Australian Government Solicitor the leading lawyers to government

Commercial notes

Number 17 | 5 October 2005

The extended reach of the Workplace Surveillance Act

The *Workplace Surveillance Act 2005* (NSW) (the NSW Act), which commences on 7 October 2005, aims to regulate the surveillance of employees at work by replacing and extending the requirements of the *Workplace Video Surveillance Act 1998* (NSW). It covers three broad types of workplace surveillance:

- **camera surveillance**
- **computer surveillance**
- **tracking surveillance.**

This note describes the purpose and effect of the NSW Act and considers the extent to which it will apply to Australian Government agencies. The note focuses on computer surveillance, since that is the area likely to be of greatest concern to the majority of agencies. 'Computer surveillance' is relevantly defined to mean '... 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, but is not limited to, the sending and receipt of emails and the accessing of Internet websites.[1]

The requirements of the NSW Act

The relevant requirements of the NSW Act can be summarised as follows.

Any surveillance that does not comply with Part 2 of the NSW Act is 'covert surveillance' and must be authorised under Part 4 of the Act. Part 2 is expressed to apply to the surveillance of employees carried out or caused to be carried out by their employer while they are at work for the employer (s 9). The meaning of 'at work' is broadly defined (s 5), so employees are deemed to be at work for an employer when they are:

- at a workplace of the employer, whether or not they are actually performing work at the time, or
- at any other place while performing work for the employer.

Part 2 of the NSW Act imposes two major requirements on employers conducting computer surveillance:

- Employers must provide prior written notice to employees (s 10(1)) addressing the matters set out in s 10(4), including: the type of surveillance, how the surveillance will be carried out and the likely duration of the proposed surveillance.

Darwin

Andrew Schatz *Lawyer*
T *08 8943 1400* ***F*** *08 8943 1420*
andrew.schatz@ags.gov.au

Canberra

Graeme Hill *Senior Lawyer*
T *02 6253 7080* ***F*** *02 6253 7303*
graeme.hill@ags.gov.au

This issue

— In addition, computer surveillance may only be carried out in accordance with an employer policy on the subject (s 12(a)) and employees must be notified of the policy in advance in such a way that it is reasonable to assume they are aware of, and understand, the policy (s 12(b)). If the result of similar wording in other legislation is anything to go by, the latter part of this requirement may be the subject of much litigation.

Part 3 of the NSW Act imposes four further requirements relevant to organisations planning to supervise or restrict employee Internet and email use:

— Generally, employers may not conduct surveillance of employees who are not at work. However, employers may conduct computer surveillance '... of the use by an employee of equipment or resources provided by or at the expense of the employer' (s 16(1)).

— Employers may only prevent delivery of email, or block access to an Internet website, in accordance with a policy that has been notified to employees in advance in such a way that it is reasonable to assume they are aware of, and understand, the policy (s 17(1)(a)).

— If an employer prevents an employee from receiving an email, they are generally required to give the employee notice that delivery of the email was prevented (Prevented Delivery Notice) (s 17(1)(b)). There are some exceptions – e.g. an employer is not obliged to give a Prevented Delivery Notice if a blocked email is a commercial electronic message as defined in the *Spam Act 2003* (Cth) (s 17(2)(a)).

— Finally, any surveillance record made as a result of surveillance may only be used for the purposes set out in s 18 of the NSW Act. These purposes include a legitimate purpose related to the employment of employees, or the legitimate business activities of the employer (s 18(a)), and disclosure to a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence (s 18(b)).

The NSW Act has the very real potential to create a high water mark for computer surveillance requirements.

The application of the NSW Act

The NSW Act expressly binds the Crown in right of NSW and, consistently with NSW legislative power, 'the Crown in all its other capacities' (s 6). However, it does not apply to anything done under a warrant or other authority under the *Telecommunications Interception Act 1979* (Cth) (TI Act) or any other Commonwealth law (s 39).

Many large organisations, including Australian Government agencies, have national IT policies and procedures that apply to staff in all jurisdictions. Consequently, it may be impractical for them to create one set of workplace surveillance policies and procedures for staff based in NSW while retaining a separate set of policies and procedures for the rest of the country. Accordingly, the NSW Act has the very real potential to create a high water mark for computer surveillance requirements, resulting in NSW compliant policies and procedures being applied to staff in other jurisdictions.

Does the NSW Act apply to Australian Government agencies?

Statutory construction

Section 6 of the NSW Act is clearly intended to apply to all Australian Government agencies, to the extent it can do so validly. As a matter of statutory construction, both 'employee' and 'employer' are capable of applying to Australian Government agencies as employers, as well as to any staff that they employ.

