Workplace Surveillance Bill 2010

EXPOSURE DRAFT

Consultation period: 24 March - 3 June 2010

Amanda Bresnan MLA

The ACT Greens are calling for public submissions on the exposure draft of the Workplace Surveillance Bill 2010.

The exposure draft of the bill is available at

http://www.legislation.act.gov.au/ed/db_37432/default.asp

Employer groups, unions, privacy groups, the security industry and any other interested members of the community are encouraged to comment on this draft bill. Questions have been provided to guide submission responses. Submissions may either choose to respond to the questions, or to any other matter relevant to the Bill.

How to Make a Submission

Email: BRESNAN@parliament.act.gov.au

Please put "WORKPLACE SURVEILLANCE BILL SUBMISSION" in the title of your email.

Mail: Workplace Surveillance Bill Submissions
c/o Amanda Bresnan MLA
GPO Box 1020
Canberra ACT 2601

Please include your name and organisation (if any) with all submissions.

The closing date for submissions is close of business 3 June 2010.

Overview of the Bill

The *Workplace Surveillance Bill 2010* (the Bill) seeks to regulate the conduct of surveillance of workers in the workplace by employers. The Bill proposes to establish approved means by which employers can conduct surveillance of their employees, with a focus on notification and disclosure of the purposes, duration and methods of surveillance prior to its commencement.

It is widely accepted that most Canberrans will spend a very significant period of their lives at some form of work. The ACT Greens believe that people should be able to engage in work without threat to their human rights. We further believe that the employer-worker relationship should be built upon trust and respect wherever possible.

People in the ACT, along with most others in the developed world, have experienced an ever-increasing amount of surveillance in their lives. As technology has developed, it has made it increasingly easy to engage in intrusive surveillance activity. Cameras have gotten smaller and easier to conceal, email and internet monitoring systems have become more sophisticated, and the onset of widespread satellite and GPS technology has enabled a person's location to be constantly monitored in real time.

The emergence of these technologies has been able to facilitate benefits for businesses and society at large. They provide the ability to have instantaneous real-time communication and the monitoring of businesses. There is a down-side however in that these technologies can impact on the privacy of employees in the workplace.

The ACT, as well as other jurisdictions in Australia and around the world, have seen a range of violations of worker privacy through misuse of surveillance technology. These include:

- Reading and forwarding of private emails from workers
- Use of tracking technology to monitor worker activities after working hours
- Uploading and subsequent distribution of embarrassing surveillance footage via the internet
- Concealing hidden cameras within the workplace to monitor work and non-work activities without employee's knowledge

The Greens recognize that surveillance is a legitimate tool for ensuring workplace security, employee monitoring and managing health and safety hazards. In recognition of this fact, care has been taken to ensure that, under the Bill, employers can continue to engage in all forms of surveillance necessary to the ordinary operation of a business. The Bill focuses on creating an environment of full disclosure for overt surveillance, severely limiting the use of covert surveillance to unlawful activities only, and prohibiting some forms of surveillance of non-work areas where there is a heightened expectation of privacy.

In addition, the Greens acknowledge that some households may use cameras as part of their home security decisions. The Bill will not apply to cameras in households, even when that household may have hired a worker to assist with domestic duties.

Parts of the Bill are based upon the NSW *Workplace Surveillance Act 2005* and the Commonwealth *National Privacy Principles*.

Explanation of the Draft Bill and Discussion Questions

The Workplace Surveillance Bill divides surveillance into three forms: notified; covert; and prohibited

NOTIFIED SURVEILLANCE (PART 3 OF THE BILL)

Notification

Overt surveillance, for the purposes of the Bill, is any form of legitimate surveillance for which a worker has been properly notified in advance.

Notification must inform the worker of:

- The type of surveillance device to be used
- How the surveillance will be conducted
- When the surveillance will start
- Whether the surveillance will be continuous or intermittent
- Whether the surveillance will be for a stated period or ongoing

This notification must be provided to the worker 14 days prior to the commencement of the surveillance. Transitional arrangements for surveillance currently underway will be discussed later in the paper.

QUESTION

Should a worker be notified of the purpose of the surveillance (i.e. whether or not it will be used to monitor employee performance in addition to any other function)?

QUESTION

Is the information provided via the notification process appropriate and sufficient?

