



**ACT**

Government

Chief Minister and Cabinet

Our ref: 2011/7021

Your ref:

All Staff

Dear ACT Government Employee

## **Workplace Privacy Act 2011**

I write to provide to you the attached Workplace Privacy Policy Statement and Notice to Workers.

In March of this year the *Workplace Privacy Act 2011* was made law. The Act requires that ACT employers notify workers of the nature and purpose of workplace surveillance operating within workplaces. The Workplace Privacy Policy and Notice to Workers sets out the type and purpose of surveillance operating in ACT Government workplaces.

I encourage you to read this policy statement and notice and to familiarise yourself with its contents. I also encourage you to be familiar with the related Acceptable Use of ICT Resources Policy which is available at <http://www.sharedservices.act.gov.au>

Should you wish to discuss this notice you should contact your Directorate human resources area.

Yours sincerely

Andrew Cappie-Wood  
Head of Service

August 2011

**People Management Policy Statement**  
**ISSUED: August 2011**

**Chief Minister and Cabinet Directorate**  
**Workforce Capability and Governance Division**

**Workplace Privacy Policy Statement & Notice to Workers**

**Directors - General**  
**HR Directors/Managers**  
**Building/Facilities/Security Managers**  
**Shared Services**

**Purpose**

The purpose of this policy statement is to ensure that ACT Government workplaces comply with the requirements of the *Workplace Privacy Act 2011* (the Act). This policy statement represents the Act's requirement that formal notification be provided to workers about the type and purpose of workplace surveillance devices in operation.

**Application**

This policy statement relates to service wide management of workplace surveillance and applies to all ACT Government workers and contractors.

**Background**

The Act came into effect on 10 March 2011 and provides a framework for the collection and use of workplace surveillance information by Territory employers including Government Directorates.

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

- the type of surveillance device in use;
- how surveillance will be conducted;

- who will be subject to surveillance;
- when surveillance will be in place; and
- the purpose(s) of surveillance.

### **Principles**

This policy and the attached Notice to Workers does not represent a change in the use of surveillance across ACT Government workplaces however the Act does regulate the use of such surveillance.

ACT Government is committed to fully complying with its statutory obligations under the Act.

The Notice at **Attachment A** describes the types of surveillance in place across ACT Government workplaces and the purpose for which surveillance is in place. This includes data surveillance, optical surveillance and tracking surveillance.

### *Prohibitions under the Act*

In addition to the notice requirement the *Act* contains a number of prohibitions. The Act prohibits surveillance:

- i. 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
- ii. 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 ACT Government and surveillance is restricted to the use of such equipment only.

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 Government or its information systems, or the email contains material that might reasonably be considered to be threatening, harassing or offensive.

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.

Under the Act surveillance is only permitted for the purpose identified in the attached Notice to Workers.

### *Covert Surveillance*

Any surveillance outside the parameters of the Notice is considered to be covert surveillance and must be authorised by a Magistrate.

### **Legislative Reference**

This policy relates to implementation of the Act. Associated legislation includes:

*Privacy Act 1988* (Commonwealth);  
*Territory Records Act 2002*;  
*Human Rights Act 2004*; and  
*Public Sector Management Act 1994*.

### **Dictionary**

**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.

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

An employee (including permanent, temporary, and casual employees)  
an independent contractor  
an outworker  
a person doing a work experience placement  
a volunteer

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).

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

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).

**Workplace** means a place where work is, has been, or is to be, carried out by or for someone conducting a business or undertaking.

### **Related Policy**

Related policy advice includes:

- *Acceptable Use of ICT Resources Policy*;

- *ICT Security Policy;*
- [ACT Government Code of Practice for Closed Circuit Television Systems;](#)  
*and*
- *CITRIX Remote Access Install Work Instructions.*

**Policy Owner**

Senior Manager  
Workplace Relations  
Workforce Capability and Governance  
Chief Minister and Cabinet Directorate

**Review Date**

This policy statement is due for review in July 2012.

Andrew Kefford  
A/g Commissioner for Public Administration

## **Notice to Workers: Workplace Surveillance**

This policy will be provided to all current workers and new workers on commencement. The policy will be made available on Directorate web sites and in operational guidance.

Workplace surveillance is only permitted for the uses described in this notice and in accordance with the Workplace Privacy Act 2011.

