NSW Legislative Council Hansard

Workplace Surveillance Bill

Extract from NSW Legislative Council Hansard and Papers Tuesday 21 June 2005.

Second Reading

The Hon. HENRY TSANG (Parliamentary Secretary) [3.18 p.m.]: I move:

That this bill be now read a second time.

The Workplace Surveillance Bill will create a sensible and practical system for regulating workplace surveillance by employers of employees. I seek leave to have the second reading speech incorporated in *Hansard*.

Leave granted.

Before I go into the detailed provisions of the Bill, I think it would be useful to briefly remind honourable members of its history. In 1998 this Government introduced the *Workplace Video Surveillance Act 1998*, which established a new system of regulation for video surveillance in the context of employment. The *Workplace Video Surveillance Act 1998* arose out of a number of industrial disputes over video surveillance by employers and was the result of extensive consultations between employee and employer organisations. The Act was the first of its kind in Australia.

The *Workplace Video Surveillance Act 1998* essentially prohibits video surveillance in the workplace unless certain notice requirements are satisfied, or a Magistrate has authorised covert video surveillance to establish whether employees are involved in any unlawful activity.

In 2003 submissions to the statutory review of the *Workplace Video Surveillance Act 1998* were received from both industrial organisations and employer groups, and none identified significant deficiencies in the *Workplace Video Surveillance Act 1998*"s operation. The Workplace Surveillance Bill, which I am introducing, was therefore modelled on the *Workplace Video Surveillance Act 1998*.

The Bill repeals and replaces the *Workplace Video Surveillance Act 1998*, which applied only to video surveillance. In general it takes the *Workplace Video Surveillance Act 1998* as a template and extends its provisions in a number of ways.

In June 2004 I tabled an exposure draft Workplace Surveillance Bill to provide unions, employees and the owners of small and large businesses the opportunity to have input into the development of a comprehensive commonsense solution to new workplace surveillance issues. A large number of submissions were received and the exposure draft Bill has been amended to take into account numerous concerns of stakeholders.

As the use of technology has grown, it has become apparent that the provisions of the *Workplace Video Surveillance Act* were not wide enough to protect employees from intrusive acts of covert surveillance. People are concerned that what they considered to be essentially private communications by way of email, may end up being intercepted and read by employers. Technological advances allow small tracking devices to transmit movements outside of the traditional workplace, and the capture of every word typed into a computer.

This Bill ensures that employees are made aware of any such surveillance. It extends to computer surveillance (surveillance of the input, output or other use of a computer by an employee) and tracking surveillance (surveillance of the location or movement of an employee). It restricts and regulates the blocking by employers of emails and Internet access of employees at work. It extends beyond the traditional workplace to any place where an employee is working.

In common with the *Workplace Video Surveillance Act 1998* the Bill creates a general prohibition on surveillance by employers of their employees at work unless employees have been given notice of the surveillance in accordance with the Bill, or unless the surveillance is carried out under the authority of a covert surveillance authority issued by a Magistrate. Covert surveillance authorities can only be issued for the purpose of establishing whether or not an employee is involved in any unlawful activity at work.

The Bill regulates the carrying out of surveillance under a covert surveillance authority, and the storage, use and disclosure of covert surveillance records.

It does not create an enormous burden on employers. While it is true that the notification regime seeks to ensure that employees are made aware of any surveillance being conducted by an employer, notification is not itself an onerous requirement. Essentially, the Bill promotes transparency in the workplace, obliging employers

to be open about surveillance practices.

I turn now to the major provisions of the Bill.

Part 1 contains preliminary matters such as definitions. It defines 'covert surveillance' to be any surveillance by an employer of an employee while at work for the employer that is not in compliance with the notification requirements in Part 2. In effect this creates a presumption that surveillance is covert unless the notification requirements are met. An employee is considered to be 'at work' when they are at a workplace of the employer, or if they are anywhere else while performing work for the employer.

'Surveillance' is defined to cover 'camera surveillance', 'computer surveillance' and 'tracking surveillance'. In each case there must be 'surveillance', as that term is commonly understood.

'Camera surveillance' is surveillance by means of a camera or other electronic device that monitors or records visual images of activities on premises or in any other place. This includes 'still' photographs.

