Australian
Privacy
Foundation

16 May 2005

Analysis of the Workplace Surveillance Bill 2005

Introduction

This paper sets out the Australian Privacy Foundation's analysis of the *Workplace Surveillance Bill 2005 (NSW)*.

The Workplace Surveillance Bill represents a step forward in terms of tackling the issue of employee privacy, while also being mindful of employers' interests in preventing unlawful behaviour in the workplace.

However the Bill has several key deficiencies, the most significant of which are the failure to regulate overt surveillance, and the failure to provide remedies for employees who suffer a breach of privacy as a result of workplace surveillance. We suggest that both employees and employers would benefit from a Bill which provided greater clarity in the area of overt surveillance.

It is our view that unless modified, this Bill represents more a lost opportunity than a serious attempt at law reform in the contentious area of workplace privacy. This paper therefore includes a number of suggestions for how the Bill could be modified to provide greater privacy protection to employees, and greater clarity and certainty for employers.

Overt surveillance

The Bill follows the approach of the existing Workplace Video Surveillance Act 1998 (NSW), by allowing overt surveillance with minimal regulation by way of notice requirements, and then defining every incidence of workplace surveillance which does not comply with the notice requirements as its opposite - 'covert surveillance'. Only the conduct of covert surveillance is then further regulated by the Act.

This strict 'overt / covert' dichotomous approach has two disadvantages:

- it effectively incorporates operational requirements into the very definition of covert surveillance, such that a failure to meet one of the notice requirements in Part 2 of the Bill moves conduct from being treated as overt and lawful into the opposing category of covert (and thus generally unlawful), and
- there is no regulation of overt surveillance beyond its requirement to meet the definition of overt surveillance.

This approach benefits neither employer nor employee.

No privacy for employees

Employees continue to have no privacy protection for the collection, storage, use or disclosure of information gathered through overt surveillance, beyond the notification and signage requirements of Part 2 of the Bill, which are necessary to avoid being deemed to be conducting unlawful covert surveillance. Due to the inadequacies of existing information privacy laws in this area[1], employees are virtually powerless to prevent, or seek redress for, any misuse or unfair handling of their personal information gathered by way of overt surveillance.

The NSW Acting Privacy Commissioner has previously drawn the Government's attention to the high rate of telephone enquiries and complaints lodged with his office about the use of overt video surveillance in the workplace[2]. Privacy NSW has noted:

> Uncontrolled overt surveillance can contribute to stress and a sense of powerlessness. It has the potential to be abused, for example, by zooming in on individual employees or subjecting them to an unreasonable level of continuous monitoring. In the absence of privacy protection for employee records there is a capacity for misuse of stored images from video surveillance[3].

The figures for the 2002-03 annual report of Privacy NSW indicate that the volume of enquiries about surveillance has only continued to increase since the above submission was written[4].

A set of principles relating to overt surveillance in the workplace, which balance the competing interests of both parties, have already been developed by the NSW Government:

- in 1996 – the Department of Industrial Relations published the voluntary *Code of Practice for the Use of Overt Video Surveillance in the Workplace*. The Code established a series of standards for overt surveillance systems, such as restricting the hours in which surveillance should operate, providing guidance on storage, retention and employees' access to tapes, and providing guidance on the ethical use and disclosure of surveillance material.
- in 2001 - the NSW Law Reform Commission recommended a set of binding principles governing overt surveillance. The proposed principles included core standards such as that the surveillance must not breach reasonable expectations of privacy, must only be undertaken for acceptable purposes, and that use must be consistent with its purpose.[5]

Likewise the International Labor Office's *Code of Practice on the Protection of Workers' Personal Data* was settled in 1997, and contains principles relevant to overt surveillance of employees such as:

- information collected should be used lawfully and fairly, and only for reasons directly relevant to the employment of the worker

---

[1] There are exemptions for the employee records of private sector employees under the Federal Privacy Act 1988 and the NSW Health Records & Information Privacy Act 2002, and for any information about the suitability of public sector employees under the NSW Privacy and Personal Information Protection Act 1998 and the NSW Health Records & Information Privacy Act 2002.

[2] See Attachment 1 to *Submission by Privacy NSW to the Director General, NSW Attorney General's Department on the Workplace Video Surveillance Act Review*, October 2003, available from www.lawlink.nsw.gov.au/privacynsw

[3] See pp5-6 of the *Submission by Privacy NSW to the Director General, NSW Attorney General's Department on the Workplace Video Surveillance Act Review*, October 2003.

[4] See p20 of the Privacy NSW 2002-03 Annual Report.

[5] See the NSW Law Reform Commission, *Report 98, Surveillance : An Interim Report*, 2001.

