Covert surveillance in Commonwealth administration: Guidelines

February 1992


Contents

1. Overview
   What is covert surveillance? 1
   Why is covert surveillance privacy intrusive? 2
   Public interest justification for covert surveillance 2
   Extent of use of covert surveillance by Commonwealth agencies: Current practice 3
   Need for controls 4
   Statutory and administrative controls on covert surveillance activities 5
   Application of Privacy Act 1988 to the use of covert surveillance by Commonwealth agencies 6
   Scope of application of the guidelines 7

2. Guidelines Part One: General guidelines for the conduct of covert optical surveillance 8
   Decision to undertake covert surveillance 8
   The conduct of the covert surveillance operation 9
   Handling of records arising from covert surveillance 10

3. Guidelines Part Two: Specific guidelines for the conduct of covert surveillance by optical means when used for the surveillance of claimants for compensation 11
   Determining the necessity for conducting covert surveillance 11
   Application to conduct covert surveillance 12
   Approval to conduct covert surveillance 13
   The collection process 14
   Use and disclosure 14
   Storage and security 15
   Monitoring 15

Appendix 1: Technological developments 16
Appendix 2: The Privacy Act 17
Appendix 3: Glossary of terms 18

1. Overview

What is "covert surveillance"?

Covert surveillance usually refers to:

*The secretive, continuous or periodic observation of persons, vehicles, places or objects to obtain information concerning the activities of individuals which is then recorded in material form including notes and photographs.*
The activity is sometimes a routine feature of a particular environment, and takes place on a random, non-selective basis: anyone who enters the environment under surveillance is monitored. Typical examples of this type of covert surveillance apply in business premises (and in some instances the existence of surveillance equipment is not hidden).

The form of covert surveillance which is usually of greater risk to individual privacy is targeted and selective covert surveillance. This occurs where a particular individual or group of individuals is placed under direct surveillance. In official settings typically this occurs in association with the enforcement of the law. Covert surveillance is also widely used, it would seem from press reports, by private inquiry agents sometimes to assist in insurance matters, often in relation to matrimonial and business disputes.

Covert surveillance can range from discreetly watching a person's activities by listening in to his/her conversation without the use of technical assistance or by relying on the most sophisticated technology. The availability of specialised technology has led to an increase in covert surveillance activity in recent years.

Why is covert surveillance privacy intrusive?

Covert surveillance is privacy intrusive because not only is information about an individual collected without that individual's consent or authority but the individual who is subject to the covert surveillance is usually unaware that he or she is under surveillance.

The Australian Law Reform Commission (ALRC) in its 1980 Discussion Paper on Privacy and Intrusions noted that:

"...the intentional surveillance of an individual's activities or conversations can have a corrosive effect on his sense of privacy and is generally considered as a serious affront to the integrity of the individual subjected to this practice."

Another major privacy concern about the conduct of covert surveillance is the extent to which this activity may impinge on the privacy of other people who come into contact with the surveillance subject during the surveillance period. These may include relatives, friends or any other person who may inadvertently become subject to the covert surveillance.

Public interest justification for covert surveillance

Covert surveillance plays a useful role in gathering evidence in connection with a wide range of possibly unlawful activities. It is argued by a large number of agencies that covert surveillance should continue to be allowed unhindered in the public interest.

The public interest ought, however, to be balanced against an individual's basic right to privacy. As indicated earlier, the use of covert surveillance is inevitably privacy intrusive and has the potential for impact on individuals.

In formulating these guidelines, the Privacy Commissioner recognises that there are a number of agencies where additional detailed guidelines governing most of their covert surveillance activities would not be appropriate because of the nature of their operations and existing safeguards.

These include:
• Law enforcement agencies such as the Australian Federal Police, Australian Defence Forces Service Police and Australian Customs Service (law enforcement arm), which use covert surveillance as a routine investigative technique in carrying out their law enforcement functions. These agencies are required to comply with strict internal instructions and are subject to disciplinary action for any breach. In the case of the AFP, for example, breaches are subject to the Australian Federal Police Disciplinary Regulations.

• Agencies which use untargeted optical surveillance as part of normal security arrangements, e.g. for after hours security or to protect stores from theft.

While Commonwealth agencies undertake a wide range of investigations which may use covert surveillance as an investigative tool, one area which affects all agencies involves the investigation of disputed compensation claims. Compensation cases have been singled out as they have been subject to public controversy. The purpose of conducting covert surveillance is to observe an individual's activity relating to health. As such, the technique is not only particularly privacy intrusive, the covert surveillance procedure can be all pervasive in that it may involve surveillance of every aspect of an individual's life.