'Computer surveillance' is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer. It includes the sending and receipt of emails and the accessing of Internet websites. It is important to note that this does not mean that all monitoring or recording of the use of a computer is 'computer surveillance'. The Bill requires there to be 'surveillance', as that term is ordinarily understood.

The definition of 'computer surveillance' therefore does not cover normal business practices such as back-ups of hard drives, network performance monitoring, software licence monitoring, computer asset tracking, computer asset management or the normal saving of documents, because these are not normally considered to be "surveillance" activities. However, if back-ups, for instance, were to be used to conduct surveillance to facilitate the reading of somebody's emails, that would need to be notified to employees, otherwise it would be considered to be covert surveillance.

This is a common sense approach to the issue of computer surveillance. There are obviously many functions of a computer that require the recording of activities. This has been acknowledged. Only surveillance activities, such as reading emails, or watching every web site a person goes to, or logging individual keystrokes, or covert observation of everything an employee does on their machine, require notification.

I will return later to the issue of computer surveillance as it has generated the most comment in submissions to the draft exposure Bill.

'Tracking surveillance' is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement. This has been amended from the exposure draft to focus on things such as Global Positioning System (GPS) devices which allow real time tracking of an object's location. This is to ensure that 'tracking surveillance' does not capture things like mobile phone or credit card records that may incidentally show an employee's location.

The definitions of 'employer' and 'employee' take their meaning from the *Industrial Relations Act 1996* and include people performing voluntary work and people working under labour hire contracts.

Part 1 also spells out that requirements imposed by or under the *Occupational Health and Safety Act 2000* do not limit or otherwise affect the operation of this Bill. This is to remind employers not to use occupational health and safety issues as an excuse for conducting covert surveillance. Should an employer believe they need to urgently conduct covert surveillance for occupational health and safety reasons, they should use the existing occupational health and safety consultation regime (under Part 2, Division 2 of the *Occupational Health and Safety Act 2000*) to get agreement for any surveillance. Clause 14 of this Bill makes it clear that such an agreement will ensure that any such surveillance will not be considered covert, notwithstanding that none of the notification requirements of Part 2 have been met.

Part 2 outlines the notification requirements for surveillance not to be considered covert. Essentially, employees must be given written notice 14 days prior to any surveillance commencing. This notice, which can be sent via email, must indicate the kind of surveillance to be carried out; how the surveillance will be carried out; when the surveillance will start; whether the surveillance will be continuous or intermittent; and whether the surveillance will be for a specified limited period or ongoing. An exemption applies in the case of camera surveillance of an employee working somewhere that is not their usual workplace. This is to ensure that large employers, with many workplaces, are not required to notify individual employees each time they happen to go to a different workplace to usual, for instance to attend a meeting.

Each of the three types of surveillance also has additional requirements. For 'camera surveillance' cameras used for the surveillance (or camera casings or other equipment that would generally indicate the presence of a camera) must be clearly visible in the place where the surveillance is taking place. Signs must also notify

people that they may be under surveillance in that place and must be clearly visible at each entrance to that place. These mirror the requirements under the *Workplace Video Surveillance Act 1998*.

For "computer surveillance" the surveillance must be carried out in accordance with a policy of the employer on computer surveillance. The policy must be notified in advance to an employee in such a way that it is reasonable to assume that the employee is aware of and understands the policy.

For "tracking surveillance" there must be a notice clearly visible on the vehicle or other thing that is being tracked, indicating that the vehicle or thing is the subject of tracking surveillance.

As previously mentioned in relation to occupational health and safety issues, clause 14 allows an exemption from these requirements where employees (or a body representing a substantial number of employees) have agreed to the use of the surveillance for a purpose other than surveillance of the activities of employees and the surveillance is carried out in accordance with that agreement. For instance, employees may agree that a workplace be the subject of camera surveillance under an industrial agreement.

Part 3 outlines prohibitions on surveillance. Clause 15 prohibits surveillance of employees in change rooms, toilets, showers or other bathing facilities at a workplace. Clause 16 prohibits the continuation of surveillance when an employee is not at work, except computer surveillance of the use by the employee of equipment or resources provided by or at the expense of the employer (such as laptops, internet accounts, email accounts, network resources, information systems). This will ensure, for instance, that employers will not be prevented from conducting computer surveillance of work laptops, to ensure that pornography is not being downloaded.

