its application. In developing the new Act, it is critical to ensure that:

- the proper balance is struck between the public interest in the protection of individuals' privacy on the one hand, and the public interest in law enforcement and public safety on the other;
- the privacy principles already binding on State and local government in NSW not be diminished in any way through any new legislation;
- there is consistency in the application of the privacy principles across the public and private sectors unless there is a justifiable reason otherwise; and
- that there are adequate and transparent oversight and accountability provisions backed by legislative authority.

### Overt surveillance

In relation to overt surveillance, Privacy NSW has made the following key recommendations:

- The visibility of the surveillance equipment itself ought not be considered adequate; that is, without signs or other written/audio warnings, the surveillance ought be considered 'covert'.
- Surveillance always constitutes an interference with privacy rights. Rather than the test proposed by the LRC - whether the use of surveillance has breached an individual's "reasonable expectation of privacy" - the real question is whether that interference with privacy is warranted. This approach would ensure that the onus of justifying the use of surveillance is placed upon the surveillance user rather than the individual whose privacy has been breached.
- Consequently, surveillance users should be able to justify that the surveillance is for a lawful purpose, directly related to a lawful function of that surveillance user, and the surveillance must be reasonably necessary for the achievement of that purpose.
- The Act or regulations must make clear the appropriate standards with respect to the storage and destruction of surveillance material, having given due consideration to the competing interests of privacy protection and State records obligations.
- There must be a specific principle which addresses disclosures to third parties.
- The complaints and enforcement model established under the Health Records & Information Privacy Act 2002 is the preferred option. Such a model allows for complaints about public sector agencies to be dealt with through the complaints mechanisms already established under the PPIP Act and establishes Privacy NSW as the main complaints-handling body for the private sector.

## **Covert Surveillance**

The LRC Report suggests that authorisation for covert surveillance can only be given for the purposes of law enforcement, protecting the public interest and employment-related investigations. In relation to covert surveillance, Privacy NSW has made the following recommendations:

- In relation to law enforcement activities, a covert surveillance authority should only be issued for the enforcement of serious indictable offences, being those with a maximum penalty of 7 years' imprisonment or more.
- Since the term 'public interest' is one which is commonly misunderstood, manipulated, or inconsistently applied, it is essential that the proposed Act include a specific definition of the 'public interest', which weighs appropriately the public interest in the protection of privacy as a human right against other interests.
- If an application is made under the grounds of 'unlawful activity', the employer must be required to establish that they have a legitimate interest in preventing the behaviour, and that there is a sufficient explanation for not involving NSW Police instead.
- The very nature of covert surveillance raises serious questions about unauthorised surveillance material, secondary use, disclosure to subjects of covert surveillance, nature of such disclosure and destruction of material gathered during surveillance.

Privacy NSW therefore supports comprehensive legislation to regulate these issues.

## General comments

This submission is made to the Law Reform Commission, in response to *LRC Report 98 - Surveillance: An Interim Report* (the Report).

More than 12% of telephone enquiries and formal complaints made to this Office concern CCTV, listening devices and related surveillance matters<sup>1</sup>. This demonstrates a general community concern with the use of surveillance to violate or interfere with individuals' privacy rights.

I therefore support the approach of the Report's recommendations with respect to the need for one Act to regulate all forms of surveillance, and for that Act to remain technology-neutral in application.

As recognised at 1.39 of the Report, NSW public sector agencies, including local and county councils, are already regulated in their dealings with personal information by the Information Protection Principles (IPPs) in the *Privacy and Personal Information Protection Act 1998* (PPIP Act). The PPIP Act is technology-neutral, and the definition of 'personal information' therefore includes any electronic records, still photographs, video and sound recordings which include information about a person whose identity is known or can reasonably be ascertained.

It must therefore be recognised that the Parliament of NSW has already set the balance between the public interest in the protection of individuals' privacy on the one hand, and the public interest in law enforcement and public safety on the other.

I therefore approach the proposal to develop a new Surveillance Act as an opportunity to ensure that the privacy principles already binding on NSW public sector agencies, including local and county councils, are not diminished in any way.

It is therefore my overriding submission that

- government surveillance users should be subject to the same or higher privacy standards than already exist under the PPIP Act, and
- there must be consistency in the application of the privacy principles across the public and private sectors unless there is a justifiable reason otherwise.

---

<sup>1</sup> 12.7% of telephone enquiries, 12.4% of formal complaints, and 19.6% of written requests for advice in 1999-2000 and 12% of formal complaints in 2000-01.

## Overt surveillance

### Introduction

I agree with the Report's view that a set of principles for overt surveillance would serve the public interest, by ensuring clarity and consistency for all parties. I furthermore agree that those principles must aim for a balance between the public interest in the protection of individuals' privacy on the one hand, and the public interest in law enforcement and public safety on the other.

I note with particular concern that no research has been conducted on the effect of the recent proliferation of overt surveillance, in particular CCTV in public places and public facilities, on the ability for persons with mental or psychiatric illnesses to access government services. Anecdotal evidence and complaints to this Office from the mental health community suggest that individuals with paranoia and related conditions now feel that they cannot go where surveillance cameras exist, and are therefore avoiding public transport, city streets and plazas, and public facilities such as libraries.

There is however international research to suggest that CCTV cameras, especially where being controlled in real-time by an operator, are used selectively to target individuals belonging to particular sub-groups, such as young people, black people, beggars, drunks, and homeless people.<sup>2</sup>

The extent to which use of public space and public facilities has become conditional upon an acceptance of the intrusion of surveillance cameras into our lives is of concern to me as Privacy Commissioner. However this is not just a matter of privacy but an issue of equity.

Any overt surveillance of public places may amount to indirect discrimination against people with mental or psychiatric illnesses. Targeted overt surveillance may be an instrument of both individual and institutional discrimination against the young, people from non-Anglo communities, people with intellectual disabilities or mental illnesses, and the homeless. The extent to which the proliferation of overt surveillance in public places therefore entrenches social disadvantage to create a permanent underclass of citizens should be of major concern to all of us.

### Definition of overt surveillance

The Report suggests surveillance will be considered 'overt' as long as "adequate notice" has been or is given of the surveillance. At 2.78 of the Report, it is proposed that any one of three methods would be sufficient for the purposes of establishing that adequate notice has been given: visible signs, written or audio warnings, or the visibility of the surveillance equipment itself.

Given the variety of environments and types of surveillance, the quality of notification will vary significantly. It may perhaps be necessary, for the Privacy Commissioner or another regulatory body, to develop standard signage, or at least guidelines.

I would argue that the visibility of the surveillance equipment itself ought not be considered adequate; that is, without signs or other written/audio warnings, the surveillance ought be considered 'covert'. The alternative is to consider the surveillance itself 'overt' for the purposes of the Act, but that non-compliance with the more specific requirements of Principle 4 (below) will be an offence.

---

<sup>2</sup> See for example the discussion in Electronic Privacy and Information Center & Privacy International, *Privacy and Human Rights 2001*, EPIC, USA, 2001, pp.59-62. Available from [www.epic.org/bookstore/](http://www.epic.org/bookstore/).