In acknowledging the different uses of covert surveillance by agencies, the Privacy Commissioner has decided to issue general guidelines for uses by agencies using covert surveillance for purposes other than investigation of compensation claims and specific guidelines for the guidance of agencies conducting covert surveillance in compensation cases.

Extrem of use of covert surveillance by Commonwealth agencies: Current practice

At present, a number of Commonwealth agencies undertake covert surveillance. The use of this activity is largely limited to optical surveillance, with the exception of law enforcement agencies and Telecom. Law enforcement agencies conduct covert surveillance under warrants issued for both optical and telephone surveillance in accordance with various Acts of Federal Parliament. Telecom monitors telephone calls (not conversations) in cases of nuisance calls, telephone vandalism and disputed metered calls (using charge record devices).

Agencies use covert surveillance for investigating a wide range of activities. Examples are:

• investigation of suspected fraudulent claims made by doctors and other health care providers

• investigation of suspected immigration offences including the location of illegal immigrants and of "safe" houses and factories

• investigation of suspected fraudulent claims made by clients

• investigation of claims made in relation to compensation cases or for settling disputed claims in the Administrative Appeals Tribunal. The material collected in these cases may not necessarily be used in court but used as evidence to settle out of court

• investigation of suspected employee theft of a widespread kind within an establishment

• investigation of repeated theft, vandalism or interference in public and outdoor location; e.g. payphones and vehicle parking areas.

This list of activities for which agencies use covert surveillance is by no means comprehensive.
The employment of this practice varies considerably amongst agencies and, in general, most agencies conduct covert surveillance infrequently. One agency has used this technique a few times in the past three to five years. However, another agency reported employing this technique weekly. More specifically (but not exhaustively) it is understood that the following agencies employ covert surveillance:

- the Australian Customs Service advised of its own policies for the training of officers in covert surveillance practices and the management of covert surveillance action. It is used in combating fraud and intercepting prohibited goods, in particular, illicit drugs
- the Australian Tax Office has an investigations unit set up to investigate alleged fraudulent activities which uses covert surveillance among other techniques
- the Department of Social Security occasionally uses covert surveillance to investigate instances of suspected fraud
- the Health Insurance Commission uses covert surveillance `as a last resort' and has employed it on an infrequent basis
- the Department of Immigration, Local Government and Ethnic Affairs (DILGEA) advised that on occasions it needed to resort to covert surveillance to investigate migration offences as well as allegations against DILGEA staff
- the Department of Primary Industries and Energy undertakes covert surveillance activities for the purpose of detecting breaches of quarantine regulations
- the Department of Veterans' Affairs has an investigations unit which among other techniques uses covert surveillance to investigate instances of alleged fraud
- Comcare undertakes covert surveillance to investigate suspected fraudulent compensation claims as do compensation self-administers under the Commonwealth Employees' Rehabilitation and Compensation Act, 1988, viz., the Australian Postal Corporation and the Australian Telecommunications Organisation.

**Need for controls**

The ALRC recognised in its 1980 Discussion Paper that:

>"..technological developments have given rise to sophisticated devices which render it virtually impossible for the ordinary person to take effective measures against the use of technological devices. The ancient statutory offence of peeping and the common law crimes of eavesdropping sought to restrain deliberate surveillance. But each of these were created long before the modern development of sense-enhancing technical devices. As the law currently stands there is insufficient legal protection against the use of these devices. They have proliferated. The law has not kept pace."

The ALRC went on to report the lack of controls under Australian law over forms of surveillance employing technical devices other than electronic listening devices. After examining new means of surveillance and conducting a review of overseas laws and experience the Commission concluded that a case could be made for controlling the use of optical devices. Australia's major national
communication networks, i.e. the mail and telecommunications systems, are already subject to strict legal prohibition against surveillance in that warrants need to be obtained from the appropriate legal authorities in order for covert surveillance to be undertaken.
Additionally the ALRC's Report No 22, Privacy, tabled in Parliament in 1983, noted that there was no logical reason for limiting the protection afforded to an individual to aural surveillance, and that in some ways secret optical surveillance of activities that are intended to be carried out in private is more offensive than eavesdropping on private conversations.

The ALRC also examined the use of covert surveillance by law enforcement agencies and recommended:

"The use by law enforcement agencies of surreptitious listening and optical devices should normally be permitted for very serious offences."