Clause 17 provides that an employer must not prevent the delivery of emails or block access to Internet websites unless this is in accordance with a policy that has been notified in advance to an employee in such a way that it is reasonable to assume that the employee is aware of and understands the policy. Employees must also be notified of any blocked emails, unless an exemption applies. The exemptions extend to emails that are believed to be spam (as defined by the *Spam Act 2003* of the Commonwealth), or believed to contain viruses, trojan horses, or offensive and harassing material.

However, an employer's policy cannot provide for the blocking of email or access to a website merely because the content relates to industrial matters. The final part of clause 17 states that an employer's policy on email and Internet access cannot provide for preventing delivery of an email or access to a website merely because:

(a) the email was sent by or on behalf of an industrial organisation of employees or an officer of such an organisation, or

(b) the website or email contains information relating to industrial matters (within the meaning of the *Industrial Relations Act 1996*).

This provision is to meet concerns that employers could otherwise deliberately block emails sent by industrial organisations. However, it is not the case that this will require employers to provide email access to employees, nor that this will require employers to provide Internet access to particular websites. The key phrase here is "merely because".

For example, if an employer has a policy of not allowing access to any external Internet sites on its computers, there will be no compulsion to provide access to websites containing information relating to industrial matters. This is because Internet access to the website containing industrial matters is being prevented on the basis that all access to external websites is blocked.

Similarly, if an employer operates a "white list", that is, a list of Internet websites that access is provided to, the employer will not be forced to add websites containing industrial matters to the "white list".

An employer will however be prevented from adding Internet websites containing industrial matters to any "black list", that is, a list of Internet websites that are blocked, unless there is a reason for doing this other than the fact that the website contains industrial matters. For instance, if a website containing industrial matters also contained content that was considered to be harassing or offensive, an employer would be able to block access on that basis.

Part 4 provides the regulatory framework for covert surveillance of employees at work. These provisions have been based on those in the *Workplace Video Surveillance Act 1998*.

It will be an offence for an employer to carry out, or cause to be carried out, covert surveillance of an employee while at work for the employer unless the surveillance has been authorised by a covert surveillance authority. Covert surveillance authorities may only be issued for the purpose of establishing whether or not one or more particular employees are involved in any unlawful activity while at work for the employer. They do not authorise the covert surveillance of an employee for the purpose of monitoring an employee's work performance, nor in

any change room, toilet facility, shower or other bathing facility.

There are exceptions for law enforcement agencies, correctional centres, casinos and legal proceedings. These mirror the exceptions in the *Workplace Video Surveillance Act 1998*.

It will not be an offence for an employer to carry out covert surveillance solely for the purpose of ensuring the security of the workplace or persons in it. This will apply if there was a real and significant likelihood of the security of the workplace or persons in it being jeopardised if the covert surveillance was not carried out and the employer has notified employees of the intended surveillance. This mirrors the provisions in the *Workplace Video Surveillance Act 1998*.

Applications for covert surveillance authorities are to be made to Magistrates. Applications must include the following information:

(a) A statement of the grounds the employer has for suspecting that particular employees are involved in unlawful activity, together with the names of those employees (unless it is not practicable to name them). This is needed to justify that the authority should be issued. The employer must have some evidence to substantiate any suspicions.

(b) A statement as to whether other managerial or investigative procedures have been undertaken to detect the unlawful activity and what has been their outcome. This is necessary to ensure that covert surveillance is not always the first and last option considered by an employer. There may be other, simpler and less intrusive ways to deal with suspected crime in the workplace in the first instance.

(c) The names of the employees or (if it is not practicable to name them) a description of the group or class of employees who will regularly or ordinarily be the subject of the covert surveillance. This is to help the surveillance supervisor be aware of who will be subject to the covert surveillance, so that any covert surveillance does not extend beyond reasonable bounds.

(d) A description of the premises, place, computer, vehicle or other thing that will regularly or ordinarily be the subject of the covert surveillance.

(e) A statement as to the kind of covert surveillance (camera, computer or tracking) that is proposed to be conducted.

(f) The dates and times during which the covert surveillance is proposed to be conducted. This is to control the operation of the authority and ensure that the surveillance is not conducted as an open-ended operation.