## How the principles will work in practice

I agree that non-compliance of the principles should constitute a breach of the Act.

However I disagree with some of the features of the framework of regulation suggested in the Report. The Report suggests at 4.32 that a surveillance user *must* have developed their own 'code of practice'. The code envisaged would set out how the surveillance user will "give consideration to the overt surveillance principles", and will act as an internal guide to those using such a system.

Given my comments below with respect to the scope of application of these principles, I would suggest that the development of a written code of practice *not* be mandatory, but that in any case the default position must be compliance with the principles. The absence of a code alone should not constitute an offence. An alternative is to state that the absence of a code will be taken as a decision to adopt a 'model' code, to be published by the Privacy Commissioner.

Either of these alternatives will still allow for consistency, and accessibility for the public who wish to know what principles guide the surveillance user, but will eliminate the need for the legislation to delineate between 'small' and 'relevant' surveillance users as recommended at 4.37 of the Report.

In particular my concern is that the introduction of such a delineation would result in unnecessary confusion about who must have a 'code', and therefore unnecessary expending of time and resources on answering that question, rather than focussing users' attention on their need to comply with the principles, regardless of whether or not they have developed their own code.

For public sector agencies, which must already have a Privacy Management Plan in place (pursuant to the PPIP Act), I would suggest that any 'code' which explains how the agency is to comply with the Principles for Overt Surveillance could logically sit within or as an annexure to their broader Privacy Management Plan. This will help to reinforce the message that surveillance is inherently an interference with individuals' privacy, which must be warranted and which must fit within the agency's wider privacy obligations.

I would also suggest that the nomenclature be changed, to avoid confusion with *Privacy Codes of Practice* made under s.31 of the PPIP Act (which are effectively exemptions to the provisions of the PPIP Act, made by the Attorney General), and *Privacy Codes* or *Codes* made by private sector organisations, with the approval of the Federal Privacy Commissioner, under the *Federal Privacy Act 1988 (Cwth)*, which allow organisations and industries to have and to enforce their own privacy codes that continue to uphold the privacy rights of individuals while allowing some flexibility of application for organisations.

## Scope of application of principles

The overt surveillance principles must apply to all users of overt surveillance, regardless of whether they are in the public or private sector, their size, or their purpose in seeking to use surveillance.

## Role of the Privacy Commissioner

At 4.46 and 4.73 of the Report, it is suggested that with respect to contentious issues, surveillance users (or, presumably, complainants or others with an interest in the matter) should be able to approach the Privacy Commissioner for a "ruling" on whether a particular practice complies with a Principle.

This proposal would cause some confusion as to the role of the Privacy Commissioner, particularly as my Office may need to investigate complaints which concern practices or issues addressed in earlier rulings.

In my view it is not the role of the Privacy Commissioner to establish what are acceptable community or industry standards. The Privacy Commissioner's role is primarily to promote the protection of privacy, while surveillance activity of any kind is inherently privacy invasive. In addition this would potentially be a point of conflict should I be in a position where I had endorsed some practice or type of surveillance but then had to investigate a breach of privacy which may question the appropriateness of this standard. As with the code of practice provisions in the PPIP Act, I consider it appropriate that the Attorney-General should be the person to determine any standards, on advice from the Privacy Commissioner.

With respect to users seeking "rulings", the Report tends to suggest that my staff could visit a site and after examination determine that it complies with the relevant Act or some technological standard and endorse it. My Office has neither the resources, expertise or desire to undertake such an activity and nor can it determine that the entity will use the equipment in the proper way. However, general advice and assistance could be given, as is the case under the PPIP Act, in terms of monitoring compliance.

The making of "rulings" is of course a judicial function, which should only be exercised by a court or tribunal.

However I agree with the other proposals with respect to general powers (4.68) and inspection powers (4.70).

In respect of overt surveillance I would suggest that the Act clarify that inspection might occur either:

- as part of dealing with a complaint lodged with my Office; or
- on a routine or random basis (particularly in respect of public sector agencies).

Where it is necessary for the Privacy Commissioner to issue guidelines on certain matters under the Act, it should be specified whether or not those guidelines are binding, *must* be 'taken into consideration', or *may* be 'taken into consideration'.

However, as noted further below, I would suggest that as much as possible, the boundaries of the Act must be delineated within the Act itself or within regulations made under the Act. Particularly controversial issues such as employee / performance monitoring, through the use of CCTV, listening devices and monitoring email / internet usage, ought be determined by Parliament or the Attorney General following a period of consultation.

#### Principle 1: Surveillance cannot breach individual's "reasonable expectation of privacy"

I am concerned that what is described in the Report (at 4.41) as an "intuitive" measure of the acceptability of surveillance in a particular circumstance – the expression "reasonable expectation of privacy" – is in fact an extremely malleable concept. I am concerned that individuals whose privacy has been breached by use of surveillance will have the onus of proving that their expectation was reasonable in the first place.

Despite the Report's assurances that a reasonable expectation of privacy "cannot be ousted through the provision of notice of surveillance" (4.43), I believe that respondents will be able to increasingly rely on what is perceived as a cultural shift towards less privacy as an excuse for their own actions. That is, every utterance such as that by the CEO of Sun Microsystems Scott

McNealy, who declared some years ago that “you’re already got zero privacy, get over it”, and every new CCTV camera erected on a public street, and every time airport security is beefed up, will only serve to strengthen the claims of surveillance users that individuals should no longer have any expectation of privacy, outside their own homes.

The Law Reform Commission, at 4.41, agrees with my position that privacy is a personal right. I would argue that surveillance is always, by its very nature, an interference with our privacy rights. The real question therefore is whether that interference with privacy is warranted.

I would therefore submit that the more appropriate principle ought be that the overt surveillance must not intrude *unnecessarily* or *unreasonably* into a person’s private affairs or personal space. That is, the starting position ought to be that it is for the surveillance user to justify why an interference with privacy is warranted, rather than for the subject to justify why their ‘expectation’ of what is actually their *right* is ‘reasonable’.

By way of example, IPP 4 in the PPIP Act provides:

**IPP 4: Section 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.

Such a principle would also ensure that Principle 1 is no more accommodating of privacy-invasive practices than the PPIP Act would currently allow.

International experience has shown that the test of “reasonable expectation of privacy” has not, in practice, actually been protective of privacy. In the United States, since the test was first formulated in *Katz v US* in 1967, the privacy protection afforded by the test in theory has been successively watered down by the courts, such that as technology improves there is a assumption that privacy expectations should be lowered accordingly.<sup>3</sup>

On a number of occasions, Congress has had to create legislative privacy rights after the courts had found no “reasonable expectation of privacy” in relation to various practices or information, including financial records<sup>4</sup>, and telephone dialling records<sup>5</sup>. The “reasonable expectation of privacy” test has furthermore been found not to have been breached in relation to vehicle tracking devices<sup>6</sup>, or searches of garbage left for collection<sup>7</sup>.

In the USA expectations of privacy are therefore being actively lowered by technical advances in machines and devices designed to invade privacy. In that sense the test of “reasonable expectation of privacy” has become a reflective standard rather than a proscriptive one.