- surveillance information should not be the only factor in evaluating performance
- employers must secure surveillance information against loss, unauthorised access, use, alteration or disclosure, and
- employees should have access to any surveillance information collected about them.

We suggest that in order to genuinely protect the privacy of employees, regulation of overt surveillance in the workplace is sorely needed. This Bill will not deliver any such protection.

No protection for employers

The risk to employers will be that a failure to meet the notice requirements in Part 2 of the Bill, even if simply through forgetfulness, will render the otherwise overt surveillance 'covert', and thus unlawful unless a magistrate's authority is first obtained. In doing so, the employer will commit an offence and may be fined $5,500[6], and they cannot use or disclose any information gathered through the surveillance except in relation to proceedings for an offence[7].

One example is the employer who accidentally gives only 13 instead of 14 days prior notice to employees that she is taking delivery of new fleet cars which will have their GPS systems switched on.

A second example is the home owner, who uses a CCTV system to protect their home against burglary. The system is not 'hidden', in that the camera casings can clearly be seen, and they even have a sign on a front window to indicate there is a security system with CCTV in place. The home owner employs a person to work at the home – a plumber, a cleaner, or a nanny – but forgets to provide them with written notice of the existence of the CCTV before the person commences work. The home owner is an employer[8], whose conduct does not meet the definition of 'notified surveillance'[9], and thus is now conducting 'covert surveillance' without lawful authority.

No privacy for customers or public either

Clause 14 allows overt surveillance conducted for a purpose 'other than surveillance of employees', where the employee (or a body representing a substantial number of employees) has agreed to that use, and the surveillance is 'carried out in accordance with that agreement'. This category thus requires none of the notification, visibility or signage requirements set out in the remainder of Part 2 of the Bill.

Thus it would appear that the Bill would allow for example hidden CCTV cameras in the foyer of a building, with no signage whatsoever. This is a significant departure from existing Government policy on the use of CCTV cameras in public places[10].

---

[6] See clause 18 in the Bill. The limited defence to prosecution in clause 21 won't address the scenarios outlined above.
[7] See clause 36 in the Bill.
[8] See the definition of 'employer' in clause 3 of the Bill.
[9] See clause 10(3) of the Bill – the usual requirement of providing 14 days notice prior to commencing surveillance (see clause 10(2)) sensibly does not apply in cases where the surveillance existed before the employee commenced working for the employer, but under clause 10(3) the employee must still be given notice in writing "before the employee starts work".
[10] See part 14 of the NSW Government *Policy Statement and Guidelines for the Establishment and Implementation of Closed Circuit Television in Public Places*, which also recommends the relevant Australian Standard, AS 2342 – 1992. The policy is available at http://www.lawlink.nsw.gov.au/cpd.nsf/pages/cctv_index .

Furthermore clause 15 allows the use of hidden CCTV cameras in a toilet or change room used by clients (not employees), without either signage or notice, or a magistrate's authority[11]. The Bill would also appear to allow devices such as a web-cam set up in a child-care centre to broadcast images to any person, so long as the employees or the centre have agreed.

Conclusion : a lost opportunity to deal with overt surveillance

The development of this Bill would appear to be an opportune time to implement comprehensive privacy principles governing overt surveillance of employees, as previously recommended by the NSW Law Reform Commission, and, we had thought, as promised by the NSW Government. In the absence of such regulation, this Bill adds very little of the privacy protection promised for employees or the sensible guidance promised for employers.

In particular the above scenarios illustrate the difficulty in creating an absolute dichotomy between covert and overt surveillance, in which the former is tightly regulated with criminal sanctions and the latter is entirely unregulated, in circumstances where it is easy for the unwary employer to slip from the latter category into the former.

This is not an argument in favour of lessening the requirements on those conducting overt surveillance. Our argument is that the dichotomous approach is not a workable model, when seeking to ensure an approach to surveillance regulation which adequately balances competing interests.

We therefore suggest that specific regulation of overt surveillance is needed - to include both notice requirements, but also other requirements relating to the operation of overt surveillance, and the collection, use, storage and disclosure of surveillance information obtained through overt surveillance.

Covert surveillance

Clause 18 prohibits covert surveillance of the employee at work without a magistrate's authority.

While this is a commendable development in the law, we are disappointed that it could potentially be undermined by the provision in clause 21, which provides a defence to prosecution in some circumstances. It is our submission that this particular clause undermines the basic rule in clause 18, by allowing an employer to conduct covert surveillance of employees without a magistrate's authority, and then if caught and prosecuted simply justify their actions as necessary for 'the security of the workplace or persons in it'. The employer can thus avoid both the up-front justification before a magistrate, and the post-hoc reporting requirements, for covert surveillance of employees that the Bill is predicated upon. It is difficult to see why any employer would bother complying with Part 4 of the Bill and seek a magistrate's authority at all.