Specific Requirements for particular types of surveillance devices[*]

Optical Surveillance Devices (section 14)

Optical devices are defined as any device which can visually record an activity. It is expected that this section of the Bill will primarily apply to fixed security cameras in workplaces.

[*] The definitions for these types of surveillance are drawn from the *Crimes (Surveillance Devices) Bill [2009]* for consistency.

The particular requirement for optical surveillance devices is that the device (or a housing/casing that indicates the presence of the device) is clearly visible. In addition, signs must be placed at the entrance to the workplace indicating that workers may be subject to optical surveillance whilst in the workplace. The employer will not be required to formally notify a worker in a situation where that worker is not in their ordinary workplace.

Data Surveillance Devices (section 15)

Data surveillance devices are defined as any device or program capable of monitoring or recording the input or output of a computer (as broadly defined, this will include devices such as mobile phones or any other data device).

An employer will be required to develop a policy for the usage and monitoring of data devices, and notify their worker in such a way that they would be reasonably aware of the operation of that policy. Data surveillance can only then take place in accordance with that policy (although that policy is able to be changed, provided that reasonable notification is given)

Tracking Surveillance (section 16)

Tracking devices include GPS monitors, RFID tags or any other device that can be used to determine and record a workers location. We expect that where a mobile phone or data device is used to record the location of a worker, that this section will apply to the usage of those records.

In addition to normal notification requirements, employers will be required to place a notice on the device that is being tracked that states that it may be used to track the worker.

QUESTIONS:

Are the specific notification provisions for each type of surveillance device appropriate? Are the definitions listed appropriate for workplace surveillance, and should any other specific type of surveillance devices be included?

ELECTRONIC COMMUNICATIONS

Sections 19 and 20 of the Bill outline the requirements (and associated offences) for restricting access to electronic communications or websites. The Bill requires that an employer only restrict website and electronic communication access in accordance with a policy of the employer on electronic communication and internet access, where that policy has been clearly communicated to the employee.

These sections also require an employer to provide a *stopped delivery notice* in the event that the employer stops a communication in accordance with the policy. Exceptions are created for spam, communications which may cause damage to a computer or network, and anonymous communications.

QUESTION

Is this the best or most appropriate manner in which to inform a worker that a communication has been blocked? Should a worker be notified if a specific communication is read by a third party?

Section 20 prevents an employer from restricting access to a website or blocking communications purely on the basis that the communication or website is from an industrial organisation or relates to industrial matters. It should be noted that this does not require an employer to permit access to websites or electronic communications relating to industrial organisations or matters where those websites/communications would be blocked under a more general policy (for example if a worker is only permitted access to 'whitelisted' websites directly relevant to their work).

USE AND DISCLOSURE OF SURVEILLANCE RECORDS

Sections 21 and 22 are partly based upon the Commonwealth National Privacy Principles, and establish offences for inappropriate use or disclosure of surveillance records, and provide a limited right for an employee to access a surveillance record relating to themselves as a worker.

The right to access is necessarily limited to prevent frivolous or vexatious requests, requests which would violate the privacy of other employees or persons, or for a range of other matters specified in the legislation.

COVERT SURVEILLANCE (PART 4 OF THE BILL)

This part of the Bill outlines the requirements for conducting covert surveillance in the workplace. It limits the use of covert surveillance to when an employer can demonstrate that there is evidence of unlawful activity in the workplace. The employer is required to apply to the Magistrates Court for an authority, to be determined upon a range of criteria set out in the Bill. An employer will be required to nominate a fit and proper person, with the requisite experience, to be the *surveillance supervisor*, who will oversee the conduct of the surveillance, and has responsibility for passing on any data relevant to unlawful activity onto the employer. Surveillance records generated by covert surveillance that are not relevant to the discovery of unlawful activity are not to be used for any purpose, and are to be destroyed within a short period following the cessation of the surveillance authority.

Offence - Conduct of Covert Surveillance without an Authority

This Part of the Bill establishes an offence to conduct covert surveillance without an authority. It is a defence against this offence if it can be demonstrated that *specifically* covert surveillance is material to, and only used for, the security of the workplace, and that the covert surveillance was notified in accordance with the notification provisions in the previous section.