---

<sup>3</sup> EPIC & Privacy International, as above.

<sup>4</sup> *US v Miller*, 1977; Right to Financial Privacy Act 1978. See discussion of this in *Privacy and Human Rights 2001* (as above), and at [www.cdt.org](http://www.cdt.org) - the website of the Centre for Democratic Technology, USA.

<sup>5</sup> *Smith v Maryland*; Electronic Communications Privacy Act 1986 - as per note 4.

<sup>6</sup> *US v Knotts* - see Lessig L, Post D & Volokh E, *Cyberspace Law for Non-Lawyers*, Social Science Electronic Publishing Inc, USA : [www.ssrn.com](http://www.ssrn.com)

<sup>7</sup> *California v Greenwood* - as per note 6.

This test alone would not be robust enough to prevent the proliferation of a surveillance society and eventually a police state. Given the fundamental nature of our need for privacy, as a cornerstone for the freedom of speech and freedom of association at the heart of a healthy democracy, the onus must be upon those who seek to invade peoples' privacy through surveillance to justify the reasonableness of their own actions.

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

In line with the ordering of the information privacy principles in the PPIP Act, which arguably reflects the sense of the fundamental threshold nature of the 'purpose' test, this Principle should really be 'No. 1'.

The Report suggests at 4.44 that surveillance can be established so long as one or more of the following purposes apply:

- protection of the person
- protection of property
- protection of the legitimate public interest, or
- protection of a legitimate commercial interest.

In addition, the Report suggests that "public bodies" must prove that the surveillance is, on balance, "in the interests of the general public".

It is my submission that these tests are too broad and too weak. A stricter threshold test must be applied, in order to ensure that protection of the surveillance subjects' privacy is being properly balanced against the surveillance user's interests.

I agree with the position of the NSW Council for Civil Liberties that if surveillance is to be permitted at all, sufficient safeguards must be in place. The ostensible purpose of surveillance must be tied to a realistic and demonstrable need to conduct surveillance in order to achieve a legitimate and lawful objective, and in so doing ensure that the surveillance only collects such information which is necessary to achieve the objective.

Again I make the point that public sector agencies in NSW must already justify any collection of personal information in terms of IPP 1 in the PPIP Act, and any new legislation must not allow a diminishing of privacy protection.

IPP 1 provides:

#### **IPP 1: Section 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 that 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.

I would therefore suggest that surveillance users should first be able to justify that:

- the surveillance is for a lawful purpose, directly related to a lawful function of that surveillance user, *and*
- the surveillance must be *reasonably necessary* for the achievement of that purpose.

I have, for example, recently expressed my concern that the use of CCTV in public places by local councils, for the purposes of general law enforcement (crime prevention and crime detection), may for the most part be *ultra vires*.

Councils have the power to enforce various provisions of the *Local Government Act 1993*, as well as act on potential breaches of other Acts administered by Councils (eg. the *Environmental Planning and Assessment Act (1979)*). Councils are of course entitled to inform relevant authorities (such as the NSW Police) where they become aware of breaches of the criminal law, as long as these become known to them incidentally, through exercising their own prescribed functions. However, it is my view that nothing in the *Local Government Act* or any other law allows councils to widen their regulatory functions to actively monitor or detect inappropriate public behaviour and/or potential breaches of the criminal law.

Therefore, it is my view that in order to comply with IPP 1 (s.8(1)(a) of the PPIP Act), the use of CCTV by councils must be for the lawful purpose of preventing breaches of, detecting breaches of, or enforcing the provisions of, the *Local Government Act* (or other Acts administered by councils in a regulatory capacity), since the prevention, detection and enforcement of such breaches is a lawful function of councils.

I have also expressed concern that with one exception (Fairfield City Council), councils have not complied with the Inter-Departmental Committee's Guidelines on CCTV with respect to conducting evaluations, and making such evaluations public. This silence raises a suspicion that they could not actually justify the scope of their CCTV operations.

With respect to Fairfield City Council's evaluation report, I note that of the 7,848 incidents detected in the 5 year period 1997-2001, only 451 (5.7%) related, in my view, to functions arising out of legislation which the Council administered under the *Local Government Act* or related Acts.<sup>8</sup>

The drafting of the proposed Surveillance Act ought therefore be absolutely clear about delimiting the functions of public sector agencies. I would suggest that in the case of public sector agencies, 'lawful functions' ought be linked to specific legislative authority for such functions.

While the notion of a 'lawful function' is reasonably familiar in its application to public sector agencies, it may not inherently make sense when applied to private individuals and private sector organisations. The Act should therefore state that the following 'lawful functions' may be attributable to private individuals and private sector organisations:

- protection of the person,
- protection of property, or
- protection of a legitimate commercial interest.

I would suggest that with respect to private individuals or organisations, only the news / current affairs media could claim that they had a 'lawful function' of

- protection of the legitimate public interest.

By putting the onus on the surveillance user to initially justify its *need* for surveillance, this stricter test will effectively prevent those abuses of privacy which might otherwise be seen to involve 'pushing the envelope' with respect to the tests described in the Report at 4.46.

---

<sup>8</sup> These related to the following items listed on the second last page of Annexure 1 of the Report - Environmental, Waste, Health, Ordinance Breach, Damage/Maintenance and Water.

For example, a television news report on skin cancer which features close-up footage of sleeping topless female sunbathers, rather than footage of general beach scenes, ought be described as *not* “reasonably necessary” for its purpose.

The area of ‘domestic’ surveillance use is particularly fraught. My Office has in recent months noticed a rise in the number of enquiries being made with respect to the alleged installation of surveillance devices by landlords in rented premises. Neighbour-to-neighbour disputes remain common.

With respect to formal complaints closed by my office since 1 July 2001 (ie. not yet the full year’s worth), 24 complaints (11.7% of the total of 204) were primarily with respect to surveillance / monitoring issues. (This figure is quite high, given my Office has no responsibilities under the Listening Devices Act or the Workplace Video Surveillance Act.)

Of the 13 formal complaints made with respect to CCTV / video / listening device surveillance, the most common respondents were private individuals (46%), followed by private organisations (30%), and then the State government (23%). The most common relationship between the complainant and the respondent was as the respondent’s neighbour (54%), as the subject of the respondent’s investigation (15%), or as an interested member of the public (15%).

I am concerned by the extent to which ‘domestic’ users of surveillance see themselves as protecting the ‘public’ interest by conducting surveillance on their neighbours. It is therefore imperative that clear limits be placed upon what ‘lawful functions’ may be contemplated by ‘domestic’ users of surveillance, and the extent to which surveillance is reasonably necessary for the pursuit of those functions.

The Act (or regulations) ought prescribe that, for example, overt surveillance in the pursuit of “protection of the person” or “protection of property” can only operate on a person’s own property, including entrances and exits. Overt surveillance of neighbouring properties (other than incidental capture) should not be permitted by ‘domestic’ users at all, notwithstanding the ‘vigilante’ stance adopted by some surveillance users currently.