## **Data Surveillance (Computers and ICT Equipment)**

### ***Types of Data Surveillance***

Data Surveillance refers to the monitoring and logging of use of ACT Government information communication technology (ICT) transactions and records, i.e. computers, computer networks and related systems. This includes the use of Territory owned or leased personal computers, laptop computers and smart phones

Use of ACT Government ICT is governed by the [Acceptable Use of ICT Resources Policy](#). This policy is in place to ensure the, efficiency, integrity, confidentiality and availability of ACT Government information systems.

The [Acceptable Use of ICT Resources Policy](#) describes worker obligations in regards to the use of ICT systems. The policy also describes the processes 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 ACT Government ICT systems and networks. This includes, but is not limited to, workers of ACT Government, contractors engaged by ACT Government, and clients of ACT Government services including students.

### ***How Data Surveillance is Carried Out***

ACT Government ICT Security has access rights to all worker ICT related activity. This access is in accordance with the [Acceptable Use of ICT Resources Policy](#). All ICT use is monitored using content filtering to detect and report inappropriate use as described in the policy. Only staff authorised by the General Manager, Shared Services ICT, may examine such records.

ACT Government monitors staff use of Government 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 and tablets;
- monitoring email server performance and retention of logs, backups and archives of emails sent and received through ACT Government servers; and
- retaining logs, backups and archives of all internet access and network usage.

Even where the user has deleted an email, ACT Government may still retain archived and/or backup copies of the email.

Records of workplace surveillance are retained in accordance with the provisions of the *Territory Records Act 2002*. Where necessary or relevant surveillance records may be kept for a period longer than required under the *Territory Records Act 2002*: for example records may be kept until the end of legal proceedings.

#### ***When Data Surveillance Occurs***

Data surveillance is 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 ACT Government, such as desktop computers, laptop computers and smart phones, including where they are used away from the workplace. Data surveillance when the worker is using equipment and/or resources supplied by the ACT Government away from the workplace will also operate when the worker is outside of the Territory.

#### ***Purpose of Data Surveillance***

Surveillance of ACT Government ICT systems and networks is in place to protect the efficiency, integrity, confidentiality and availability of these systems.

#### ***Security of the Network***

Malicious software and viruses pose a significant risk to the ACT Government and its operations. Excessive use of streaming data presents a significant cost to the ACT Government and poses a risk to the availability of the network. Inappropriate use of ICT systems and networks, including internet and email, presents a risk to the integrity of ACT Government and its process.

### *Audit and Legal Requirements*

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

### *Misconduct and Underperformance*

ACT Government may rely on ICT monitoring and logging to investigate alleged breaches of ACT Government policies or the law, including *Section 9* of the *Public Sector Management Act 1994*, by staff using its ICT systems.

Any such investigation will be carried out in accordance with the requirements of directorate enterprise agreements and the *Public Sector Management Act 1994*, and in accordance with the principles of natural justice and procedural fairness.

### *Efficiency of ACT Government Business Activities*

Data surveillance devices may be used for process control and business monitoring.

## **Optical Surveillance (Cameras and CCTV)**

### ***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. Such devices are primarily used for the security and safety of ACT Government workers and assets and for the safety and security of members of the public.

The [ACT Government Code of Practice for Closed Circuit Television Systems](#) governs the use of CCTV and related systems operating within ACT Government.

### ***Who will be the Subject of Optical Surveillance?***

Optical surveillance is applied to ACT Government staff and members of the public. This includes, but is not limited to, workers of ACT Government, contractors engaged by ACT Government directorates, and clients of ACT Government services including students.

### ***How Optical Surveillance is Carried Out***

The [ACT Government Code of Practice for Closed Circuit Television Systems](#) requires that CCTV be operated:

*with due regard to the privacy and human rights of individual members of the public and agency staff. The ACT is committed to ensuring the protection of*

*human rights as described in the Human Rights Act 2004, and the operation of CCTV systems must consider the impact on Human Rights.*

Procedures for use of CCTV systems must also be in accordance with the requirements of the *Privacy Act 1988* (Commonwealth) and the *Public Sector Management Act 1994*.

CCTV systems are used to monitor and record images necessary for the safety and security of ACT Government workers and assets and for the safety and security of members of the public. Recorded images are retained and used only in accordance with the purpose for which the CCTV system was installed unless they are subject to Territory or Federal laws that may require these records to be used as evidence in legal proceedings or otherwise in accordance with the provisions of this policy.

CCTV systems will not operate in private areas such as toilets or change rooms and should be used in accordance with the *Privacy Act 1988*.