(g) A statement as to whether any previous application for a covert surveillance authority has been made in respect of the proposed covert surveillance and a statement as to the results of the application and of any covert surveillance conducted under a covert surveillance authority issued as a result of the previous application.

(h) In the case of an application made by an employer's representative, verification acceptable to the Magistrate of the employer's authority for the person to act as an employer's representative for the purposes of the covert surveillance operation.

The Magistrate can require further information, and applications are to be dealt with in closed court. The Magistrate must not issue a covert surveillance authority unless satisfied that there are reasonable grounds to justify its issue. In making such a determination the Magistrate will take into account matters such as the strength and seriousness of the employer's suspicions, what other actions the employer has taken to investigate these suspicions and the invasion of privacy that employees will suffer as a result of the surveillance. The Bill sets a tougher test if an employer wishes to place a recreation room, meal room or any other part of a workplace in which employees are not directly engaged in work under surveillance. This mirrors the *Workplace Video Surveillance Act 1998*.

The *Workplace Video Surveillance Act 1998* contained a requirement that a person holding a Class 1 licence issued under the *Security (Protection) Industry Act 1985* (since repealed by the *Security Industry Act 1997*) oversee the conduct of authorised covert video surveillance. Class 1 licences were issued, amongst other things, to people employed to install electronic equipment designed to provide security or watch property. A similar licence requirement has not been included in the Bill.

Instead, a Magistrate must be satisfied that the person designated to act as a surveillance supervisor under a covert surveillance authority has qualifications or experience that suit the person to be responsible for overseeing the conduct of the surveillance operations.

It is important to note that the requirements of the *Commercial Agents and Private Inquiry Agents Act 1963*, the

Commercial Agents and Private Inquiry Agents Act 2004, and the *Security Industry Act 1997* are not affected by this Bill. People will still need to obtain the appropriate licences required under these Acts for activities covered by these Acts. Simply having a covert surveillance authority will not absolve someone from any other legal requirement to hold a private inquiry agents licence or security industry licence when conducting surveillance or installing surveillance equipment.

Covert surveillance authorities will be in the form prescribed by the regulations. They will specify information relevant to the covert surveillance, such as the type of surveillance, the names of the people suspected of unlawful activity, the dates and times during which the surveillance is authorised, the places and things that are to be subject of the surveillance, the name of designated surveillance supervisors, the period the authority remains in force, the period for which the authority remains in force and the conditions to which the authority is subject.

Covert surveillance authorities remain in force for a period not exceeding 30 days, as specified in the authority. They are subject to conditions, mirroring the conditions in the *Workplace Video Surveillance Act 1998*. In brief these require that:

• Surveillance supervisors can only give employers access to those portions of surveillance records relevant to establishing the involvement of employees and others in unlawful activity;

• Surveillance supervisors must erase or destroy all parts of a surveillance record, not required for evidentiary purposes, within three months of the expiry of the authority;

• Employees must be provided with access to covert surveillance records that are to be used in taking detrimental action against the employee.

Contravention of a condition of a covert surveillance authority, or causing the contravention of a covert surveillance authority, is an offence.

Covert surveillance authorities can be varied or cancelled by a Magistrate, who must keep a record of all relevant particulars of any issue, variation or cancellation of an authority. Again, this mirrors the conditions in the *Workplace Video Surveillance Act 1998*.

A report must be given to the Magistrate on the use of a covert surveillance authority, within 30 days after the expiry of the authority. Failure to provide a report will be an offence. The report must set out briefly the result of the surveillance and specify other details as required, including any reasons why an employee who was the subject of the surveillance should not be informed of the surveillance. The Magistrate may then make such orders as considered appropriate with respect to the use or disclosure of any surveillance record, including that the record be delivered up to the Magistrate or that the surveillance record be given to a particular person or body. A Magistrate must make an order informing a person who was the subject of the surveillance unless there is good reason not to. In determining this, the Magistrate is to consider whether the surveillance was justified and whether it was an unnecessary interference with privacy.

Covert surveillance records must be properly stored and protected against loss or unauthorised access or use. Failure to do so will be an offence.

