



Workplace surveillance policy
ACT Legislative Assembly Secretariat

1. Purpose and basis of the policy

1.1. The purpose of this policy is to achieve compliance with the requirements of the *Workplace Privacy Act 2011* (the Act) including to formally notify Legislative Assembly Secretariat (Secretariat) workers about the type and purpose of workplace surveillance devices in operation at the workplace.

1.2. This policy is made in accordance with s13(5) of the Act.

2 Application

2.1. The Clerk of the Legislative Assembly (the Clerk) causes to be operated and has day-to-day control over a number of surveillance devices as defined by s11 of the Act.

2.2. This policy refers to only those surveillance devices which the Clerk causes to be operated and applies only to workers for whom the Clerk is responsible (see paragraph 1.10.2).

2.3. A policy is in place that applies to workers from across the wider ACT public service which is available from the website of the Commissioner for Public Sector Administration at <http://www.cmd.act.gov.au/governance/public>

3 Continuation of existing arrangements

3.1. This policy codifies the arrangements that apply to surveillance activities that have been in place at the Legislative Assembly for a number of years and before the enactment of the *Workplace Privacy Act 2011*. It does not introduce any new surveillance activities at the Legislative Assembly workplace.

4 Notice of surveillance

4.1. This policy constitutes 'notice of surveillance' to workers pursuant to s13(1)(a) of the Act (see Attachment A).

5 Background

5.1. The Act came into effect on 10 March 2011 and provides a framework for the collection and use of workplace surveillance information by ACT employers, including the Secretariat. Under the Act, **workplace** means "a place where work is, has been, or is to be, carried out by or for someone conducting a business or

undertaking".

5.2. The Act requires that, from 24 August 2011, workers be formally notified of surveillance arrangements in place at their workplaces. This notification must state:

- the kind of surveillance device to be used for the surveillance;
- how the surveillance will be conducted;
- who will regularly or ordinarily be the subject of the surveillance;
- when the surveillance will start;
- whether the surveillance will be continuous or intermittent;
- whether the surveillance will be for a stated period or ongoing;
- the purpose for which the employer may use and disclose surveillance records of the surveillance; and
- that the worker may consult with the employer about the conduct of the surveillance under section 14.

6 Consultation and prior notice

6.1. In accordance with s13 of the Act and Pt 19.5 of the Legislation Act 2001, this policy was provided to all affected workers on 19 July 2011 for comment and consultation.

6.2. As part of the Secretariat's induction arrangements, and in accordance with s13(3)(c) of the Act, all new workers will be provided with a copy of this policy *before* commencing work at the Assembly.

7 Prohibitions

7.1. In addition to the requirement to provide notice to workers about surveillance activities, the Act contains a number of prohibitions. The Act prohibits surveillance:

- in a toilet facility; a change room, a shower or other bathing facility, a parent or nursing room, a prayer room, a sick bay, a first-aid room, and any other area in a workplace prescribed by regulation; and
- when the worker is not at work (except in cases of data (computer) surveillance where the worker is using equipment and/or resources supplied by the Secretariat and surveillance is restricted to the use of such equipment only).

7.2. The Act prohibits the blocking of emails unless a notice (a blocked delivery notice) has been given to the worker or where the incoming communication is perceived to be spam or a threat to the security of the Legislative Assembly or its information systems, or the email contains material that might reasonably be considered to be threatening, harassing or offensive.

7.3. The Act prohibits action to prevent delivery of an email or access to a website because it has been sent by or on behalf of an industrial association or contains information about industrial matters.

8 Covert surveillance

8.1. Any surveillance outside the parameters of a 'Notice of Surveillance' is considered to be covert surveillance and must be authorised by a magistrate.

9 Legislation

9.1. This policy relates to implementation of the *Workplace Privacy Act 2011*. Associated legislation includes:

- *Privacy Act 1988* (Cwlth)
- *Territory Records Act 2002*
- *Human Rights Act 2004*
- *Public Sector Management Act 1994*
- *Safe Work Act 2009*
- *Fair Work Act 2009* (Cwlth)

10 Dictionary

10.1. **Worker** means an individual who carries out work in relation to a business or undertaking, whether for reward or otherwise, under an arrangement with the person conducting the business or undertaking.

10.2. Examples of a **worker** include but are not limited to:

- an employee;
- an independent contractor;
- an outworker;
- a person doing a work experience placement; and
- a volunteer

10.3. The Act defines **surveillance** in the following broad terms:

Surveillance means surveillance using a surveillance device (s11)

10.4. There are three types of surveillance devices provided for in the Act. These are: 1. data surveillance devices; 2. optical surveillance devices; and 3. tracking devices.

10.5. A **data surveillance device** is a device capable of being used to record or monitor the input or output of information from a computer (e.g. monitoring device on a laptop or an electronic door access).

