2010

THE LEGISLATIVE ASSEMBLY FOR THE AUSTRALIAN CAPITAL TERRITORY

WORKPLACE PRIVACY BILL 2010

EXPLANATORY STATEMENT

Circulated by
Amanda Bresnan MLA

OVERVIEW

The objects of this Bill are to ensure that employers inform and consult with employees on any surveillance that takes place in the workplace, except where:

1. The employer is able to demonstrate to the Magistrates Court
    a. a reasonable suspicion that an employee is engaging in unlawful activity, and
    b. that covert surveillance is necessary to prevent the unlawful activity; and
    c. the covert surveillance is conducted by a nominated responsible person authorised by the Magistrate
2. Surveillance of an area is prohibited on the grounds of an increased expectation of privacy in that area, for example change rooms or prayer rooms.

Surveillance of employees by employers is currently unregulated in the Australian Capital Territory, and this Bill arises out of a concern that security cameras and other monitoring devices are being installed in workplaces without the knowledge of employees.

The Bill recognises a right to privacy for workers in the workplace, and requires that employers must inform workers when their right to privacy will be limited through use of surveillance and the reason for the limitation. It seeks to do this in such a fashion that balances a worker's right to privacy with a business owner's right to take reasonable steps to protect their business and monitor their employees.

In addition to providing a framework for the conduct of surveillance, the Bill creates limitations on the use of surveillance data, and creates a limited right for workers to access data their employers have collected on them through surveillance.

A similar Act to this proposed Act has been in operation in New South Wales since 2005.

OPERATION OF THE BILL

Notified Surveillance

In order to conduct ordinary (i.e. not covert) surveillance of a workplace, an employer is required to go through a process of notification and consultation prior to implementing surveillance in the workplace.

The notification is required to outline the manner in which surveillance will be conducted and what surveillance records generated by the surveillance can be used for. Significantly, while surveillance can be used for employee monitoring and performance management under the scheme outlined in the Bill, the employer *must* disclose that surveillance may be used to do so, or else the employer will not be able to take adverse action against the employee based upon activities captured by the surveillance records.

The notification may take the form of a generalised 'surveillance policy' that is issued to all workers (provided the policy notifies the employees in accordance with the Bill), or individual notices, or a combination of both. This allows the employer the ability to only notify relevant employees where surveillance is limited, and similarly notify all employees of workplace- or company-wide implementation of surveillance.

For example, if an employer intends to install cameras in 5 separate workplaces, the employer could:

- issue notices regarding each individual conduct of surveillance to the workers in each individual workplace; or
- issue a uniform notice to workers in all 5 workplaces; or
- append the notice to an existing company-wide surveillance policy, and draw the affected employees attention to that policy.

A consultation period of 14 days is in place following the initial notice of surveillance. An employer is required to give consideration to concerns raised by workers regarding the conduct of surveillance.

This Bill regulates three types of surveillance; optical, data and tracking surveillance, and places particular requirements on each type.

For optical surveillance, an employer is required to have the camera or camera casing visible in the workplace where surveillance is conducted, and to place signs on that workplace indicating that surveillance may take place there. The employer is required to provide a notice to workers who ordinarily work in the workplace where optical surveillance is being conducted. No specific notice is required for workers who do not usually work in that workplace, however, the signage and visible camera requirements should make those workers sufficiently aware of the conduct of the surveillance without requiring an employer to specifically notify them.

For computer surveillance, an employer is required to develop a policy on the use of data surveillance (which can include computers, internet, smartphones or other device capable of electronic communication), and then comply with that policy. In effect, an employer is required to outline in a policy how data device usage may be monitored (such as internet usage audits, email content monitoring and installation of computer use monitoring programs) and then comply with the policy.

For tracking surveillance, an employer is required to place a visible notice on any vehicle or other thing that is being tracked. It should be noted that this may, in some circumstances, include smartphones where GPS data can be used to track location.