Constitutional inconsistency

However, there is a question whether the NSW Act is inconsistent with Commonwealth legislation in its application to Australian Government agencies. If the NSW Act is inconsistent with Commonwealth legislation, it will be inoperative to the extent of the inconsistency by reason of section 109 of the Constitution. A number of pieces of legislation are potentially relevant here, including:

— the TI Act; and

— any Commonwealth Acts that confer power to employ and manage staff, such as the *Public Service Act 1999* (Cth) (PS Act).

The TI Act

The TI Act regulates the 'interception' of communications passing over a telecommunications system and, on decided cases, [2] does so to the exclusion of state and territory law. However, the definition of 'interception' in the TI Act is limited to 'listening to or making a record of a communication', which is narrower than the definition of 'computer surveillance' in the NSW Act. Accordingly, there is an issue regarding the extent to which the TI Act excludes the operation of the NSW Act in relation to computer surveillance.

It should also be noted that the Commonwealth Attorney-General's Department is currently reviewing the telecommunications interception regime. On 14 September 2005, the Attorney-General tabled in Parliament the *Report of the Review of the Regulation of Access to Communications* (http://www.ag.gov.au/blunnreview). The Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Bill 2005 (Cth) (SCOM Bill) was introduced on the same day, and it aims to extend the effect of the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (Cth) by six months.

Depending on the wording of each relevant statute, there may or may not be an issue of constitutional inconsistency vis-à-vis the NSW Act.

It will be interesting to see whether the review results in changes to the TI Act, or even entirely new legislation dealing with computer surveillance, including computer surveillance in the workplace. However, if the SCOM Bill is passed, it is unlikely that any such changes would take effect until some time in 2006.

The Public Service Act and other employment related statutes

Many Commonwealth employees are employed under the PS Act. It authorises agency heads to monitor the use of Internet and email facilities by agency staff. Accordingly, there is an issue as to whether the PS Act authorises agencies to conduct computer surveillance to the exclusion of state and territory law, or whether agencies are only authorised to conduct computer surveillance in accordance with other laws of general application (including, for these purposes, the NSW Act).

The position with respect to staff employed by Australian Government agencies under legislation other than the PS Act is also uncertain. Many agencies are provided with powers to employ and manage staff pursuant to their parent legislation. Accordingly, depending on the wording of each relevant statute, there may or may not be an issue of constitutional inconsistency vis-à-vis the NSW Act. It is therefore important that all Australian Government agencies take their own advice on whether the NSW Act applies to them, and if so, how it will affect their workplace surveillance activities (including any consequent need to review IT security and acceptable use policies and procedures).

Geographical reach of the NSW Act

Finally, there is a separate issue regarding whether the NSW Act applies to conduct or persons outside NSW. This issue may be of concern to agencies with employees that:

— are normally based outside NSW but are seconded to a position in a NSW workplace; or

— are normally based in NSW but are seconded or directed to work in a workplace outside NSW.

NSW legislation is usually presumed to apply only to things and persons *in and of* NSW. However, Part 1A of the *Crimes Act 1900* (NSW) provides that NSW offences may sometimes apply to persons and things outside NSW. A NSW offence may apply to conduct outside NSW if there is a nexus between the offence and NSW (for example, if the offence has an effect in NSW).

The question of whether the NSW Act applies to particular surveillance or blocking activities occurring, or partly occurring, outside NSW can only be answered after consideration of all the relevant circumstances. Accordingly, agencies should consider the NSW Act's application to any specific conduct that is an essential part of their operations. Legal advice on these matters could be requested at the same time as the advice recommended in relation to the Act's statutory application.

In a sense, the NSW Act simply codifies what many organisations would already regard as best practice.

A sign of things to come?

The commencement of the NSW Act raises a number of complex issues for agencies. However, it may simply be a sign of things to come and, depending on the outcome of the Attorney-General's review of the telecommunications interception regime, other jurisdictions may soon follow NSW's lead.

The commencement of the NSW Act may also focus attention on the need for the review of the telecommunications interception regime to include consideration of the interaction between state and Commonwealth legislation dealing with computer surveillance in Australian workplaces.

Of course, even if the NSW Act does not apply to particular Australian Government agencies, that does not prevent them from choosing to conduct computer surveillance in a manner consistent with the Act. In a sense, the Act simply codifies what many agencies would already regard as best practice. Accordingly, the commencement of the NSW Act presents an ideal opportunity for all agencies to review their IT security and acceptable use policies and procedures regardless of whether or not they are likely to be directly affected by the Act.