To provide a clear criterion, the ALRC suggested that aural and optical surveillance (not including surveillance of mail and telecommunications) should only be permissible in the case of the investigation of offences attracting a maximum penalty of not less than three years imprisonment.

The ALRC also recommended that consistent with aural surveillance, optical surveillance should be permitted, if carried out under the authority of a judicial warrant. That is, the regime adopted in relation to the use of listening devices should be adopted to cover the use of optical devices.

Since these ALRC reports of the early 1980s, technological developments have vastly improved with the introduction of highly sensitive electronic equipment capable of performing a range of tasks unimagined at the time the above reports were written.

**Statutory and administrative controls on covert surveillance activities**

At present, the use of **listening devices** is regulated by:

- *Telecommunications (Interception) Act 1979*
- *Customs Amendment Act 1979*
- *Australian Federal Police Act 1979*
- Various state laws in all states.

The use of **locational devices** (see Appendix One) is subject to and controlled by the law of trespass which in effect limits the unlawful use of the device for covert surveillance purposes.

**Interference with mail** is regulated by the *Crimes Act 1914*, by virtue of the *Telecommunications and Postal Services (Transitional Provisions and Consequential Amendments) Act 1989*; and the *Australian Security Intelligence Organisation Act 1977*. The ASIO Act enables the Director-General of that organisation to obtain a warrant to inspect postal articles.

The protection given by the laws against covert surveillance of postal and oral communications has not been extended to **optical surveillance** of personal activities, despite the Australian Law Reform Commission's recommendations and despite the potential for breaches of privacy posed by the vast range of technological devices available. Provided one can avoid breaching the law of trespass, Australian law does not prevent people from using optical devices to monitor private activity.

By way of overseas contrast, in Canada and North America:

- In **Canada**, the law does not regulate wiretapping or invasion of privacy through the use of cameras or sound recording devices. Privacy protection against electronic monitoring and surveillance is not explicitly covered in the Canadian Privacy Act.
• In the **United States of America**, the Constitution protects communications by an individual or business only against governmental action. In reality these federal constitutional provisions afford only limited privacy protection against electronic surveillance by government agencies. However, some state constitutions, have explicit protections of privacy that provide more protection than the US Constitution.

Agencies which have supervisory guidelines in place include:

• the Health Insurance Commission, which undertakes covert surveillance investigations very infrequently. Covert surveillance is used primarily to investigate fraudulent servicing claims by doctors. The Commission has brief guidelines already in place which require approval of covert surveillance to be given at a very senior executive management level.

• Australia Post, which has developed guidelines which largely reflect these revised draft guidelines in terms of its covert surveillance activities under *the Commonwealth Employees' Rehabilitation and Compensation Act 1988*.

• Comcare, which has its own guidelines which address factors that need to be considered when undertaking covert surveillance in relation to compensation claimants.

**Application of Privacy Act 1988 to the use of covert surveillance by Commonwealth agencies**

Where covert surveillance results in the creation of some kind of record of personal information concerning an individual, the activity, if undertaken by Commonwealth agencies is regulated by the Privacy Act. In the situations where covert surveillance does not lead to the creation of a record, agencies, while not bound to comply with the Privacy Act, are encouraged to adopt the following guidelines where relevant.

In those cases where covert surveillance is used to collect personal information about the activity of an individual and it results in the creation of a record, the practice is governed by Information Privacy Principle (IPP) 1 and 3 of the Privacy Act. These principles apply regardless of whether the individual is aware of the collection. IPPs 1 to 3 deal with standards that should be observed by Commonwealth agencies when collecting information. IPP 2 deals with solicitation of information from the individual concerned and the need to notify the person in relation to the purpose of the collection, the authority of the collection and any usual disclosures. This will not generally apply because of the nature of the activity.

IPP 1 states that:

"1. **Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:**

(a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

(b) the collection of the information is necessary for or directly related to that purpose.

2. **Personal information shall not be collected by a collector by unlawful or unfair means.**"
IPP 3 states that:

"Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principles 1 and 3 clearly apply to collections leading to the creation of records. IPP 1 (a) refers to the need for information to be directly relevant to the functions of the collector while IPP 1 (b) stresses the need for information collected to be necessary for the purpose for which it is collected. However, the principle of most relevance to covert surveillance is IPP 1 (2) which states `Personal information shall not be collected by a collector by unlawful or unfair means'. Whilst IPP 3 paragraph (d) does not strictly apply it ought nevertheless be borne in mind. It states that the record collector shall take such steps to ensure that `the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.'