The Bill outlines a series of offences for failure to comply with appropriate notification procedures, and also places a requirement upon an employer to take reasonable care of surveillance records generated by notified surveillance.

The Bill makes it an offence to use or disclose surveillance records for anything other than a legitimate purpose. This effectively prohibits the usage of surveillance records generated by workplace surveillance for anything other than workplace or legal activity.

Covert Surveillance

The Bill sets up a scheme whereby an employer is required to demonstrate to the Magistrates Court that covert surveillance is required to detect suspected unlawful activity in a workplace.

The employer will be required to set out the grounds for the use of covert surveillance in the application to the Court. The hearing to decide the application is to be held in private.

The employer is required to nominate a suitable person to be the surveillance supervisor, who will then conduct the covert surveillance on behalf of the employer. Surveillance records generated are kept by the surveillance supervisor, who then may transfer relevant parts of the surveillance record to the employer. The employer is only entitled to see parts of records that relate to the unlawful activity specified in the authority or other unlawful activity, in order to protect the privacy of workers subject to the covert surveillance.

The surveillance supervisor is required to submit a covert surveillance report to the Court within 30 days of the conclusion of the authority. The Court may make orders in regards to surveillance records for the duration of the authority or beyond, including to have surveillance records given to the Court for safekeeping. The Court must make an order to release surveillance records to a worker subject to covert surveillance except where there is sufficient reason not to.

A surveillance supervisor is required to destroy surveillance records generated by covert surveillance within 3 months of the expiry of the authority, except for those with relevance to ongoing matters.

Use of records generated by covert surveillance is strictly limited, primarily to the discovery of unlawful activity in the workplace as per the covert surveillance authority, however, some exceptions for health and safety and law enforcement exist. Importantly, covert surveillance records cannot be used for employee performance monitoring or management.

Prohibited Surveillance

The prohibited surveillance section makes it an offence to conduct any form of surveillance in specific areas where there is a heightened expectation of privacy, for example prayer rooms and bathrooms. Whilst the legislation outlines a specific list, there is provision for the relevant Minister to add more by regulation.

This section also prohibits the surveillance of workers not at work, and where the nature of the surveillance makes that unavoidable, requires that the employer not use the surveillance record for any purpose.

HUMAN RIGHTS

This Bill engages the right to privacy as set out in the Section 12 of the *Human Rights Act 2004*:

'Everyone has the right—
(a) not to have his or her privacy, family, home or correspondence interfered with unlawfully or arbitrarily; and
(b) not to have his or her reputation unlawfully attacked.'

The current lack of regulation of this area allows employers to conduct surveillance of their workers without notification or any regard to privacy considerations. In particular, employers are able to misuse and/or disseminate surveillance records without a worker's permission. The current situation allows for arbitrary interference with privacy and correspondence. This Bill mandates that an employer must notify and consult with an employee prior to surveillance commencing, or seek an authority from the Magistrates Court to conduct covert surveillance, and thus ensures that surveillance does not *arbitrarily* interfere with privacy. The scheme created sets up a proportionate limitation on the right to privacy consistent with Section 28 of the *Human Rights Act 2004*.

Clause 27 engages the *Human Rights Act 2004*, s21 (Fair Trial) by requiring that hearing for an application for covert surveillance authority be held in private. This is reasonable in this circumstance as a public hearing would compromise the objective of covert surveillance, and the Magistrates Court is required to consider the effect on privacy when considering whether to grant a covert surveillance authority.

Clauses 35 and 36 engage the *Human Rights Act 2004*, s21 (Fair Trial) by casting a legal burden on the defendant. This is reasonable in this circumstance as conducting covert surveillance in a workplace always causes harm to workers' right to privacy, and should be prohibited except where an employer can justify doing so. As such, the conduct of covert surveillance in the workplace should be considered a strict liability offence, and the legal burden should be placed upon the defendant.