In respect of private sector ‘commercial’ users (which predominantly will be businesses seeking to use surveillance for the protection of their property, commercial interests, or the personal safety of their staff or clients), the Act should allow regulations to be prescribed to define the limits of what may be considered ‘reasonably necessary’ for each of the above purposes, allowing for some differences across industry sectors, taking account for instances of the type and frequency of surveillance and the relative risks to the organisation.

It should be noted, for example, that an inappropriate use of surveillance from commercial premises was recently brought to the attention of this Office. The commercial premises next door to the Safe Injecting Room in Sydney had cameras in place, which were purportedly for the premises’ security, but which in fact served to intimidate people potentially seeking to use the Safe Injecting Room. This type of practice may have adverse public health and social outcomes, which is why guidance is required to define the limits of what may be considered ‘reasonably necessary’ in terms of CCTV and similar devices.

The introduction of this two-stage threshold test – purpose of surveillance linked to lawful function; surveillance must be reasonably necessary for that purpose - may also help to relieve or minimise the importance of relying on surveillance subjects’ ability to meet subjective tests such as ‘reasonable expectation of privacy’ (see my comments in regard to Principle 1, above).

The Act could also allow, in addition to or instead of regulations, the Privacy Commissioner to develop guidelines on what might activities might fit within the above ‘functions’, but, as noted above, any ‘rulings’ on the topic must be left to the judiciary.

### Principle 3: Use must be consistent with purpose

I agree with this Principle.

In the absence of a code of practice developed by the user defining what the intended 'purpose' of the surveillance was, the 'model' code ought be taken as the default position in this respect.

NSW public sector agencies are already bound by IPP 10, which provides:

#### **IPP 10: Section 17. Limits on use of personal information**

A public sector agency that 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.

### Principle 4: Notice provisions shall identify the surveillance user

I agree that surveillance users must be readily identified for accountability purposes.

As per my comments above with respect to the definition of 'overt' surveillance, I would argue that the visibility of surveillance equipment itself ought not be considered adequate 'notice' under Principle 4. However I concede that with respect to news / current affairs media, the use of station logos on equipment could suffice.

Again, public sector agencies in NSW, including local councils, are bound to comply with IPP 3, which provides:

#### **IPP 3: Section 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 that is collecting the information and the agency that is to hold the information.

I would therefore argue that public sector agencies, under the proposed Surveillance Act, must be obliged to meet a higher test than simply notifying who the user is. This is consistent with my general argument that the proposed Act must not diminish the privacy protection already afforded by the PPIP Act.

It is my view that at a minimum, public sector users should be obliged to erect signs which show the agency's name, the purpose of collection, and the circumstances in which footage will be used and disclosed to other authorities. A phone contact number should be included to identify who should be contacted to obtain additional information.

#### Principle 5: Users to be accountable for consequences of use

I agree that the Act should prohibit any attempt by surveillance users to 'outsource' or delegate their responsibilities for compliance with these Principles to contracted operators.

I agree with the suggestion that a register be maintained by each surveillance user, open for inspection by the Privacy Commissioner. This provision could be avoided by 'domestic' users by instead complying with a verbal or written request from the Privacy Commissioner for information about the number and type of devices being used, and their location and scope of coverage.

I agree with the recommendation that public sector agencies must report on their overt surveillance activities in their annual reports.

I would add a recommendation that public sector agencies must also explain in their Privacy Management Plan (a document required of them already under the PPIP Act) the purposes and scope of their overt surveillance activities. The Privacy Management Plan, as noted above, could double as the 'code of practice' which explains how their use of overt surveillance complies with the Principles.

#### Principle 6: Security of surveillance system

Public sector agencies in NSW must already comply with IPP 5:

##### **IPP 5: Section 12. Retention and security of personal information**

A public sector agency that holds personal information must ensure:

- (a) ...
- (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.

In determining what is the appropriate standard with respect to the storage of personal information, either in the form of the original surveillance material (eg. CCTV footage) or in another form arising from that material, agencies currently have to consider a number of matters including IPP 5 in the PPIP Act, and their obligations under the State Records Act.

I would therefore suggest that rather than guidelines to be issued by the Privacy Commissioner, the Act or regulations themselves must make clear the appropriate standards with respect to the appropriate storage of surveillance material, such as video footage. (I would of course seek to be consulted in the development of such provisions, as should the State Records Authority.) There may already be appropriate Australian or International Standards which could be referenced in the legislation.

## Principle 7: Material to be used in a fair manner and only for purpose obtained

Principles 3 and 6 already touch upon the issue of improper use of surveillance material – for example, the images obtained from overt surveillance should not be displayed on ‘wanted’ posters. It may be appropriate to merge principles 3 and 7.

The proposed Act should in this respect use IPPs 9 and 10 of the PPIP Act as a guide:

### **IPP 9: Section 16. Agency must check accuracy of personal information before use**

A public sector agency that 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.

IPP 10 provides:

### **IPP 10: Section 17. Limits on use of personal information**

A public sector agency that 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.

The proposed Surveillance Act could incorporate appropriate exemptions for law enforcement / protection of the public revenue purposes (eg. see s.23(4) of the PPIP Act) or investigative functions (eg. see the current s.41 direction under the PPIP Act ‘Direction On Processing of Personal Information By Public Sector Agencies In Relation To their Investigative Function’).

As a way of ensuring the integrity of Principle 7, there should also be a legislative prohibition on the provision of information gained through overt surveillance for profit or benefit. Clearly there would need to be some exceptions to this prohibition, such as

- people involved in the media (including freelance journalists and photographers), and
- people engaged by others to collect information (eg. licensed private inquiry agents or surveillance operators).

## Principle 8: Destruction of surveillance material

As noted above, public sector agencies in NSW must already comply with IPP 5 in the PPIP Act:

### **IPP 5: Section 12. Retention and security of personal information**

A public sector agency that 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) ...

In determining what is the appropriate time period to retain personal information, either in the form of the original surveillance material (eg. CCTV footage) or in another form arising from that material, agencies currently have to consider a number of matters including:

- IPP 5 in the PPIP Act;
- the effect of the State Records Act;
- the criteria that should be applied in making decisions to retain information for possible future use or disclosure;
- the ability to retain only information useful for the purposes for which it was collected; and
- the utility of originals (versus copies or extracts) for evidentiary purposes.

This is already a complicated area for public sector agencies, given the competing interests of privacy protection (that information be kept no longer than is necessary for its original purposes) and state records obligations (that government records must be kept for certain periods). As both these interests are inherently about government accountability, it is appropriate that the appropriate balance between them be clarified in legislation by Parliament.

In addition, the existing tension between the PPIP Act and the State Records Act requires resolution through legislative amendment, to explicitly exclude the operation of the State Records Act to surveillance material, and then set specific legislative rules with respect to maximum retention periods. These periods must apply equally to public and private sector surveillance users.

I agree that a standard maximum retention period of 21 days, with an exception for the media, is appropriate, with the ability to seek an order from a magistrate to allow a longer period if the material is necessary evidentiary material with respect to law enforcement, civil or criminal proceedings, or to find a missing person.