Andrew Schatz *has an extensive knowledge of technology related legal issues and has worked on a range of IT/IP legal matters. He regularly presents on information technology and communications law issues.*

Graeme Hill *specialises in constitutional litigation, with a particular expertise in federal jurisdiction and inter-governmental immunities.*

Notes

1 See paragraph (b) of the definition of 'surveillance' in s 3 of the NSW Act.

2 See, for example, *Edelsten v Investigating Committee of NSW* (1986) 7 NSWLR 222 at 230 (per Lee J) and *In the Marriage of Byrne* (2002) 172 FLR 81 at 88 (per Judicial Registrar Halligan); see also *Miller v Miller* (1978) 141 CLR 269.

Fitout and make-good issues

Every agency property manager will at some stage be required to oversee fitout of accommodation and deal with making good at the end of a lease. Here are some of the issues that your agency should consider in any fitout or make-good project.

Sydney
Simon Konecny *Senior Executive Lawyer*
T *02 9581 7585* ***F*** *02 9581 7445*
simon.konecny@ags.gov.au

Regulatory requirements

Early in any proposed accommodation project, likely regulatory requirements need to be considered. Financial approvals that will be required under the *Financial Management and Accountability Act 1997* (FMA Act) are the most obvious of these for FMA agencies (in particular FMA Regulations 9, 10 and 13).

Aside from financial approvals, the regulatory matters that agencies may need to consider in any fitout include:

Environmental matters

An assessment as to whether the fitout is likely to have a 'significant impact on the environment' will need to be done for the purposes of the *Environment Protection and Biodiversity Conservation Act 1999* (EPBC Act). In the context of a fitout the most likely situation to trigger referral under the EPBC Act is if the relevant building housing the premises is heritage protected.

Public Works Committee Act/Mandatory Procurement Requirements

If the value of the fitout will exceed $6m the fitout will need to be referred to the Public Works Committee for approval. Additionally, agencies will need to comply with the Mandatory Procurement Procedures of the *Commonwealth Procurement Guidelines* (assuming that the fitout is paid for by the agency).

State requirements

Whether agencies are required to comply with state or territory environmental, planning or other regulatory laws will depend upon their legal status and what is agreed to under their lease. (If, for example, an agency agrees to comply with state laws under the lease, it will be contractually bound to comply with state laws, regardless of any Commonwealth immunity.)

If, for example, an agency agrees to comply with state laws under the lease, it will be contractually bound to comply with state laws, regardless of any Commonwealth immunity.

The fitout process

Although each agency's fitout has its peculiarities, there are four common stages in any fitout project:

User requirement

This details your agency's instructions to its designer of its requirement. It generally is a functional statement of what is wanted in terms of budget, program requirements, space requirements, relationships within and between functional groups, special technical requirements, security issues, and environmental issues. It is generally not effective for agencies to pass this task on to the lessor or a consultant, as only the agency will know precisely what it wants.

Fitout brief

This is an architect or designers' interpretation of your agency's user requirement. It usually results in a detailed specification of the requirement, including all finishes. This phase of the process is often outsourced by the agency. The fitout brief is usually prepared in

cooperation with an architect or designer, taking into account evolving requirements, budgetary constraints and, often, in preparation for either a precommitment arrangement or some form of design and construct fitout arrangement. (Whilst it is possible that the fitout brief process could be passed to a lessor, in reality this rarely occurs as agencies will usually require a high degree of control in the preparation of the brief.)

Design documentation

This is the interpretation of the fitout brief for fitout construction. It is usually undertaken by a designer or architect engaged by the agency. The architect or designer will also take into account the physical characteristics of the actual premises.

It is possible that the design documentation could be prepared by, or on behalf of, the builder or the lessor (effectively passing on the design/construction integration risk to the builder or lessor). If this is done, your agency is essentially giving up 'control' of the design phase. To avoid quality problems arising you should only do so where you have a detailed fitout brief.

Construction

Provided the design is right, construction should not be a significant risk. If there are design issues these are likely to be exacerbated if responsibility for construction has been shifted to the lessor or managed via some sort of design and construct process.

The typical risks associated with fitout construction are time, cost, design/construction integration, and quality. Time, cost and design/construction integration can be shifted to the lessor if the lessor agrees to undertake the fitout via a precommitment lease or some similar arrangement. The downside of this is that quality potentially suffers unless the required quality is detailed in the fitout brief and design documentation.

Quality potentially suffers unless the required quality is detailed in the fitout brief and design documentation.

Alternatively, risk can be managed by use of appropriate contract strategies and use of consultants (e.g. project management and design/construct arrangements).

Incentives

If your agency is an anchor tenant, or has a significant leasing requirement, it is now common for it to be offered incentives by the lessor to secure the agreement. In most instances the incentives will be in the form of rent holidays, cash or provision of fitout (provided directly by the lessor or as reimbursement of costs that your agency incurs).