SUMMARY OF CLAUSES

Part 1 - Preliminary

Clause 1 Name of Act
Sets out the name (also called the short title) of the proposed Act.

Clause 2 Commencement
Provides for the commencement of the parts of the proposed Act. The requirements for notified and covert surveillance will commence 6 months after the Act's notification day. The requirements for prohibited surveillance will commence 14 days after the Act's notification day. The commencement of these sections of the Act is to enable employers to have a greater period of time to comply with the requirements under the Act.

Clause 3 Dictionary
Provides for the dictionary to be part of the legislation.

Clause 4 Notes
Provides that notes do not form part of the proposed Act.

Clause 5 Offences against Act – application of Criminal Code etc
Stipulates that offences under the proposed Act are subject to the Criminal Code

Part 2 - Object and important concepts

Clause 6 Object of Act
Sets out the main object of the proposed Act. The main object is to regulate the collection and use of surveillance information in the workplace.

Clause 7 Meaning of *worker*
Gives an extended meaning to *worker* to encompass people who carry out work under arrangement with another, whether it be for reward or otherwise. This is to ensure that the Act applies to individuals in relationships similar to employee relationships, such as independent contractors or volunteers.

Clause 8 Meaning of *employer*
Defines an employer as a person who engages the worker to carry out work in a business or undertaking. Gives an extended meaning to *employer* where corporations are related, so that an employer's employees will include employees of a related corporation of the employer. It specifically excludes householders to ensure that home security systems are not subject to the Act where a householder engages a worker to conduct work on home premises.

Clause 9 Meaning of *business or undertaking*
Specifies that *business or undertaking* includes not-for-profit business as well as activities conducted by local, state or territory government.

Clause 10 Meaning of *workplace*
Defines *workplace* for the purposes of the proposed Act.

Clause 11 Meaning of *surveillance* etc
Clarifies that a person is taken to *conduct* surveillance if the person causes someone else to conduct surveillance. It defines a *data surveillance device* is a device or software program that can be used to monitor input or output from a data device, such as a computer or smartphone. It defines an *optical surveillance device* as a camera, which can include cameras that capture either motion or still images. It defines *tracking device* as a device that can be used to deduct the location and/or status of a person or object.

Part 3 - Notified surveillance

The purpose of this Part is to enable employers to engage in surveillance of workers, provided that they provide notification to those workers that they will be under

surveillance and whether surveillance may be used to take adverse action against workers based upon surveillance records generated by that surveillance.

This Part also creates offences for failure to comply with notification requirements under this Part.

Division 3.1 General

Clause 12 Meaning of *surveillance* – pt 3
Excludes covert (part 4) and prohibited (part 5) surveillance from the provisions of this part.

Division 3.2 Notifying workplace surveillance

Clause 13 Notice of surveillance required
Specifies that surveillance may only be conducted where an employer gives notice to an employee, and that the surveillance is conducted in accordance with that notice, except in the case of optical surveillance devices where the workplace is not the worker's usual place of work. The clause provides requirements for the notification of surveillance of employees. It specifies that this notice must be given 14 days in advance of the surveillance commencing, or for new employees, prior to the employee starting work. It also requires an employer to set out in the notice the purposes for which the employer can use surveillance records.

Clause 14 Requirement for consultation on proposed surveillance
Creates a requirement for the employer to consult in good faith with affected employees about the conduct of the surveillance during the notification period.

Clause 15 Additional requirements for optical surveillance devices
Imposes additional requirements for the notification of optical surveillance. Employers using optical surveillance devices must make sure the device is visible in the workplace and that a sign is visible at the entrance of the workplace notifying people that they may be under surveillance.

Clause 16 Additional requirements for data surveillance devices
Imposes additional requirements for the notification of data surveillance. Data surveillance must be conducted in accordance with a data surveillance policy, and that the employer must inform the worker in a way that it is reasonable to assume that the worker is aware of and understands the policy.