As previously expressed with respect to my proposed functions under the Act, it is not appropriate for the Privacy Commissioner to issue 'rulings'. Likewise, with respect to the recommendation at 4.66 of the Report, I do not believe it is appropriate for a surveillance user to seek the Privacy Commissioner's 'consent' to a practice which would otherwise breach this Principle. This is an appropriate request of a magistrate, as recognised at 4.65.

#### An additional Principle – third party disclosure?

Principles 6 and 7 touch upon the issue of unauthorised disclosure to third parties – for example, the images obtained from overt surveillance should not be sold, used for entertainment purposes, or given to unauthorised persons. I would suggest that, along the lines of the PPIP Act, there be a specific Principle which addresses disclosures to third parties. This Principle should address when surveillance material may properly be passed to law enforcement agencies.

A particular issue that has recently come to light involves private companies which provide parents with live video footage (via the internet) of their children while attending child care centres. The most active seems to be a Western Australian organisation, Kindercams. This effectively provides information gained by surveillance to third parties (ie. the parents who have internet access), who are not legally associated with the entity conducting the surveillance (the child care centre). The footage will of course not only show the viewer's own child, but other children and staff of the centre.

The schemes raise considerable concerns on a number of fronts (eg. industrial relations issues for staff, and what happens to parents who don't want their children subject to surveillance). However, they raise particular concerns in respect of security (including how does the entity conducting the surveillance ensure that the information in the hand of parents is used for the appropriate purpose and ensure against inappropriate access, for instance, by paedophiles).

It is arguable whether these schemes would be permitted under the four 'purposes' recommended by the Report with respect to Principle 2. The strongest argument in favour of its use would seem to rest on the public interest test. The operators of such schemes may initially market their schemes on the basis that they satisfied this criteria.

However it is my view that such programs represent a significant invasion of privacy (of both the children whose parents are opposed to such a program, and to staff). The proposed legislation provides the opportunity for the government to decide its position on these type of programs before they extend significantly into NSW.

I would therefore argue that there should be a Principle which limits disclosure of footage obtained, along the lines of IPPs 11 and 12 (ss.18 and 19(1) of the PPIP Act), as modified with respect to law enforcement and investigative matters as per ss.23 and 24 of the PPIP Act.

#### An additional Principle – first party access?

The enforceable right to see what information is held about oneself by an organisation – and to seek correction of that information where appropriate - is an important accountability mechanism. Public sector agencies in NSW must already comply with IPP 7 in this regard, which provides:

##### **IPP 7: Section 14. Access to personal information held by agencies**

A public sector agency that 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.

However it should be noted that the current direction issued under s.41 of the PPIP Act 'Direction On Processing of Personal Information By Public Sector Agencies In Relation To their Investigative Function' provides at clauses 3 & 4 that agencies need not comply with IPP 7 if "compliance might detrimentally affect (or prevent the proper exercise of) any of the agency's investigative function or its conduct of any lawful investigations". Therefore, if an agency is conducting an investigation into an incident and this condition is satisfied, then access can be denied. In addition, by virtue of s.20(5) of the PPIP Act, if access could be refused to this information under the FOI Act, then it may also be refused under the PPIP Act.

Many private sector organisations are now likewise obliged to let individuals see the personal information held about them, under the *Privacy Act 1988 (Cwth)*. I would therefore suggest that an additional Principle for Overt Surveillance be introduced with respect to reasonable requests for first party access rights. In particular, public sector agencies must continue to be bound by IPPs 7 (access) and 8 (correction rights) or a provision with an equivalent level of privacy protection. It may however be appropriate to allow 'domestic' surveillance users an exemption to this provision.

In providing 'first party' access, surveillance users will need to ensure they do not inadvertently also disclose information about a third party without their consent.

## Overt surveillance: enforcement and remedies

The complaints and enforcement model proposed by the Report in respect of alleged breaches of overt surveillance is generally based on the model that currently operates in the Anti-Discrimination arena (ie conciliation between parties and appeal to the ADT if conciliation is not successful). It is a different model to that found in the PPIP Act, in which complaints dealt with by the Privacy Commissioner cannot proceed to the ADT. However I understand that the Government is currently reviewing the efficacy of the Anti-Discrimination complaints model.

In light of this I have taken the view that an alternative complaints model, as per that now being considered by Parliament in relation to the Privacy Commissioner's role under the Health Records & Information Privacy Bill 2002, is to be preferred to that outlined in the Report under Recommendations 92-94, 96, 98, and 102.

Such a model would allow for complaints about public sector agencies will be dealt with through the complaints mechanisms already established under the PPIP Act. The complaints mechanisms under the PPIP Act include an internal review by the agency in question, followed by a right to take an alleged breach of the IPPs to the Administrative Decisions Tribunal.

Part 6 of the Health Records & Information Privacy Bill creates a complaints regime for the private sector, establishing Privacy NSW as the main complaints-handling body, providing for this Office to receive, investigate and, where possible, conciliate complaints. Where the Privacy Commissioner concludes that there is a *prima facie* breach of a health privacy principle, an individual will also have the right to take his or her complaint to the Administrative Decisions Tribunal. In determining a complaint, the Tribunal will have the same powers, and the same available remedies, irrespective of whether the complaint is made against a private or public sector body.

The benefit of this model is that Privacy Commissioner will conduct the investigation of a complaint, and where there is a *prima facie* breach will recommend remedies. The respondent is free to comply with or ignore the Privacy Commissioner's recommendations. Only if the complainant is dissatisfied with the outcome of this process will they need to approach the ADT, in which case a copy of the Privacy Commissioner's investigation report may be tendered in evidence by either party.

Therefore the application to the ADT represents a merits review of the respondent's original decision or conduct, not an administrative review of the Privacy Commissioner's decision. This process allows the Privacy Commissioner to remain an independent and non-judicial body, able to make recommendations but not binding decisions.

I furthermore suggest that it be clear that a complaint may be made in relation to the violation of, or interference with, the privacy of any person. This provision is important to allow third party complaints (eg. by whistleblowers) to be dealt with.<sup>9</sup>

---

<sup>9</sup> The equivalent provision in the PPIP Act, s.45(1), is unclear on this point: "A complaint may be made to ... the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual".

## Covert surveillance

### Introduction

The Report suggests that all covert surveillance must be authorised by an independent arbiter, either prior to the surveillance being conducted, or retrospectively. Authorisation can only be given for the purposes of:

- law enforcement,
- protecting the public interest, or
- in the course of employment.

Given the different nature of these purposes, the Report recommends three 'parallel' systems of authorisation, namely:

- law enforcement - law enforcement officers to seek a warrant from a judge;
- protecting the public interest - any person may seek authorisation from a court or tribunal; and
- in the course of employment - an employer may seek authorisation from a judge or magistrate of the Industrial Relations Commission.

The Report furthermore recommends that these requirements not be subverted by allowing 'participant monitoring' without a warrant. That is, even if the person who wishes to conduct surveillance of an activity or conversation is also a party to that activity or conversation, they must seek authorisation as outlined above. I strongly agree with this approach.