[11] The prohibition on either overt or covert surveillance being conducted in a toilet area, change room, etc, only applies to surveillance of 'an employee'. Thus hidden cameras within public toilets or a changing room in a retail clothing store will not be prohibited by this Bill. Other privacy-related legislation is still inadequate in this area, as the capturing of images by small businesses is unregulated by the Federal Privacy Act. Filming for sexual gratification purposes will covered by the Summary Offences Act, but other types of surveillance will not.

Use of covert surveillance material

The Bill provides at clause 36(3) that illegally obtained surveillance material (that is, material gathered through covert surveillance that was not authorised) may still be used or disclosed in some circumstances.

There are two circumstances in which material could potentially be gathered through covert surveillance that was not authorised:

- the employer who intended to conduct 'overt' surveillance, but whose actions accidentally tipped them into the definition of 'covert' surveillance, and
- the employer whose intention was to conduct hidden surveillance, and who does so without obtaining the appropriate authorisation, whether through ignorance of the law or by intention.

That the Bill does not distinguish between these two categories is of concern, as previously dealt with above. Furthermore there should be a distinction between the covert surveillance which could have been carried out with a magistrate's authority but wasn't, versus that which could never have been authorised in the first place.

We suggest that any use or disclosure of illegally obtained surveillance material is inappropriate in circumstances where an authority to conduct the covert surveillance could not have been lawfully obtained in the first place. That is, where the purpose of the surveillance was outside the terms of clause 22 in the Bill (eg. if the covert surveillance is conducted with the purpose of monitoring an employee's work performance, or is conducted in a toilet facility), it is our argument that any use or disclosure of the surveillance material obtained must be prohibited.

We submit that if Parliament has set rules about when covert surveillance can not be authorised in the first place, a person who contravenes those rules should not be able to benefit from their unlawful conduct in any way. To prevent the use, disclosure, or admission into evidence of illegally obtained surveillance material, where its collection could never have been lawfully authorised in the first place, would also provide greater certainty and relief for the subjects of illegal covert surveillance. Such an approach would be consistent with the Legislative Council's recommendations in relation to illegally or improperly obtained forensic material[12].

Overt or covert surveillance of employees when they are not 'at work'

Clause 16 represents an improvement on earlier drafts of the Bill, which did not recognise that in this age of flexible work practices, that many workers for example will be 'connected' to a work email or internet account while on the road or at home.

However there is still no recognition that tracking devices on work-provided resources (such as vehicles or mobile phones) may also effectively track employees when they are not 'at work'. And the wording of clause 16 suggests that employers may conduct covert computer surveillance of employees while they are not 'at work', without any need for a magistrate's authorisation.

[12] Legislative Council Standing Committee on Law and Justice, *Review of the Crimes (Forensic Procedures) Act 2000*, Report 18, February 2002. See recommendation 51.

We suggest that clause 16 should be amended so that surveillance of an employee can include when the employee is *not* 'at work' but nonetheless using work-provided resources (vehicles, phones, computers, internet accounts, email accounts, etc) for mixed work and/or personal use, but only if:

- the surveillance is overt (i.e. complies with the notice requirements in Part 2 of the Bill), and
- the surveillance is a continuation of the same overt surveillance conducted 'at work', and
- the purpose of the surveillance is appropriate to continue after hours, and
- the employer is unable to distinguish between when an employee is going to be 'working' away from the workplace and when they are not[13].

Enforcement

Overt surveillance

In terms of enforcement of the overt surveillance provisions, rather than the criminal offence approach to non-compliance with the 'covert surveillance' provisions of the Bill, we recommend that there be a system of civil remedies available for any non-compliance with the overt surveillance provisions, more in line with existing information privacy laws.

For example, there should be the ability for any person affected by the conduct of overt surveillance to lay a complaint with the NSW Privacy Commissioner in the case of refused access to the surveillance material, unethical use or unauthorised disclosure of surveillance material. As with existing information privacy laws in NSW, the Privacy Commissioner could attempt to conciliate the complaint, or the complainant could seek an enforceable remedy in the Administrative Decisions Tribunal.

Covert surveillance

The Workplace Video Surveillance Act, upon which this Bill is based, has not proven a successful model in terms of prosecutions for breaches of the covert surveillance provisions, despite evidence of widespread non-compliance with the Act[14]. To our knowledge there have to date been no prosecutions, although one matter has been referred by the Industrial Relations Commission to the Attorney General for consideration[15]. It would appear that no single agency has both the capability and willingness to investigate and prosecute for breaches of the offence provisions of the WVS Act[16].