Clause 17 Additional requirements for tracking devices
Imposes an additional requirement for the notification of tracking surveillance. Employers must place a notice on the vehicle or other device being tracked stating that the device is being tracked.

Clause 18 Offences – failure to comply with notified surveillance requirements
Creates offences for failure to comply with notification requirements.

Division 3.3 Other matters

Clause 19 Surveillance by agreement
Provides for surveillance by agreement of the worker, or a body representing a substantial number of workers.

Clause 20 Offence – restrictions on blocking electronic communication and internet access
Creates an offence where an employer fails to provide stopped delivery notices in accordance with s(21)

Clause 21 Notice of blocking electronic communication and internet access
Requires an employer to provide a stopped delivery notice if the employer blocks an electronic communication (for example e-mail) or access to a website. It provides exemptions for communications believed to be spam or contain malicious software, and requires an employer to not block a communication solely on the grounds that it is a communication from an industrial association or relates to industrial matters.

Clause 22 Offences – use and disclosure of surveillance records
Creates an offence where an employer takes adverse action against a worker based upon a surveillance record generated by notified surveillance where the employer did not specify that such action could be taken in the surveillance notice. The clause also creates an offence where a surveillance record is used or disclosed outside the legitimate purposes set out in the clause.

Clause 23 Access to surveillance records of notified surveillance
Provides that an employer must provide a worker with access to surveillance records in relation to the worker, subject to some restrictions set out in the clause. It should be noted that the guidelines for disclosure are based upon *National Privacy Principles*.

Part 4 - Covert surveillance

The purpose of this Part is to enable employers to conduct non-notified, covert surveillance of workplaces for a limited period where the employer has a reasonable suspicion that a worker or workers are engaged in unlawful activity. Applications for such surveillance must be made to the Magistrate's Court, and the surveillance itself is conducted by a nominated surveillance supervisor that is not the employer.

This Part also creates offences for covert surveillance conducted without an authority.

Division 4.1 General

Clause 24 Meaning of *covert surveillance* – Act
Defines *covert surveillance*.

Clause 25 Definitions – pt 4
Provides further definitions for the purpose of this Part.

Division 4.2 Covert surveillance authorities

Clause 26 Application for covert surveillance authority

Provides for an employer to make an application to the Magistrates Court for a covert surveillance authority for the purpose of finding out if the worker is engaged in an unlawful activity in the workplace. The clause specifies the particulars that must accompany an application, including:

(a) the grounds that the employer has for believing a worker or workers are engaged in unlawful activity.
(b) The actions (if any) the employer has taken to detect the unlawful activity
(c) The name (if practicable) or a description of a group or class of workers who will be regularly or ordinarily be subject of the surveillance
(d) Description of the place or thing that will be subject of the surveillance
(e) The kind of surveillance device
(f) The period of the covert surveillance
(g) Information relating to previous applications for a covert surveillance authority for the proposed surveillance

The application must nominate at least 1 person to be a surveillance supervisor. If an application fails, any further application must provide additional relevant information.

Clause 27 Hearing in Private

Requires an application for a covert surveillance authority to be heard in private. Acknowledging that this engages with the right to a fair trial, it is necessary to conduct these hearings in private in order to preserve the purpose of covert surveillance.

Clause 28 Issuing covert surveillance authority

Requires that reasonable grounds exist to justify the issue of a covert surveillance authority, and sets out the grounds by which the Magistrates Court shall consider an application reasonable, including having regard to whether the covert surveillance might unduly intrude on the privacy of other employees or any other person, or whether there are other appropriate means of investigating unlawful activity.

Clause 29 Appointing surveillance supervisor

Requires that the Magistrates Court issuing a covert surveillance authority to designate one or more appropriate persons to be surveillance supervisors to oversee the conduct of surveillance operations under the authority.

Clause 30 Duration of covert surveillance authority

Provides that a covert surveillance authority remains in force for 30 days or as otherwise as prescribed by legislation.