However I note at the outset the latest figures available with respect to warrants issued under the *Listening Devices Act 1984*. According to the latest Report tabled in Parliament by the Attorney General, 1,214 warrants were sought through 830 applications by law enforcement agencies in 2000. *Not one* application was refused by the Supreme Court. Nor were any applications refused during 1999, when 1,544 warrants were issued. These figures beg the question as to how genuinely vigilant the Supreme Court is.

The sheer volume of applications is also of concern, especially as the number of warrants is no indication of the number of individuals covered by those warrants. I note that in the entire United States, at both federal and state levels in the year 2000, a total of 1,190 wiretaps were authorised for use by law enforcement officers<sup>10</sup>, and that this figure is higher than the number of occasions in which listening devices are used<sup>11</sup>. That is, wiretaps on telephones are used more frequently than listening devices by law enforcement officials in the USA, and yet the number of wiretap authorisations throughout the USA each year is less than the number of listening device warrants issued in the State of New South Wales alone.

### Law Enforcement Authorisations

I suggest that in relation to law enforcement activities, a covert surveillance authority should only be issued for the enforcement of serious indictable offences, being those with a maximum penalty of 7 years imprisonment or more.

In line with previous submissions by the then Privacy Committee, I submit that Recommendation 25 be changed to only allow Supreme Court judges to issue warrants.

---

<sup>10</sup> EPIC & Privacy International, as above - p. 315.

<sup>11</sup> EPIC & Privacy International, as above - p.57.

## Public Interest Authorisations

I suggest that 'public interest' test ought only be applicable to the news / current affairs media, licensed security operators and licensed private investigators.

I have noted the submissions previously made, prior to and subsequent to<sup>12</sup> the release of this Report, by various media representatives. While I note the media's role in such 'public interest' matters as exposing corruption or financial mismanagement in the public sector, or in highlighting human rights abuses or the conditions in refugee camps for example, I do not believe that the media themselves can define the necessary balance between the 'public interest' in the story and the public interest in the protection of privacy.

A recent example of what I would regard as the inappropriate use of a hidden camera was the covert filming by *A Current Affair* of the interior of the home of Ray Williams, former Director of collapsed insurance company HIH<sup>13</sup>. The story 'angle' - to compare the assets of the company director with that of some of HIH's creditors - could well have been achieved without intrusive and covert filming inside the subject's house.

I furthermore do not accept the view that the small number of complaints to the Australian Broadcasting Authority about breaches of privacy is evidence that the proposed Act is not necessary<sup>14</sup>. In 2000-01, approximately 10% of the privacy complaints finalised by my Office were complaints against media organisations. The lack of a unified system to regulate surveillance no doubt deters many individuals from bothering to complain, or even knowing to whom they could complain, when their privacy has been breached by the media.

I therefore believe that the requirement to seek prior authorisation, as outlined in the Report, for covert surveillance, is appropriate, and will not prevent legitimate public interest stories from being published.

The term 'public interest' however is one which is commonly misunderstood, manipulated, or inconsistently applied. I am therefore concerned that when a person is seeking a covert surveillance authorisation in the name of the 'public interest', there will be no 'counter' viewpoint to argue to the issuing authority in favour of defending the privacy of the subject/s.

In my view it is therefore essential that the proposed Act include a specific definition of the 'public interest', which weighs appropriately the public interest in the protection of privacy as a human right against other interests. In particular, the examples at 6.11 of the Report are appropriate. An emphasis on 'unethical' rather than 'immoral' behaviour (*cf* the Western Australian definition) is also appropriate. Furthermore, this definition could be supplemented by binding Guidelines, made by the Attorney-General under a regulation, on the advice of the Privacy Commissioner. This should ensure that decisions to grant surveillance authorisations are made from the perspective intended by Parliament.

It is submitted that to ensure greatest consistency in the application of a 'public interest' test, the issuing authority ought be the same as for law enforcement authorisations (ie. a judge of the Supreme Court).

---

<sup>12</sup> On this point in particular, see S. Rice, "They'll soon be safe from candid cameras", *Sydney Morning Herald*, 13 June 2002.

<sup>13</sup> See J. Stapleton, "Nine defends 'invasion of privacy' claim", *The Australian*, 30 May 2001.

<sup>14</sup> See note 10, above.

## Employment Authorisations

The Report recommends at 10.19 that covert surveillance in the workplace should only be authorised for one of three purposes:

- where unlawful activity on work premises is reasonably suspected;
- where employment-related unlawful activity, not on work premises, is reasonably suspected;  
or
- where serious misconduct justifying summary dismissal is reasonably suspected.

The Report recognises that the first two items ideally should be matters brought to the attention of the NSW Police for its investigation, but a lack of resources means this is often impractical.

I am therefore concerned with the generality of the term 'unlawful activity' as appears in the first purpose outlined above. There are many behaviours and incidents occurring in the workplace which may represent potential breaches of the law, excluding activity which may represent breaches of industrial law. Clearly some of these activities may be in response to what is perceived by employees to be potential breaches of an award or legislative provisions by employers. However, given the nature of covert surveillance applications, the issuing authority will not be in a position to understand the events and motives behind an employer's application.

For this reason I consider that an issuing authority must be satisfied that if an application is made under the grounds of 'unlawful activity' the employer must be required to establish that they have a legitimate interest in preventing the behaviour, *and* that there is a sufficient explanation for not instead involving NSW Police.

In relation to the appropriate issuing authority, I again believe that consistency would be best achieved by using the same system as for the other categories, ie. a Supreme court judge.

## Issuing authorisations: standard of proof

The ability to obtain a covert surveillance certificate (whatever the category of authorisation or warrant) should be governed by the imposition of a higher standard of proof than that recommended in the Report, since:

- covert surveillance represents a significant violation of privacy;
- the party subject to the surveillance is not able to defend the application; and
- covert surveillance usually captures far more personal information than just that which can be legitimately used under the authorisation, and this excess information can easily be used for other purposes, without much risk of being detected by the issuing authority or the subject of surveillance.

For instance covert surveillance allows law enforcement agencies to gain far more information than a search warrant would allow. For these reasons there should be a presumption against issuing covert surveillance authorisations.

As noted above, the practice at least in the past few years has been for the Supreme Court to not refuse a single application for warrants under the *Listening Devices Act*. A system by which issuing authorities must complete a report reviewing the outcome of the surveillance conducted under each warrant, including making recommendations for the future use / destruction of the material, may focus the minds of those issuing warrants and/or authorisations in the first place. The ability for the Privacy Commissioner to issue guidelines as to what may or may not be considering in the issuing of a warrant or authorisation may also be of assistance in this respect.

## Administrative Requirements

There is no doubt that law enforcement agencies, media representatives and other groups will protest against the amount of 'paperwork' involved in gaining and complying with a covert surveillance authorisation. However, it is important to resist such pressure as this is an essential test to help prevent frivolous and vexatious applications, applications not made in good faith and inappropriate use of the information.