Application for Surveillance Authority

Section 25 of the Bill outlines the requirements for a covert surveillance authority application. This application must specifically include:

- The grounds the employer has for suspecting unlawful activity in the workplace
- Actions that the employer has taken to detect the suspected unlawful activity to date
- The name(s) of the worker(s), as well as a description of the place, computer, vehicle or other thing that will be regularly and ordinarily subject to covert surveillance
- The kind of device proposed to be used
- The proposed period of surveillance
- The existence and result of any previous application for a covert surveillance authority
- The proposed surveillance supervisor
- Anything else prescribed by regulation

QUESTION

Is this list of requirements appropriate and sufficient for a covert surveillance authority application?

The hearing for a covert surveillance authority will need to be held in private. The grounds on which the Magistrates Court may consider issuing a covert surveillance authority is as follows:

- The seriousness of the suspected unlawful activity
- The potential intrusion upon another worker or person's privacy
- If the surveillance is proposed to be conducted in a non-work area that isn't prohibited by the Bill, a workers heightened expectation of privacy for that area
- Whether there are any other appropriate means of discovering unlawful activity in the workplace
- Whether it is more appropriate that the suspected unlawful activity is investigated by police
- The suitability of the nominated workplace surveillance supervisor

QUESTION

Are there any other considerations that the Magistrate's Court should make in considering whether or not to grant a covert surveillance authority?

Contents of a Covert Surveillance Authority

A covert surveillance authority must list specifically the duration, location, type of device, workers who will be subject to surveillance, as well as any additional conditions placed upon the authority, as well as the reporting and disclosure requirements under section 36 and section 38 of the Bill.

The duration of a covert surveillance authority may be no longer than 30 days under the Bill, although this may be changed by regulation.

QUESTION

Are the penalties for the offences listed in Part 4 of the Bill appropriate?

Use and disclosure of covert surveillance records

The surveillance supervisor (or supervisors) is responsible for reviewing covert surveillance records. The supervisor(s) may only release to the employer parts of covert surveillance records directly related to unlawful activity in the workplace. It should be noted that this is open to any unlawful activity that occurs, not just the unlawful activity that was specified in the original application.

It will be an offence to knowingly use or disclose covert surveillance records other than in line with the conditions laid out in the Bill and the relevant covert surveillance authority. A further list of exemptions is laid out in section 38 (3).

It should be noted that if an employer engages in unlawful covert surveillance, the record generated by that surveillance may still be used against the employee, even though the employer has committed an offence in unlawfully conducting covert surveillance without an authority.

QUESTION

Should the Court have the power to compel an employer to disclose surveillance records to employees not involved in or suspected of unlawful activity?

Where an employer will use all or part of a covert surveillance record to take detrimental action against an employee, an employee has a right to access the relevant part of the surveillance record being used against them.

Covert Surveillance Report

An employer is required to give a report upon the conduct of the surveillance within 30 days after the expiry of the authority. The report must list the duration, location, type of device, workers who were subject to surveillance, details of any surveillance records generated under the authority, reasons (if any) that the records should be concealed from any worker, actions taken as a result of information gained under the authority, as well as any additional conditions placed upon the authority.

The Court may make orders in regard to records generated by the authority, including orders for the record to be passed over to the court for safekeeping or action, or disclosure to an employee. The Court must make an order to disclose the record to an employee unless the Court is satisfied that there is good reason for not doing so.

PROHIBITED SURVEILLANCE (PART 5 OF THE BILL)

This part of the Bill makes it an offence to conduct any form of surveillance of certain non-work areas where there is a particularly heightened expectation of privacy, including sick bays, toilets, parenting facilities and prayer rooms.

This Part of the Bill also makes it an offence for an employer to conduct surveillance of a worker when not at work. There are exceptions built in for tracking devices that cannot be

turned off (where an employer is required to not use data generated by the device after hours for any purpose) and for employer-provided computer equipment, which may be subject to a notified computer surveillance policy as per the Notified Surveillance part of the Bill.

MISCELLANEOUS PROVISIONS (PART 6 OF THE BILL)

This part of the Bill makes it an offence to not take reasonable steps to prevent unauthorised access or use of surveillance records, and if the employer fails to de-identify or destroy a surveillance record where it is no longer needed for any purpose.

It also requires the relevant Minister to give a report to the Assembly upon a range of matters relating to covert surveillance authorities in the previous year, and a requirement to review the operation of the Act after a year.