IPP 4, which concerns storage and security of personal information, also needs to be observed in conducting covert surveillance. This principle covers the way that records are to be safeguarded and how precautions should be taken to ensure that unauthorised access, use and disclosure of recorded information is prevented.

IPPs 10 and 11, which govern use and disclosure of personal information address the important consideration that information obtained by means of covert surveillance is not generally to be used or disclosed for a purpose other than that for which it was collected.

The Privacy Act has been in operation for over three years now and it has become clear from training sessions on the implementation of the Act and from inquiries from the general public that guidance on the way the Privacy Act affects the conduct of covert surveillance is desired.

These guidelines are intended to clarify the standards that need to be met to satisfy the requirements of these principles and specifically the requirement that information not be collected by unfair means.

Scope and application of the guidelines

The guidelines are of a general advisory nature. They are intended to provide a framework for agencies to develop their own detailed guidelines taking into account their role, their priorities and other operational factors, when conducting covert surveillance.
The first set of guidelines are intended to be followed by Commonwealth agencies conducting covert surveillance by optical means, the results of which are then recorded in either a material form - for example, notes made during or after the surveillance activity, or in some other form. Optical means includes photography, video cameras or direct observation (including the use of binoculars). The guidelines are relevant to any non law enforcement agencies conducting covert surveillance in the course of performing their statutory functions.

Agencies not affected by these guidelines are national security organisations and agencies using covert surveillance for law enforcement purposes.

The second set of guidelines is intended to be followed when covert surveillance is used for the surveillance of claimants for compensation under the Commonwealth Employees' Rehabilitation and Compensation Act 1988.

For both parts, the bold type face denotes actual guidelines. Unbolded text seeks to provide additional interpretative assistance.

The guidelines have been issued following extensive consultations. The cooperation of Commonwealth agencies in the consultation process and in preparing the guidelines is gratefully acknowledged.

Guidelines Part One: General guidelines for the conduct of covert optical surveillance

[For a definition of the term "covert surveillance" please refer to Appendix 3 at the back of this document.]

Limitation to optical surveillance guidelines: The guidelines are limited to optical surveillance activities because whilst there is a fairly comprehensive body of legislation dealing with aural, postal and telecommunications surveillance devices, there is no law dealing with optical surveillance devices.

Adoption: These guidelines are of an advisory nature and are intended to provide a framework for agencies to develop their own guidelines taking into account their role, their priorities and other operational factors, when conducting covert surveillance for statutory investigations.

Not affected: National security organisations and agencies who use covert surveillance for law enforcement purposes.

Agencies in preparing their guidelines for conducting covert surveillance by optical means should consider the following:

Decision to undertake covert surveillance

IPP 1 requires that information shall not be collected unless the purpose is lawful and directly related to a function or activity of the collector and the collection is necessary or directly related to the purpose. It also states that collection shall not be by unlawful or unfair means.

Purpose of Covert Surveillance
1.1 Covert surveillance may only be undertaken for a lawful purpose which is related to the function and activity of the agency.

1.2 Each agency should identify the circumstances or offences for which covert surveillance may be used and the Acts which may justify the agency undertaking the practice.

Examples include:

- surveillance of healthcare providers suspected of fraud in claiming payments for services provided under the Health Insurance Act 1973 or the Veterans' Entitlements Act 1986
- surveillance of suspected illegal immigrants under the Migration Act 1958
- surveillance of staff suspected of theft under the Crimes Act 1914.

Decision-maker

1.3 Approval to conduct covert surveillance in any particular case should be made at a senior level, taking into account procedures in place for the conduct of such activities.

Criteria for decision

1.4 In deciding to conduct covert surveillance agencies should consider the following factors:

(a) That there be reasonable suspicion to believe that an offence or an unlawful activity is about to be committed, is being committed or has been committed

(b) That other forms of investigation have been considered and have been assessed to be unsuitable, or other forms of investigation have been tried and have found to be inconclusive or unsuitable

(c) The benefits arising from obtaining relevant information by covert surveillance are considered to outweigh to a substantial degree the intrusion on the privacy of the surveillance subject/s.

Where considered appropriate by agencies the Commonwealth Director of Public Prosecutions or other legal advisers should be consulted concerning the desirability or necessity of obtaining information by covert surveillance.