## Retrospective Determinations

I do not believe that the ability to issue retrospective authorisations, as recommended in the Report, is appropriate. Courts will come under considerable pressure to authorise a practice which could only be justified in hindsight, and which would, had it been contemplated beforehand, been properly regarded as no more than a 'fishing expedition'.

Retrospective determinations for public interest and employer conducted surveillance should be limited to situations where the situation was an emergency, in that the covert surveillance was deemed necessary to prevent or lessen a significant injury to one or more persons, or a significant theft or damage to property, and prior authorisation could not have been obtained in time.

## Unauthorised surveillance material

The Report recommends at 9.45 (Recommendation 83) that illegally obtained surveillance material may still be admitted in evidence, under the general and statute law on evidence.

I would suggest that such discretion is inappropriate with respect to material that was not only unlawfully obtained (ie. obtained in the absence of a warrant, 'public interest' authorisation or 'employment' authorisation) but could not have been lawfully obtained in the first place (ie. its purpose was entirely outside the scope of law enforcement, public interest or employment).

If Parliament has set rules about when covert surveillance can never be authorised in the first place, a person who contravenes those rules should not be able to benefit from their crime in any way. To prevent the admission into evidence of illegally obtained surveillance material, where its collection could never have been lawfully authorised in the first place, would also provide greater certainty and relief for the subjects of illegal covert surveillance.

I further note that the Legislative Council, in its report on amendments to the Crimes (Forensic Procedures) Act, has recommended<sup>15</sup> that illegally or improperly obtained material (in that case, forensic material such as DNA samples) ought not be admitted into evidence. I also draw your attention to the discussion of the evidentiary use of improperly gained forensic material in the recent Australian Law Reform Commission Issues Paper on genetic privacy<sup>16</sup>.

## Secondary use and incidental material

The Report effectively allow for what may be called 'secondary use' of information or material gained through covert surveillance.

---

<sup>15</sup> Legislative Council Standing Committee on Law and Justice, *Review of the Crimes (Forensic Procedures) Act 2000*, Report 18, February 2002. See recommendation 51.

<sup>16</sup> ALRC / AHEC, *Protection of Human Genetic Information : Issues Paper*, October 2001, ALRC, Canberra. See Chapter 14 'Evidence' - in particular, 14.2 - 14.13.

In relation to law enforcement authorisations, the Report at 9.50 (Recommendation 84) suggests that material which inadvertently or unexpectedly comes to the attention of law enforcement officers, through their covert surveillance of the subject, could still be admitted into evidence, even if this material was not relevant to the purpose of the warrant as initially authorised. I would suggest that as with the original scope of the warrant for law enforcement purposes, this only be allowed with respect to serious indictable offences.

I agree with Recommendation 82 that there should furthermore be a requirement that prior authorisation be granted before publishing material gained from the surveillance, if the publication of that material was not contemplated by the original authorisation issued for the covert surveillance to be conducted.

For example, if a 'public interest' authorisation was granted to an investigative journalist aiming to expose a corrupt politician, the subsequent publication of material going to the allegation of corruption would not require further authorisation. However such an authorisation should be required if the journalist or media outlet in possession of the surveillance material separately proposes to publish the material in the context of a story about the sex life or fashion sense of the politician's spouse.

#### Restrictions on Gaining Profit or Benefit

As noted above in relation to overt surveillance, restrictions should be imposed to ensure that information gained through covert surveillance is not used to generate profit or benefit, with an exception for the media, and for private inquiry agents and investigators who are paid for the material in the course of their contract.

#### Accountability mechanisms

Given the proposed role for the Privacy Commissioner in investigating complaints relating to both overt and covert surveillance, I would suggest that it is appropriate that the Privacy Commissioner also be the "inspecting authority" as per Recommendation 73 in the Report. To introduce another regulator such as the Ombudsman into the process would only lead to overlapping investigations, a waste of resources, and confusion for surveillance users and subjects alike. However I should also note that, as an independent statutory authority, it is not appropriate for the Privacy Commissioner to be "directed" by the Attorney General to conduct an inspection (Recommendation 75).

#### Enforcement and remedies

As noted above in my initial comments, I approach the proposal to develop a new Surveillance Act as an opportunity to ensure that the privacy principles already binding on NSW public sector agencies, including local and county councils, are not diminished in any way.

The enforcement of and remedies for breaches of the proposed Surveillance Act must also be consistent with, or at least no less stringent (in terms of enforcement) or expansive (in terms of remedies) than already exist under the PPIP Act.

#### *Ability to prosecute criminal breaches of covert surveillance*

The Report suggests that breaches of covert surveillance ought be subject to criminal sanctions.

The three type of breaches that are most likely to occur are:

- persons conducting covert surveillance without an authorisation;
- persons not complying with or exceeding the powers provided by the authorisation (eg. continuing beyond the authorised surveillance period); or
- persons using or disclosing information, gained during legitimate covert surveillance, for a purpose which was not authorised.

In my view, based on experience with the Listening Devices Act and the Workplace Video Surveillance Act, there are likely to be very few cases where successful prosecutions occur.

The very fact that the surveillance in question is covert means that breaches will only be detected if the subject of the surveillance discovers or is told of their surveillance, if the issuing authority realises that orders have been breached, or if the inspection authority detects the breach. Once detected, a law enforcement body must be willing to investigate and pursue criminal prosecution. It is unlikely, in my view, that issuing authorities will do so except in the most extreme cases, and questions are also raised as to whether the NSW Police would likely investigate breaches involving fellow officers.

As well, there are many factors impinging on the law enforcement and prosecution bodies which will mitigate against prosecutions being commenced or concluded (ie. workload and other priorities of the investigating authority, the likelihood of successful prosecution, and the criminal standard of proof).

It is therefore questionable whether the threat of criminal sanctions will act as a deterrent by major users of covert surveillance, who will be aware of the inherent difficulties in mounting prosecutions. Breaches of the covert surveillance provisions will usually present a much greater violation of the subjects' privacy than a breach of the overt surveillance principles. Despite this, the subject of the surveillance will have no recourse to any personal redress, a remedy which is available to subjects of overt surveillance.

#### *Civil remedies*

I therefore strongly support Recommendation 105 (see the discussion at 10.38 of the Report) that subjects of unlawful covert surveillance should have the same rights to gain a civil remedy as would subjects of unlawful overt surveillance. I do not believe that it is unreasonable that the covert surveillance operator is potentially subject to both a criminal and civil penalty.

I also consider that a person subject to covert surveillance should be able to seek a civil remedy if it can be subsequently established that an application for covert surveillance was not made in good faith.

It is also my view that, in order to streamline the administration of civil remedies arising from infractions of covert orders, the issuing authority should be empowered to determine remedies, rather than require the subject of the surveillance to take action through the process outlined in the Report. The issuing authority would be fully cognisant of the issues involved and would be in a position to make such decisions. However, it should be permissible for the issuing authority to refer the matter as a complaint to the Privacy Commissioner if they considered that this was a preferable course.