Clause 31 Conditions on covert surveillance authority

Provides conditions for covert surveillance authorities. The conditions include restrictions on the use and distribution of covert surveillance records, and a requirement that surveillance supervisors only provide the employer with surveillance records relevant to the purpose of that authority.

Clause 32 Defects in covert surveillance authority

Provides that defects in the authority do not invalidate the authority, except where the defects are material.

Clause 33 Varying or cancelling covert surveillance authority
Provides for the variation or cancellation of a covert surveillance authority by the Magistrates Court on its own authority or by application of an affected person.

Clause 34 Magistrates Court to record details of covert surveillance authority orders
Requires the Magistrates Court to keep records of surveillance authorities, and allows for regulation to prescribe requirements for record-keeping.

Division 4.3 Restrictions on covert surveillance

Clause 35 Offence – conducting covert surveillance other than under covert surveillance authority
This clause creates an offence where an employer conducts covert surveillance not under a covert surveillance authority. Exceptions are made for law enforcement agencies in the exercise of a law, optical surveillance of correctional facilities, optical surveillance of casinos and optical surveillance of legal proceedings.

Clause 36 Defences – surveillance for security of workplaces
Creates a defence to an offence against s35 where covert surveillance was deemed necessary to the safety and security of the workplace, and the employer notifies the workers affected. Records generated under this section are not admissible in evidence in a proceeding against the worker unless it relates to the security of the workplace or people within the workplace, or the desirability of admitting the evidence outweighs the undesirability of admitting evidence that has been obtained in the way in which the evidence was obtained.

Division 4.4 Reporting on covert surveillance authority

Clause 37 Offence – failure to give covert surveillance report
This clause creates an offence if an employer fails to provide the Magistrates Court with a written report on the stated information in the covert surveillance authority within 30 days of the end of the authority.

Clause 38 Orders for covert surveillance record
Provides that the Magistrates Court may make orders in regards to use or disclosure of covert surveillance records.

Division 4.5 Covert surveillance records

Clause 39 Offence – use and disclosure of covert surveillance other than for a relevant purpose.
Creates an offence to use or disclose information in covert surveillance records other than for a purpose set out in the authority, or in certain specific situations set out in the clause.

Clause 40 Information inadvertently obtained under covert surveillance authority

This clause provides that information inadvertently obtained under a covert surveillance authority is admissible as evidence in a criminal proceeding, except where the application for the covert surveillance authority was not made in good faith.

Part 5 – Prohibited surveillance

Clause 41 Offence – surveillance of private areas etc
This clause creates an offence if an employer conducts surveillance of any kind in the prohibited areas set out in the clause or prescribed by regulation

Clause 42 Surveillance of workers not at work
This clause creates an offence if the employer conducts surveillance of a worker not at work. The clause makes an exception for surveillance of equipment or resources provided by the employer, if the tracking function of a device cannot be turned off, or the employer is a law enforcement agency.

Clause 43 Use and disclosure of certain tracking device records.

Provides that data gathered on a worker not at work from a tracking device that cannot be turned off must not be used or disclosed for any purpose.

Part 6 – Miscellaneous

Clause 44 Offences – security of surveillance records
This clause requires an employer to take reasonable steps to secure surveillance records and to de-identify or destroy surveillance records no longer needed for any purpose under the Act, and makes it an offence if the employer fails to do so.

Clause 45 Report on covert surveillance authority to Legislative Assembly
This clause provides that the Minister must provide a report each year to the appropriate Legislative Assembly committee on the use of covert surveillance records in the Territory.

Clause 46 Approved forms
Provides that the Executive may approve forms for this Act

Clause 47 Regulation-making power
Provides that the Executive may make regulations for this Act

Clause 48 Review of Act
Requires that the minister must review the operation of this Act after the end of its first year of operation.

Clause 49 Court Procedures Act 2004 – New section 41 (2) (fa)
Inserts a reference to the Act in the *Court Procedures Act 2004*.