The conduct of the covert surveillance operation

IPP 1 imposes obligations on Commonwealth Agencies relating to the collection of personal information. Collection must be fair and lawful. The information collected must be for a lawful purpose which is directly related to the function or activity of the agency and the collection of information must be necessary for or directly related to that purpose.

In order to comply with these obligations agencies should be mindful of the following:

2.1 The collection of personal information using a covert surveillance operation should be conducted in a lawful manner. Any covert surveillance operation which may involve the
commission of a criminal offence or which may give rise to civil action, for example, trespass to lands or goods cannot be sanctioned.

2.2 The collection should not involve entrapment of the surveillance subject. Hence, passive observation is permissible, however, any attempts to actively induce the surveillance subject into a situation in which that person would not ordinarily and voluntarily enter should not be permitted. For example, whilst an investigator could pose as a patient in cases of investigations for overservicing by a doctor to afford an opportunity for the doctor to commit a crime if the doctor is so minded, the investigator should not induce a doctor into a crime the doctor is otherwise unwilling to commit.

2.3 Agencies should avoid any actions which may unreasonably impinge on the privacy and rights of other people, e.g. when using photography, avoid, where practicable, including other individuals such as relatives and friends in the photograph.

2.4 Where practicable only material relevant to the purpose of conducting the covert surveillance should be collected. There should be a clear separation of facts from opinions and only relevant personal information should be included in records resulting from the surveillance.

Handling of records arising from covert surveillance

Security

IPP 4 requires agencies to protect information with reasonable security safeguards against loss, unauthorised access, use, modification or disclosure; and other misuse. If it is necessary for the record to be given to a person who is providing a service to the agency, then everything which is reasonably within the power of the agency, must be done to prevent unauthorised use or disclosure of information.

Clear instructions on obligations of investigators to safeguard the material collected should be developed by agencies. Agencies should include confidentiality clauses in contracts when employing private investigators.

Access and correction

IPP 6 concerns access by individuals to their personal information. Individuals are entitled to have access to their files unless a specific provision of a law of the Commonwealth refusing such access applies. In general, the Freedom Of Information exemptions will often apply.

IPP 7 concerns an agencies obligations to ensure that the quality of data is maintained by seeing that it remains relevant and is tested for accuracy, is up-to-date, complete and not misleading. This IPP also provides for individuals to attach to records any statement relating to the correction, deletion or addition they consider should be made to the personal information on that record.

Use and disclosure

IPPs 8 and 9 require agencies to:

- check that information is accurate, up-to-date, complete and relevant prior to using it.
In order to comply with the requirements of IPP 8 agencies will need to consider tests for accuracy of information prior to use. These tests would need to be appropriate to each agencies' specific operations. (For example, how long ago the information was collected, how often it was collected, and the general relevance of historical data - whether the information is up-to-date or not.)

IPP 10 limits the use of personal information. Agencies may not use personal information for purposes other than those for which it is collected unless one of the five exceptions apply.

To comply with this requirement agencies should be aware of the exceptions which authorise use of material collected by covert surveillance for purposes other than the purpose for which the material was collected. In particular agencies should note exception (e) in IPP 10.1, which authorises the use of information where "the purpose for which the information is used is directly related to the purpose for which the information was collected". Agencies should observe IPP 10.2 which requires that agencies keep a note of the uses of particular records where the information has been used for enforcement of the criminal law or a law imposing a pecuniary penalty or for the protection of the public revenue. IPP 11 limits disclosure of information outside an agency unless one of the five exceptions apply. IPP 11.2 requires agencies to keep a note of records that are disclosed for the enforcement of the criminal law or a law imposing a pecuniary penalty or for the protection of the public revenue.

Hence material collected by covert surveillance should not be disclosed to any person, body or agency other than in accordance with the IPPs. Agencies should be cognisant of the exceptions which authorise disclosure of information.

It is recommended that safeguards be in place to ensure that, where information is disclosed according to the IPPs, the information is only used or disclosed for the specific purpose for which it was collected. Agencies could consider formal agreements or memoranda of understanding with persons or agencies to whom information is disclosed.

Agencies should also be aware of any relevant secrecy provisions within their enabling legislation.

**Retention and destruction**

No IPP directly applies here and the Archives Act is the principal control but the Privacy Commissioner reserves power to give advice on those matters if pertinent to security under IPP 4. It should be noted that information that is unnecessarily kept could be in breach of IPPs 7, 8, or 9.