Optical surveillance may only be carried out where the device used for the surveillance is clearly visible in the workplace and where there is clear signage at the entrance to the workplace advising that surveillance is in place.

Records of workplace surveillance are retained in accordance with the requirements of the *Territory Records Act 2002*. Where necessary or relevant surveillance records may be kept for a period longer than required under the *Territory Records Act 2002*: for example records may be kept until the end of legal proceedings.

Optical surveillance of workers must not be conducted in a toilet facility; a change room, a shower or other bathing facility, a parent or nursing room, a prayer room, a sick bay, or a first-aid room.

#### ***When Optical Surveillance Occurs***

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

Where optical surveillance is operating in an ACT Government vehicle or other thing the optical surveillance will also operate when the vehicle or other thing is outside of the Territory.

### ***Purpose of Optical Surveillance***

Surveillance of ACT Government premises and assets is in place to ensure the security and safety of ACT Government workers and assets and for the safety and security of members of the public.

### ***Security of ACT Government Workers and Assets and Members of the Public.***

CCTV is used in reducing and preventing crime against property and/or persons.

### ***Audit and Legal Requirements***

CCTV records and images may be audited, are subject to Territory and Federal laws and may be used as evidence in legal proceedings.

### ***Misconduct and Underperformance***

ACT Government may rely on optical surveillance to investigate alleged breaches of ACT Government policies or the law, including *Section 9* of the *Public Sector Management Act 1994*, by workers.

Any such investigation will be carried out in accordance with the requirements of directorate enterprise agreements and the *Public Sector Management Act 1994*, and in accordance with the principles of natural justice and procedural fairness.

### ***Efficiency of ACT Government Business Activities***

CCTV systems may be used for process control and business monitoring. Examples of such use include traffic flow in car parks, at weigh bridges and monitoring of impounded animals.

## **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 will include personal GPS tracking devices, radio frequency identification devices, GPS tracking devices that are in Territory owned and leased vehicles, and on Territory owned and leased Portable Electronic Devices including mobile telephones, smart phones and iPhones.

### ***Who will be the Subject of Tracking Surveillance?***

Operators of ACT Government vehicles and mobile plant and equipment may be the subject of tracking surveillance. Electronic controlled access systems (proximity

cards, building access cards, entry swipe cards, etc) may also track access of ACT Government workers and contractors to ACT Government workplaces and other assets. ACT Government workers engaged in field work may be subject to GPS (Global Positioning Systems) devices.

#### ***How Tracking Surveillance is Carried Out***

Procedures for use of tracking systems must be in accordance with the requirements of the *Privacy Act 1988* (Commonwealth), Human Rights Act 2004, and *Public Sector Management Act 1994*.

Electronic controlled access systems are used to control access and entry to ACT Government buildings and assets. Such systems may include the recording of entry and, in some cases, exit from premises. Records and logs of access and entry may be retained for specified periods.

GPS devices are used to track the location of ACT Government vehicles and other assets. In the case of field workers a GPS device may be used to track the location of an individual worker or contractor.

ACT Government 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 vehicle or asset stating that the vehicle or asset is being tracked.

Records of workplace surveillance are retained in accordance with the requirements of the *Territory Records Act 2002*. Where necessary or relevant surveillance records may be kept for a period longer than required under the *Territory Records Act 2002*: for example records may be kept until the end of legal proceedings.

#### ***When Tracking Surveillance Occurs***

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

Where tracking surveillance is operating in an ACT Government vehicle or other thing the tracking will operate when the vehicle or other thing is operating outside of the Territory.

#### ***Purpose of Tracking Surveillance***

Tracking surveillance of ACT Government workers and assets is in place to ensure the security and safety of ACT Government workers and assets and for the safety and security of members of the public.

*Security of ACT Government Workers and Assets*

Tracking surveillance is used to ensure the safety and security of ACT government workers and the security of ACT Government property and assets.

*Audit and Legal Requirements*

Records of tracking surveillance may be audited, are subject to Territory and Federal laws, and may be used as evidence in legal proceedings.

*Misconduct and Underperformance*

ACT Government may rely on tracking surveillance to investigate alleged breaches of ACT Government policies or the law, including *Section 9* of the *Public Sector Management Act 1994*, by workers.

Any such investigation will be carried out in accordance with the requirements of directorate enterprise agreements and the *Public Sector Management Act 1994*, and in accordance with the principles of natural justice and procedural fairness.

*Efficiency of ACT Government Business Activities*

Tracking devices may be used for process control and business monitoring.