#### *Disclosure to Subjects of Covert Surveillance*

In my view the Report's conclusion in respect of disclosure to the person subject to the surveillance is unsatisfactory. The Report suggests that the subject of covert surveillance should only be made aware that surveillance has occurred by one of three means:

- as a result of an order by the issuing authority (see Recommendation 80);
- as a result of a decision of the inspection authority (eg. where it was considered that the agency had breached the conditions of the authority); or
- through proceedings commenced as a result of the surveillance, in which the material gathered through surveillance shows up as evidence.

I understand that under the Workplace Video Surveillance Act and the Listening Devices Act it is possible for courts to order that the surveillance subject be made aware that surveillance has occurred. I further understand however that there have been very few, if any, orders made in this regard.

The subjects of covert surveillance who do not later become aware that surveillance had occurred would be substantially denied their privacy rights. In addition they would be unable to determine if the surveillance was carried out in accordance with any orders made by the issuing authority. This would include situations where the surveillance material was never used, or was used in such a way that the person did not know that it had been gained from covert surveillance.

I find it difficult to accept that whether or not subjects become aware of covert surveillance having taken place ought be a matter of luck or circumstance. In my view subjects of covert surveillance should have the right to know that such surveillance has taken place. Of course, there would need to be exceptions such as if disclosure would jeopardise the health and safety of identifiable people, or compromise ongoing investigations by law enforcement agencies.

It is therefore my strong view that there should be a 'right to know'. There are three major reasons for this:

1. While issuing authorities are well able to adequately determine many issues in respect of applications there are two essential issues that they cannot adequately assess:
  - whether the stated reasons for the surveillance were made in good faith. As the application is *ex parte*, the issuing authority can never really test the veracity of the reasons and evidence put forward by the applicant; and
  - whether the use of the information or material was in accordance with the stated purpose. Organisations may be tempted to use the information gained as a result of the surveillance for many other purposes, and well after the surveillance period has ended. The issuing authority has only a limited capacity to know this, and must rely on the statements made by the applicant. Much of this information can be extremely personal and damaging. The subject of the surveillance is the only person who is in a position to determine if the information gathered in covert surveillance has been used for its intended purpose.
2. The fact that applicants knew that their surveillance activities would later be made known to the subject of surveillance would prevent vexatious and borderline applications from being lodged in the first instance.
3. If it was accepted that civil remedies should be available for breaches of covert surveillance then these cannot be pursued if a person is not aware that covert surveillance has occurred. It would only be available for those who became aware that covert surveillance had occurred.

There should therefore be a general right of access to information by the first party, which must be facilitated by first making the person aware that surveillance material actually exists. The enforceable right to see what information is held about oneself by an organisation – and to seek

correction of that information where appropriate - is an important accountability mechanism. Public sector agencies in NSW must already comply with IPPs 7 and 8, as outlined above in relation to overt surveillance practices, while many private sector organisations are now likewise obliged to let individuals see the personal information held about them, under the *Privacy Act 1988 (Cwth)*.

I note in particular that the United States has incorporated this practice into its covert surveillance program for many years, as a way of protecting civil liberties. I understand that this has been in place for some years, without causing undue concern about difficulties for law enforcement officials. I have outlined below how I consider the right to disclosure could be incorporated into the decision making of the issuing authority, and in particular with reference to the procedures for destruction of information.

I do however accept that a general presumption in favour of notifying the subject is not appropriate with respect to law enforcement warrants. The following comments therefore relate only to 'public interest' and 'employment' authorisations.

#### *When should the subject be informed*

Decisions about when the subject of covert surveillance should be informed that covert surveillance material about them exists ought be dependent on a number of factors, the most important of which is the type of investigation being undertaken.

Material gained through surveillance conducted on public interest grounds should generally be disclosed to the subject of that material prior to the material being used. This would provide the subject with the ability to seek injunctive relief, to defend the use of the material prior to its publication.

Disclosure to the subject of material gained through surveillance conducted on law enforcement or employment grounds would not necessarily have to occur until after the information was used (eg. at the time it is sought to be used in evidence). However where the information gained from covert surveillance is not to be used (eg. a decision is made not to prosecute), disclosure to the subject should be made immediately after that decision is taken, or at the latest, before the time that the information is to be destroyed.

The issuing authority could determine when disclosure should be made as part of its original authorisation, or at the time of the 'reporting back' required as per Recommendation 69.

#### *What the subject should be informed about*

The surveillance user should be required to include, as part of any disclosure to the subject of the surveillance, a copy of all applications for authorisation, any orders made by the issuing authority, any other documents prepared by the issuing authority, and the material gathered through the surveillance.

#### *Destruction of surveillance material*

I agree with Recommendation 87 in respect of the destruction of surveillance material, although given my comments above regarding the accountability of surveillance users I suggest that prior to the destruction of the information, the surveillance user should be required to prepare documentation for presentation to the issuing authority. Included in the documentation should be:

- a statement advising that documents obtained under an authority are going to be destroyed;
- any reasons why the subject of the surveillance should *not* be advised that covert surveillance has occurred or that such an order has already been made;

- any information which is required to be retained;
- a copy of the documents necessary for disclosure to the subject, or a statement to the effect that these have previously been issued to the subject; and
- a declaration that there are no outstanding matters in relation to any actions or likely actions by the subject of surveillance in respect of the surveillance or any other judicial processes.

If there are objections to advising the subject then the issuing authority could make a decision *ex parte*. Otherwise the issuing authority should then send the information to the subject with a letter advising that the information will be destroyed within X days unless the person can show just cause why the information should not be destroyed. In this respect, 'just cause' could be that the person required the information as evidence for the purpose of seeking a legal remedy against the surveillance user.

These principles should apply equally to surveillance material that was illegally obtained.

### **Other comments**

I merely seek to raise for future discussion the following matters:

- In drafting the Act, it should be made clear whether information or material arising from surveillance is to be excised from the definition of 'personal information' in the PPIP Act (as for example health information will be, under the provisions of the Health Records & Information Privacy Bill 2002). If not, the IPPs, offence provisions and remedies in the PPIP Act will still apply to information gathered via surveillance by public sector agencies, and by virtue of s.25 of the PPIP Act, non-compliance with the IPPs will only be authorised to the extent that such compliance will be authorised, necessarily implied or reasonably contemplated by the Surveillance Act.
- The introduction of the proposed Act will require adequate resourcing of both Privacy NSW and the Administrative Decisions Tribunal.

### **Conclusion**

I strongly support the overt-arching recommendations of the Report, in relation to the development of a comprehensive Surveillance Act which is technology-neutral in its application. I am however concerned to ensure that the proper balance is struck between the public interest in the protection of individuals' privacy on the one hand, and the public interest in law enforcement and public safety on the other.

In particular I trust that the privacy principles already binding on State and local government in NSW will not be diminished in any way through any new legislation.

## **Privacy NSW**

Office of the NSW Privacy Commissioner  
PO Box A123  
Sydney South NSW 1235

Phone (02) 9268 5588  
Fax (02) 9268 5501  
TTY (02) 9268 5522

[www.lawlink.nsw.gov.au/privacynsw](http://www.lawlink.nsw.gov.au/privacynsw)

Reference: AD08-2002-02

© Privacy NSW June 2002