**Monitoring**

Agencies should consider incorporating regular monitoring procedures on covert surveillance practices in their reviews of operational procedures/instructions. The Privacy Commissioner has powers under section 27 1 (h) of the Privacy Act to conduct audits of agencies. (Further information on this is available in the Privacy Audit Manuals 1 and 2.)

**Guidelines Part Two: Specific guidelines for the conduct of covert surveillance by optical means when used for the surveillance of claimants for compensation**
These guidelines apply to the use by Commonwealth agencies of covert surveillance by optical means in cases involving compensation claims under the *Commonwealth Employees’ Rehabilitation and Compensation Act 1988*.

1. **Determining the necessity for conducting covert surveillance**

1.1 Prior to undertaking covert surveillance the agency should assess the need to use this technique. Covert surveillance should only be used:

    (a) When other less intrusive methods of investigation have been considered and have been assessed to be ineffective and inadequate; or have been tried and the outcome found to be inconclusive.
(b) When the claim is of such a nature as to warrant the use of covert surveillance and when there is adequate evidence to suggest that the claimant may be:

- misrepresenting his/her disability,
- claiming excessive disabilities,
- malingering, or
- involved in the commission of a fraud.

1.2 Where the benefits arising from obtaining relevant information by covert surveillance are considered to outweigh to a substantial degree the intrusion on the privacy of the surveillance subject.

1.3 Where, if appropriate, the Australian Government Solicitor or other legal advisers have been consulted concerning the desirability or necessity of obtaining information by covert surveillance.

2. Application to conduct covert surveillance

IPP 1 imposes obligations on Commonwealth agencies relating to the collection of personal information. Collection must be fair and lawful. The information collected must be for a lawful purpose which is directly related to the function or activity of the agency and the collection of information must be necessary for or directly related to that purpose.

2.1 An application to conduct covert surveillance should be in writing, and include a clear statement on the following:

(a) The purpose for the covert surveillance i.e. document the basis in terms of 1.1 (b) above.

(b) The name, address, and other relevant details of the surveillance subject, including:

- the personal characteristics of the surveillance subject to minimise the risk of misidentification
- a description of the surveillance subject's premises e.g. a particular office location or building.

(c) The nature and details of the claim e.g. muscular-skeletal injuries.

(d) The kind of information to be collected by covert surveillance, including:

- the performance of physical activities that may indicate that the individual concerned is making a false claim e.g. ability to lift objects known to be very heavy.

(e) Whether alternative investigative methods have been considered/undertaken to obtain the information required and the results, if any, of these investigations.

Alternative methods may include:

- interviewing claimants
- interviewing witnesses
- reviewing agency records
- reviewing claimant's records.

(f) The relative cost/benefits of undertaking or not undertaking the surveillance, for example:

- an estimate of the financial or other resource costs of the surveillance
- whether the amounts involved in a worker's compensation claim warrant the costs involved in the covert surveillance.

(g) Particulars of the investigator undertaking the surveillance

i.e. whether the covert surveillance is to be conducted by:

- departmental investigators
- contract private investigators.

(h) Whether the procedure has been recommended by the Australian Government Solicitor or relevant legal advisers.

(i) The method by which information is to be collected, for example:

- by photography
- by video recordings
- by recording of observations in a log
- by combinations of the above.

(j) The period and scope of the surveillance, including:

- surveillance period e.g. daily
- surveillance dates
- activities to be observed, e.g. gardening, lifting, shopping
- whether the surveillance is to be confined to the domestic environment or extended beyond the claimant's premises.

3. Approval to conduct covert surveillance

Covert Surveillance should normally be approved in writing on a case-by-case basis, at a senior level in the agency following a written application.

3.1 Approval to conduct covert surveillance in a particular case is only to be given by senior officers at an appropriate management level.

3.2 Approval is to be issued for a limited time only, as follows:

(a) The period of surveillance should be appropriate to the circumstances of each case, but should not extend beyond 30 continuous days. This period may be extended when there is difficulty locating the claimant.

(b) A new application should be made to extend or recommence covert surveillance after the expiry of the initial approval.
4. The collection process

4.1 Covert surveillance should be undertaken by trained investigators/surveillance officers. Strict instructions on the conduct of covert surveillance should be issued to the surveillance officers. Points (a) to (d) are of a general nature whilst (e) and (f) are case specific. The instructions should cover:

(a) Avoidance of any actions which may unreasonably impinge on the privacy and rights of other people, e.g. when using photography, avoid, where practicable, including other individuals such as relatives and friends, who may be in contact with the surveillance subject during the surveillance period, in the photograph.