10.6. An **optical surveillance device** is a device capable of recording visually or observing an activity (e.g. video camera or CCTV).

10.7. A **tracking device** is an electronic device capable of being used to work out or monitor the location of a person or the status of an object (e.g. a GPS device in a vehicle).

11 Related policies

11.1. Related policy advice includes:

- *Information technology security policy and framework for the Legislative Assembly for the Australian Capital Territory*
- *Policy on the acceptable use and management of electronic information and information technology*
- *ACT Legislative Assembly Secretariat Code of Conduct*

Notice to Legislative Assembly Secretariat workers: workplace surveillance

This notice, which forms part of the Legislative Assembly Secretariat's Workplace Surveillance Policy, will be provided to all current workers and to new workers before commencement. The policy will be made available on the recruitment page of the Legislative Assembly's (Assembly) website and on the Assembly's intranet.

This Notice sets out details of how those surveillance devices are, or may be, used and contains the information required under section 13(4) of the *Workplace Privacy Act 2011*.

Consultation

The policy and this notice has been subject to consultation with workers. Workers may continue to consult with their employer about the conduct of surveillance.

The kind of surveillance devices used for surveillance

In carrying out its business, the Legislative Assembly Secretariat (Secretariat) uses the following kinds of surveillance devices and further details of the use of these surveillance devices are set out in this notice:

- (a) data surveillance devices;
- (b) optical surveillance devices; and
- (c) tracking devices.

Data surveillance

Types of data surveillance

Data surveillance refers to the monitoring and logging of use of the Assembly's information communication technology (ICT) (i.e. computers, computer networks and related systems). This includes the use of Secretariat owned or leased personal computers, laptop computers, access control system (also discussed under tracking surveillance below) and smart phones or mobile devices.

Use of the Assembly's ICT is governed by the *Information technology security policy and framework for the Legislative Assembly for the Australian Capital Territory*. This policy is in place to ensure the efficiency, integrity, confidentiality and availability of the Assembly's information systems.

The *Policy on the acceptable use and management of electronic information and information technology* describes workers' obligations regarding the use of ICT systems. Under the arrangement the Assembly has with Shared Services ICT the Assembly IT systems are subject to the processes which the ACT Government has in place to log and monitor ICT records.

Who will be the subject of data surveillance?

Data surveillance is applied to all users of Assembly ICT systems and networks. This includes, but is not limited to, employees of the Secretariat, some contractors engaged by Secretariat, volunteers and work experiences students engaged by the Secretariat.

How data surveillance is carried out

The Clerk of the Legislative Assembly (the Clerk) may approve access rights to an authorised person to all worker ICT related activity. This access is in accordance with the *Policy on the acceptable use and management of electronic information and information technology*.

Some ICT use is monitored using content filtering to detect and report inappropriate use as described in the policy.

The Secretariat monitors workers' use of Assembly computers and ICT systems by:

- maintaining logs, backups and archives of computing activities including workstations, lap top computers, servers, printers, and network connected devices, including smart phones, tablets and other mobile devices;
- monitoring email server performance and retention of logs, backups and archives of emails sent and received through Assembly servers;
- retaining logs, backups and archives of all internet access and network usage;
- even where the user has deleted an email or another data file/record, the Secretariat, through its ICT provider, may still retain archived and/or backup copies of the email or data file/record; and

When data surveillance occurs

Data surveillance is continuous, ongoing and is in place as at the date of approval and promulgation of this policy.

Data surveillance may operate when the worker is using equipment and/or resources supplied by the Secretariat away from the workplace including personal computers, laptop computers, smart phones and other mobile devices. Surveillance away from the workplace is restricted to the use of such equipment only.

Purpose of data surveillance

Inappropriate use of ICT systems and networks, including internet and email, presents a risk to the Assembly and the integrity of its data and that of its users. Surveillance of Assembly ICT systems and networks is in place to protect the efficiency, integrity, confidentiality and availability of these systems.

Optical surveillance

Types of optical surveillance

An optical surveillance device is a device capable of visually recording or observing an activity. Video cameras or Closed Circuit Television (CCTV) are examples of optical surveillance.

Who will be the subject of optical surveillance?

Optical surveillance is applied to all workers at, and visitors to, the Assembly precincts. Optical surveillance also extends to areas beyond the Assembly precincts, including:

- parts of civic square;
- the Assembly car park;
- the laneway adjacent to the Canberra Theatre; and
- parts of London circuit and the bus stop on the Eastern side of the building.

How optical surveillance is carried out

CCTV systems are used to monitor and record images necessary to satisfy the purpose of optical surveillance (see below)

CCTV systems do not operate in private areas of the Assembly building such as toilets, change rooms or the sick room (see paragraph 1.7.1 of the Policy).

Signage identifying that CCTV surveillance is being conducted at the Assembly precinct is prominently displayed at each of the Assembly's three entrances (i.e. public entrance, members' entrance and laneway entrance adjacent to the Canberra Theatre).