Although this Bill provides one possible workable alternative, which is to allow an industrial association to prosecute a breach of the covert surveillance offence provisions, we recommend additional powers and funding for the NSW Privacy Commissioner to undertake

[13] This proposal would for example require tracking devices in vehicles and phones to be switched off when the employee is not working (where both employee and employer can define their normal working hours), but would allow continuous monitoring of internet and email use through work-provided email or internet accounts.
[14] See p6 of the *Submission by Privacy NSW to the Director General, NSW Attorney General's Department on the Workplace Video Surveillance Act Review*, October 2003.
[15] Staal and Tupene and Health and Research Employees' Association of New South Wales (on behalf of Nagy and Others) and Western Sydney Area Health Service [2004] NSWIRComm 27.
[16] See pp6-7 of the *Submission by Privacy NSW to the Director General, NSW Attorney General's Department on the Workplace Video Surveillance Act Review*, October 2003.

this role, to cater for situations where there is no union who can represent the employee, or where the employee is not a member of the relevant union.

Evidence of the lack of any prosecutions under the existing WVS Act, despite Privacy NSW's evidence of widespread non-compliance, suggests that the threat of criminal sanctions may not act as a deterrent to employers, who will likely be aware of the inherent difficulties in mounting prosecutions.

Recommendation 105 of the NSW Law Reform Commission in its 2001 review of surveillance was that subjects of unlawful covert surveillance should have the right to gain a civil remedy[17]. We support this recommendation, and do not believe that it is unreasonable that the covert surveillance operator is potentially subject to both a criminal and civil penalty.

We also support the recommendation of the NSW Privacy Commissioner that a person subject to covert surveillance should be able to seek a civil remedy if it can be subsequently established that an application for covert surveillance was not made in good faith[18].

We therefore recommend a civil complaints model for non-compliance with the covert surveillance provisions, as per that proposed above with respect to overt surveillance.

Accountability

The Bill provides, at clause 34, a system by which employers with a covert surveillance authority must provide a 'report back' to the magistrate on various matters, including 'any action taken or proposed to be taken in light of the information obtained'. Under clause 34(5)(b), the magistrate may then order that the employee who was the subject of the surveillance be informed of and/or given access to the surveillance material. We approve of these provisions.

We also commend the requirement, at clause 41, for a report to be tabled each year by the Attorney General on the number of covert surveillance authorities sought, and the number issued during the reporting year. However we suggest that the report should also include details of:

- what actions were taken after the period of surveillance (as reported back to the magistrate under clause 34), and
- whether or not the magistrate made any subsequent orders in relation to the employee subject being informed of or receiving access to the surveillance material (under clause 34(5)(b)).

An additional accountability measure would be to allow for the random or periodic audit of local court files by the Privacy Commissioner to assess the operation of the scheme, including compliance with the report-back requirements.

[17] See the discussion at 10.38 of the Report.
[18] See p24 of the Privacy NSW *Submission on the NSW Law Reform Commission Report 98, Surveillance: An Interim Report*, June 2002.

Conclusion

While advancing the reasonable protection of employees privacy by expanding on existing law to cover not only video but all camera, computer and tracking surveillance, the Bill fails to actually regulate the conduct of overt surveillance beyond signage and notification requirements. The reality for many employees is that they will continue to have no choice about whether or not they are to be subject to surveillance in the workplace, and how surveillance information may be used.

This is particularly disappointing, given the amount of work already conducted in the past decade by NSW government agencies in the industrial relations, privacy and law reform fields to develop a workable model of regulation for overt surveillance.

The rigid dichotomy between overt (Part 2-compliant) surveillance and 'covert' surveillance will not translate easily to the real world. There is a risk that employers who are trying to comply with Part 2 will nonetheless find themselves in breach of the law and facing criminal sanctions. Yet at the same time a wronged employee has no ability to obtain a remedy for an invasion of their privacy.

We have also identified several key loopholes in the Bill, which would allow employers to conduct covert computer surveillance of employees while they are not at work, and also may conduct covert surveillance of clients and visitors, even in particularly private areas such as toilets and change rooms. Furthermore we believe that the Bill provides inadequate protection for employees against the conduct of covert surveillance by an employer who has not obtained the requisite magistrate's authority, and provides little protection against the misuse of any information obtained as a result of such unauthorised and covert surveillance.

We are also disappointed that the enforcement model proposed in this Bill follows that of the existing Workplace Video Surveillance Act, despite evidence of the failure of that Act, with no known prosecutions in over five years despite evidence of widespread non-compliance. We propose an alternative model.

In conclusion we believe that this Bill promises much, but delivers little of benefit to either employers or employees.

About the Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. For further information see www.privacy.org.au

Since 2003 the Australian Privacy Foundation has hosted the Australian *Big Brother Awards*, which are presented around the world to corporations, public officials and governments that have shown a blatant disregard for privacy, and those who have done the most to threaten personal privacy in their countries. See www.privacy.org.au/bba for further details.