In relation to cash incentives, if your agency is an FMA Act regulated body you will need to take account of section 81 of the Constitution, as the incentive is likely to be regarded as 'public monies'. Whether or not your agency can retain any cash incentive received will depend upon whether you have in place appropriate arrangements with the Department of Finance and Administration under section 31 of the FMA Act.

Alternatively, your agency could obtain an undertaking from the lessor to pay for fitout costs up to a pre-agreed amount. The only drawback with this option is the need to obtain security from the lessor to cover potential liability for the construction costs.

If you use a fitout cost undertaking you also need to take into account the impact of GST. The relevant ATO ruling is GSTR 2003/16. Generally where a

fitout incentive is paid and the fitout remains your property you will be regarded as making a taxable supply to the lessor and will be required to pay GST on the value of the incentive.

Make-good issues

On the expiration of your lease you will need to consider your obligations to remove the fitout. The best time to consider these obligations is when you enter into the lease. As an anchor tenant in a new development, or as part of a precommitment arrangement, your agency will be in a good position to negotiate that there will be no make-good obligation – especially if the lessor remains the owner of the fitout. (The opening position in most standard Commonwealth leases, including those recommended by AGS, is no make-good obligation – rather a right on the part of the Commonwealth to remove its 'fixtures and fittings' if it elects, making good any damage in any such removal.)

There is no general legal obligation to make good. It is a matter of agreement between the parties. If the lease is silent on the issue, you have no make-good obligation and technically your fitout will become the property of the lessor. However, you might still have a pseudo make-good obligation if the lease requires you to repair damage caused during the term of the lease.

There is no general legal obligation to make good. It is a matter of agreement between the parties.

If you have a make-good obligation be clear what you have to make good on. Returning the premises to the condition they were in at the time the lease was entered into does not necessarily require you to take the premises back to base building, which is often what lessors desire. Good records are essential to identify the state of the building at the commencement of the lease. Usually you are not required to make good on lessor fitout (i.e. fitout existing at the commencement of the lease or subsequently done by the lessor).

Beware of requests from the lessor for you to make a payment in lieu of making good. Even if you have a make-good obligation you may be able to avoid liability in certain circumstances, for example where:

— the lessor proposes to demolish the building containing the premises

— the lessor proposes to retain the fitout

— the incoming tenant is willing to take over your fitout.

If you are prepared to make a payment in lieu of making good, ideally it should be a reimbursement of costs agreement, and at the very least be on condition that any payment will be used in making good.

Simon Konecny *has extensive knowledge and experience in property and contracting matters including acquisitions and disposals, leasing and advice on leasing obligations, fitouts, building and construction matters, tenders and advice in relation to tender processes and strategies, outsourcing and consultancy arrangements, indemnities and licence arrangements.*

AGS contacts

For legal advice on the articles in this issue please contact the authors or any of the lawyers listed below:

National	John Scala	03 9242 1321
Canberra	Linda Richardson	02 6253 7207
	John Snell	02 6253 7025
Sydney	John Berg	02 9581 7624
	Simon Konecny	02 9581 7585
Melbourne	Paul Lang	03 9242 1322
	Josephine Ziino	03 9242 1312
Brisbane	Robert Claybourn	07 3360 5767
Perth	Lee-Sai Choo	08 9268 1137
Adelaide	Mary Hannigan	08 8205 4287
Hobart	Peter Bowen	03 6220 5474
Darwin	Andrew Schatz	08 8943 1400

For enquiries regarding supply of issues, change of address details etc.

T *02 6253 7052* ***F*** *02 6253 7313* ***E*** *ags@ags.gov.au*

Canberra
50 Blackall Street Barton ACT 2600

Sydney
Level 23, Piccadilly Tower, 133 Castlereagh Street Sydney NSW 2000

Melbourne
Level 21, 200 Queen Street Melbourne VIC 3000

Brisbane
Level 12, 340 Adelaide Street Brisbane QLD 4000

Perth
Level 19, Exchange Plaza, 2 The Esplanade Perth WA 6000

Adelaide
Level 20, 25 Grenfell Street Adelaide SA 5000

Hobart
Level 8, 188 Collins Street Hobart TAS 7000

Darwin
Level 3, 9–11 Cavenagh Street Darwin NT 0800

Web site
For a full review of AGS services, visit <www.ags.gov.au>

Electronic versions of AGS newsletters are available for clients who prefer to receive issues in this form. Please contact 02 6253 7052 or email ags@ags.gov.au to arrange supply.

ISSN 1433-9549
Approved Postage PP 255003/05310