(b) Where practicable only material relevant to the purpose of conducting the covert surveillance should be collected. There should be a clear separation of facts from opinions and only relevant personal information should be included in records resulting from the surveillance.

(c) Instructions on the manner of collection of personal information.

- the collection should not involve the commission of a criminal offence or give rise to a civil action, for example, trespass to land or goods

- the collection should not involve entrapment of the claimant. Hence, passive observation is permissible, however, any attempts to actively induce the claimant into a situation in which that person would not ordinarily and voluntarily enter, thereby creating a false or misleading impression of the person's disabilities, should not be permitted.

(d) Instructions by agencies on obligations of investigators to safeguard the material collected. Agencies should include secrecy provisions in contracts employing private investigators.

(e) The method by which information is to be collected e.g. photography, video recordings or logs with observations recorded. This should be appropriate to the purpose of collection in the particular case.

(f) The period and scope of the surveillance procedure as specified in 2.1 (j).

5. Use and disclosure

5.1 Material collected by covert surveillance is to be used in accordance with the following conditions:

(a) The material is to be used only for the purpose for which the approval described under 3.1 is given, or where exceptions under IPP 10 apply, and

(b) Each agency should ensure that information is accurate, up to date and complete prior to the information being used. Material collected by covert surveillance should not be used in isolation but corroborated by other information to ensure accuracy.

Tests for accuracy may include:
- identity check, i.e. name and address of surveillance subject
- checking timing of the surveillance procedure
- verifying that material collected is consistent with 2.1 (c)
- checking that there is no other reasonable explanation for the particular information collected such as:
  * injured worker able to lift box because he/she was wearing a splint
  * box lifted by injured worker was empty
  * activity performed by worker did not involve using injured muscles.

5.2 Material collected by covert surveillance is not to be disclosed to another person, body or agency, other than in accordance with IPP 11.

5.3 When material is disclosed there should be a record of:

(a) The reason/s for disclosure.
(b) The recipient of the information.
(c) The officer authorising disclosure.

5.4 Disclosures for the purpose of enforcement of criminal law or revenue protection must be noted in the surveillance subject's record. (See IPP 11.2).

5.5 Where material is disclosed to another person, body or agency, safeguards should be in place to ensure that the information is only disclosed by the receiving agency or person in accordance with IPP 11. Agencies should consider formal agreements or memoranda of understanding with persons or agencies to whom the information is disclosed to ensure that an audit trail of information can be established for any subsequent use or disclosure.

6. Storage and security

Agencies should put in place appropriate measures to protect the material against loss; unauthorised access, use, modification or disclosure by:

(a) Restricting access of material to relevant personnel on a "need to know" basis e.g. Comcare case manager.

(b) Storing the material in a secure area e.g. a locked file.

(c) Storing material separately to other routine administrative information about the surveillance subject.

(d) Maintaining a log of all personnel accessing, using or removing the material, in order to establish an audit trail.

7. Monitoring

7.1 Agencies should review their covert surveillance practices periodically. This review may include:

(a) An evaluation of compliance with the guidelines.
(b) A cost/benefit analysis to evaluate the use of covert surveillance as a means of achieving the agency's objectives and taking into account the surveillance subject's right to privacy.

7.2 Agencies should include in their annual reports a summary of the incidence of covert surveillance undertaken. This report should not contain personal information that may lead to identification of particular individuals.

7.3 Agencies should conduct ongoing monitoring of the conduct of covert surveillance and should provide training of staff involved in all aspects of covert surveillance.

Appendix 1: Technological developments

In the past two decades there has been significant development of electronic equipment that can be used for surveillance purposes. These sophisticated devices are capable of greatly enhancing the capacity to intrude into every aspect of the private life of an individual.

These surveillance devices include:

Electronic eavesdropping devices capable of listening to communications or intercepting digital communications, such as:

- telephone interception and recording devices
- parabolic and long range microphones
- miniature radio transmitters
- cellular telephone and radio interceptors (scanners)
- satellite beam interceptors
- concealed microphones
- lasers used to amplify window vibrations and convert them to audible sounds

Optical devices which visually monitor behaviour, such as:

- electronic photographic equipment
- nightvision and low light systems such as image intensifiers
- closed-circuit television
- cable television
- lightweight compact TV cameras for video surveillance
- satellite based visual technology

Locational devices capable of tracking movement and location of individuals, such as:

- electronic vehicle tracking devices
- electronic beepers
- locational bracelets
- access control systems such as key cards
- fixed video camera devices

In addition there are other devices which monitor and record actions such as dialling of telephone numbers or automated transactions, and those which test or measure reactions and emotions.
Individuals can now be subject to electronic surveillance by a wide range of technical devices which monitor actions, communications and psychological states.
Appendix 2: The Privacy Act

The Privacy Act came into operation on 1 January 1989. One of the major concerns of this Act is to protect personal information which is collected by Federal Government Departments or agencies.