When optical surveillance occurs

Optical surveillance is continuous, ongoing and is in place as at the date of approval and promulgation of this policy.

Purpose of optical surveillance

Surveillance of Assembly precincts is in place to ensure the safety and security of workers, members of the public and visitors to the Assembly building. Optical surveillance is also used to protect Assembly property and assets.

Security

CCTV is used in deterring, preventing, investigating and prosecuting crime against property and/or persons.

Tracking surveillance

Types of tracking surveillance

Tracking surveillance refers to electronic devices capable of being used to work out or monitor the location of a person or the status of an object. Such devices include, but are not limited to, Secretariat owned or leased, mobile devices (including mobile telephones), and laptop computers. They could also include official credit cards, cab-charge e-tickets and fuel cards issued in association with official vehicles.

Who will be the subject of tracking surveillance?

Operators of mobile devices (including mobile phones) and staff who are issued with official credit cards, cab charge e-tickets and who use a fuel card for an official

vehicle may be the subject of tracking surveillance. Workers at the Assembly precincts are also subject to surveillance associated with the building's access control system.

How tracking surveillance is carried out

The electronic access control system used at the Assembly building records the entry, movement around and exit from the premises of all workers with a valid access control pass (sometimes referred to as a proximity or prox pass). Records and logs of access and entry are retained for up to five years.

The Secretariat may only conduct surveillance of a worker that involves the tracking of a vehicle or asset using a tracking device if there is a notice clearly visible on the tracking device stating that the vehicle or asset is being tracked. To meet this requirement, a notice has been placed on all Secretariat devices that are capable of being tracking devices (this includes mobile phones and other mobile devices).

When tracking surveillance occurs

Tracking surveillance is continuous, ongoing and is in place as at the date of approval and promulgation of this policy.

Purpose of tracking surveillance

Tracking surveillance of Secretariat workers and assets is in place to ensure the security and safety of workers, visitors to the building, members of the public, and visitors to the Assembly precincts. Tracking surveillance is also used to protect Assembly property and assets.

The purposes for which the Secretariat may use and disclose surveillance records of surveillance activities

Efficiency of Secretariat business activities

Data surveillance, use of CCTV systems (optical surveillance) and tracking devices may be used for process control and business monitoring.

Audit and legal requirements

Surveillance records may be audited, are subject to ACT and Federal laws, and may be used as evidence in legal proceedings.

Misconduct and underperformance

The Secretariat may rely on surveillance records to investigate alleged breaches of its policies or the law, including Section 9 of the *Public Sector Management Act 1994* or general obligations of workers.

Any such investigation will be carried out in accordance with the requirements of the relevant industrial agreement and in accordance with the principles of natural justice and procedural fairness.

The Clerk may use records of surveillance to take adverse action against a worker.

Access to and disclosure of surveillance records

Access to and disclosure of surveillance records will not occur without the express written authorisation of the Clerk, or an officer authorised by the Clerk for that purpose (in which case the term Clerk in the following also refers to such a person).

Pursuant to s22(3) of the Act, the Clerk will ensure that a surveillance record in relation to surveillance is only accessed or otherwise used where:

- the record is used or disclosed for a legitimate purpose in relation to the employment of a worker or the legitimate business activities or functions of the employer; or
- the record is disclosed to a member of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence; or
- the record is used or disclosed for a purpose directly or indirectly related to a civil or criminal proceeding; or
- the Clerk reasonably believes that the use or disclosure of the record is necessary to avoid an imminent risk of death of, or serious injury to, someone or substantial damage to property.

A record will be maintained of all requests for access to surveillance records and all determinations made by the decision maker in relation to requests. The following information must be recorded:

- the person making the request;
- the date of the request;
- the purpose for which the request was made;
- the specific record of surveillance requested and the relevant date and times;
- whether or not access was approved and how the access was provided and any conditions attached to the access.

Access by workers to surveillance records of the surveillance

A worker is able to seek access to records associated with surveillance of them through a written request to the Clerk.

Access to records by a worker may not be permissible in certain circumstances such as where such the access would impinge on the privacy of another person or where the request is frivolous or vexatious. Section 23(3) of the Act outlines further provisions in relation to the circumstances in which a request may be refused.

However, where a worker's request for access to a surveillance record is not granted, the record cannot be used to take adverse action against the worker or in a legal proceeding between the employer and the worker.

Management of Surveillance Records

As for all its records, the Secretariat has obligations under the *Territory Records Act 2002* and under the Secretariat's approved records management program. Under those arrangements, surveillance records are secured appropriately. Whether a record is destroyed and, if so, when it is eligible for destruction, is determined in accordance with disposal schedules approved by the Director of Territory Records. Any disposal action is taken in accordance with the Secretariat's Records Management Procedures.