Covert surveillance records must only be used or disclosed for a relevant purpose. Other uses or disclosures will be an offence. Where covert surveillance has been authorised, the Bill makes it clear that it is acceptable for the records to be used:

• as authorised or required under the conditions of the covert surveillance authority;

• to establish whether or not an employee is involved in unlawful activity while at work for the employer;

• to take disciplinary action or legal action against an employee as a consequence of alleged unlawful activity while at work for the employer;

• to establish security arrangements or take other measures to prevent or minimise the opportunity for unlawful activity while at work for the employer of a kind identified by the surveillance record to occur while at work for the employer;

• to avert an imminent threat of serious violence to persons or of substantial damage to property;

• to disclose to a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence; and

• for purposes related to the taking of proceedings for an offence or for taking any other action required or authorised under the Bill.

This is to ensure that covert surveillance records are not used for frivolous, vexatious, or any other irrelevant purposes.

Where covert surveillance of an employee has not been authorised, use or disclosure is only allowed for a

purpose related to the taking of proceedings for an offence or by and to law enforcement agencies for any purpose in connection with the detection, investigation or prosecution of an offence.

Part 5 contains miscellaneous provisions. It includes that appeals are to be heard by judicial members of the Industrial Relations Commission; that the Minister is to report to Parliament each year on covert surveillance authorities issued during the year; and that regulations may be made by the Governor. Schedule 1 includes savings and transitional provisions, including that surveillance records and information obtained before commencement are not subject to clause 36 (concerning use of covert surveillance records for relevant purposes only).

I wish finally to return to computer surveillance. Numerous concerns have been raised about the intention to cover computer surveillance. I will therefore pay particular attention to this aspect of the Bill.

There is an urgent need for a new system of regulation for the surveillance of computer communications, which strikes a fair balance between an employer's right to limit use by employees of a computer network provided in the workplace, and the employees' reasonable expectations of privacy. Some blocking of electronic communications by employers is clearly desirable, for example to prevent employees from receiving spam, viruses or offensive material. However, there have reportedly been cases where employers have caused messages relating to trade union activities to be blocked.

Consistent with the general scheme contained in the Bill, it will be an offence for an employer to monitor an employee's use of e-mail and the internet unless certain notice requirements are satisfied, or a covert surveillance authority is obtained from a Magistrate.

The notice requirements for computer surveillance are not onerous. They do not require notices on computers nor a notice each time an employee logs onto a computer. During consultation employers indicated that prescribing such requirements would be costly, especially for small business. Some employers indicated they already had in place suitable, but different, notification systems for ensuring that employees were aware of their computer, Internet and email surveillance policy.

The Bill places an obligation on employers to ensure employees are notified of any computer surveillance and email and Internet access policy in such a way that is it reasonable to assume that the employee is aware of and understands the policy. This is surely best practice and should not trouble employers. An example of such a system for a larger employer is one including induction and training courses and regularly emailed reminders. An example for a small business is individual discussion of the employer's policy with each employee and placing the policy on a work noticeboard.

Employers will also be required to give notice to an employee on any occasion when an e-mail message sent by or to the employee is blocked (that is, prevented from reaching its intended recipient). Such notice is not required if the email has been blocked because it was spam, contained a virus, or was harassing or offensive (for example, if it is pornography). It will be unlawful for an employer to block an e-mail message, or access to a website:

- otherwise than in accordance with the employer's stated policy on e-mail and internet use; or
- solely because the message or website includes information relating to industrial matters.

While employers needs to be able to monitor emails received by their employees, indiscriminate use of such technology can result in breaches of employee privacy. What we are seeking is for these competing interests to be addressed in a sensible and workable manner.

A number of amendments were made to the exposure draft Bill to take account of concerns raised in submissions on the draft Bill. These amendments:

- introduce more flexibility into notification procedures;
- ensure that use of anti-virus and anti-spam software is not affected;
- make it clear that an employer only has to give notice of their computer surveillance policy and not notice of every individual act of computer surveillance;
- allow accepted business practices; and
- address the use of work computers at home.

In conclusion, the Government considers, as it did with the *Workplace Video Surveillance Act 1998*, that this Bill provides an appropriate balance between workers' expectations of privacy and the genuine concerns of employers to protect their workplaces from unlawful activity by regulating the use of covert surveillance of employees at work.

I commend the Bill to the House.