The Act sets out eleven Information Privacy Principles (IPPs) that govern the collection; storage and security; access; accuracy of records; and the use and disclosure of personal information by Commonwealth agencies.

The following IPPs are relevant to the practice of covert surveillance:

IPP 1: Manner and purpose of collection of personal information

IPP 1 imposes obligations on Commonwealth agencies relating to the collection of personal information. Collection must be fair and lawful. The information collected must be for a lawful purpose which is directly related to the function or activity of the agency and the collection of information must be necessary for or directly related to that purpose.

IPP 3: Solicitation of personal information generally

IPP 3 requires agencies who solicit personal information (whether from the person that the information is about or otherwise), to take reasonable steps to ensure that the information is relevant to the purpose of collection, up-to-date, complete and that there is not unreasonable intrusion into a person's personal affairs.

IPP 4: Storage and security of personal information

IPP 4 requires agencies to protect information with reasonable security safeguards against loss, unauthorised access, use, modification or disclosure; and other misuse. If it is necessary for the record to be given to a person who is providing a service to the agency, then everything which is reasonably within the power of the agency, must be done to prevent unauthorised use or disclosure of information.

IPP 6: Access to records containing personal information

IPP 6 grants to the individual concerned access rights to personal information held by an agency, subject to exemptions provided in the Freedom of Information Act 1982 or any other law.

IPP 7: Alteration of records containing personal information

IPP 7 requires agencies to ensure that personal information held is accurate, relevant, up to date, complete and not misleading. The individual concerned has amendment and annotation rights, subject to the exceptions listed in IPP 6.

IPP 8: Record-keeper to check accuracy etc. of personal information before use

IPP 8 requires agencies to check that information is accurate, up to date and complete prior to using it.
IPP 9: Limits on the use of personal information to relevant purpose

This IPP requires agencies to confine the use of information to purposes to which the information is relevant.

IPP 10: Limits on the use of personal information

IPP 10 limits the use of personal information. Agencies may not use personal information for purposes other than those for which it is collected except:

(a) with the consent of the person

(b) to prevent a serious and imminent threat to a person's life or health

(c) as required or authorised by law

(d) where reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or for the protection of the public revenue

(e) for a directly related purpose.

If an agency uses information for another purpose under exception (d) the use must be logged on the individual's record.

IPP 11: Limits on disclosure of personal information

IPP 11 limits the disclosure of personal information outside an agency. Agencies may not disclose personal information unless one of five exceptions apply. Four of these exceptions are the same as for IPP 10 (see (a) to (d) above). There is an additional exception where the subject of the information is reasonably likely to be aware or made aware under IPP 2 that the information is usually disclosed. The recipient of information under one of these exceptions may only use it for the purpose for which it was disclosed.

Appendix 3: Glossary of terms

Breach - refers to an act of collection, management, use or disclosure of personal information by an agency that does not conform to an IPP.

Commonwealth Agency - a Commonwealth body that collects information and keeps records and means Commonwealth Ministers and Commonwealth government departments (other than Commonwealth Parliamentary departments), bodies or persons established and performing functions under Commonwealth laws. (cf. Section 6. (1) of the Privacy Act.)

Covert Surveillance - the secretive, continuous or periodic observation of persons, vehicles, places or objects to obtain information concerning the activities of individuals which is recorded in material form.

Any reference to covert surveillance in the guidelines refer specifically to covert surveillance by optical means.
Covert Surveillance by Optical Means - refers to the conduct of covert surveillance using photography; video recorders; or direct observation, the results of which are then recorded.

Material - refers to the information obtained from the covert surveillance operation. This includes photographs, video tapes and logs on which observations are recorded.

Personal Information - means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. (cf. Section 6.(1) of the Privacy Act.)

Record - means a document, a data base (however kept) or a photograph or other pictorial representation of a person. It does not include information publicly available in a library, gallery, museum or government archives. (cf. Section 6.(1) of the Privacy Act.)

Surveillance subject - the person who is the target of the covert surveillance procedure.