[30] Ibid, per Lord Nicholls at paragraph 13, in above note 1 at [71]

[31] Above note 1 [74]

[32] Ibid [78]

[33] Ibid [85]

[34] *Lloyd Schuhfabrik v Klijsen* [1999] ETMR 690 in Ibid, at [85]

[35] Ibid [89]

[36] Ibid [94]

[37] Ibid [108]

[38] See above note 3.

[39] Above note 1, [24]

[40] Above note 3.

Is Your Employer Watching You? - Computer surveillance in the workplace

Andrew Gray & Ben Urry

Andrew Gray, Special Counsel and Ben Urry, Law Graduate are both in the Workplace and Employee Relations team at Mallesons Stephen Jaques in Sydney.

The *Workplace Surveillance Act 2005 (NSW)* commenced on 7 October 2005 and restricts the ability of employers to monitor computer usage (among other things) by its employees. Nearly a year after the commencement of this groundbreaking legislation our experience is that many employers are still not compliant with the legislation.

Non-compliance can have significant implications. Quite apart from the criminal sanctions involved, failure to comply with the Act can prevent an employer relying on computer surveillance evidence in employee disciplinary matters and legal proceedings.

Background

In order to understand the purpose of the legislation it is necessary to understand the history surrounding surveillance in the workplace in NSW. Prior to legislative intervention by the NSW government into workplace surveillance, employers could "by and large" conduct surveillance of its employees while they were at work without fear of criminal penalties. Under common law, employers are granted proprietary interests in practically every resource used by their employees in the workplace.[1] It has been argued that in order to preserve this right, employers would be entitled to conduct surveillance over these resources to ensure their proprietary right is protected.[2] For example, supplied business equipment such as computers could be subject to a search by the employer, as not only does the computer belong to the employer, but anything the employee has done as employee also belongs to the employer[3] (for example, the creation of work related Word documents and programs).

Employers could also in certain circumstances utilise surveillance over their employees where the possibility of such surveillance was expressed in an employee's contract of employment. In addition to such an express right, a general duty to obey the employer's lawful and reasonable directions is an implied term of the contract of employment. Surveillance was seen as a way to enforce the employer's ability to 'command' its employees,[4] as there is no real difference between the various forms of human and electronic surveillance (such as video and telephone recording).

Workplace Video Surveillance Act 1998 (NSW) - the forerunner to the 2005 Act

Aside from any common law ability to conduct surveillance over employees, the *Workplace Video Surveillance Act 1998 (NSW)* was introduced to regulate how employers used video surveillance in the workplace. This type of legislation was the first of its kind in Australia and was considered a step forward in attempting to reconcile privacy concerns of employees with the needs of employers in running a business[5] (including monitoring thefts and stock losses via video recordings). This is important in the absence of a common law entitlement for employees to privacy.[6]

Although this Act was a significant step forward, technology continued to develop at an exponential rate, with the result that employees became increasingly concerned that private communications sent by them via email could end up being intercepted and read by their employers due to the lack of regulation over this increasingly popular mode of communication.[7] With that in mind, the NSW government proposed that a new Act, (the *Workplace Surveillance Act 2005 (NSW)*) be implemented to ensure regulation over other forms of workplace surveillance, including computer surveillance. Not only would this new Act ensure transparency in the workplace but it would strike a fair balance between the concerns of employees regarding their privacy at work and the employer's legitimate right to limit usage of computer networks in the workplace for personal use.[8]

Workplace Surveillance Act 2005 (NSW)

Scope of the Act

The *Workplace Surveillance Act 2005 (NSW)* ("**the Act**") restricts the ability of employers to monitor the activities of its employees through computer surveillance including controlling the extent to which employers can block

their employee's access to email and the internet.

The Act extends what is meant by the term 'employee' to include other participants in the workplace, such as persons working for the employer who are employed by third parties[9] (for example, persons such as long term contractors and those under labour hire arrangements) to ensure that those 'employees' also benefit from the protections provided under the Act. Further protection is provided to employees through the Act extending beyond the traditional workplace (such as an office or the factory floor) to anywhere an employee is working.[10] This is significant given that as technology improves more and more people will begin working remotely from home or other public places in conjunction with a more 'flexible' lifestyle.

Penalties

Significantly, contravention of the Act is a criminal offence, with fines of up to $5,500 capable of being imposed. Senior managers and directors may also be personally liable where they knowingly allow their company to contravene the Act.[11]

Features of the Act

The Act prohibits employers carrying out computer surveillance - taken to include surveillance by means of software or other equipment that monitors or records the information input, output or other use of a computer (including sending and receiving emails and accessing websites) unless the surveillance complies with the Act.[12] An employer is only permitted to carry out computer surveillance of an employee if it is either 'notified surveillance' or authorised 'covert surveillance' as defined by the Act.

Record use

The scope of the permitted use of surveillance records is reasonably broad (putting aside such restrictions imposed on use of records under relevant privacy laws). Any records made or obtained by such surveillance may only be used for a legitimate purpose including relating to the:

- employment of employees;
- legitimate business activities of the employer (this would not include, for example, providing employee email addresses to third parties for the purpose of being added to marketing lists); and
- investigation or prosecution of an offence (for example, child pornography or credit card fraud).[13]

Notified Surveillance

Most employers will (other than in exceptional circumstances) seek to rely on the notified surveillance provisions of the Act to monitor computer use by employees. The requirements for notified surveillance are set out below:

- employers are required to provide written notice (which can be by email) to their employees at least 14 days (or such shorter time as agreed) before any intended surveillance is to occur.[14]
- the Act provides that the notice must provide:[15]
  - that computer surveillance is to be carried out;
  - how it will be carried out;
  - when will the surveillance start;
  - whether the surveillance will be continuous (for example, 24/7) or intermittent; and
  - whether the surveillance will be for a specified limited period (for example, 3 months) or ongoing.
- this notice is not required to appear every time a person logs onto their computer or email account.
- any type of computer surveillance must be carried out in accordance with the employer's policy on computer surveillance. Employees must be notified in advance of such a policy in a way that allows the employer to say that its employees are aware of and understand the policy.[16]

Covert Surveillance

Any surveillance which cannot be classified as notified surveillance is covert surveillance.[17] This type of surveillance is only permissible where:[18]

- a covert surveillance authority is obtained from a Magistrate for the sole purpose of establishing whether a particular employee/employees are involved in any unlawful activity at work. Such authorities are in force for no more than 30 days[19]; or
- it is for the sole purpose of ensuring the security of the workplace and/or persons in it. This involves the surveillance not being specifically directed at any employee and there being a real and significant likelihood of the security of the workplace being jeopardised if the covert surveillance was not carried out. In addition, the employer must have notified its employees in writing of such surveillance before it was carried out.

Filtering and blocking email and websites

Addressing the concern that employers could undertake a "big brother style" monitoring of emails of its employees, the Act regulates where an employer is entitled to restrict the content of emails and websites accessed by its employees. Under the Act, employers are entitled to prevent the delivery of emails (inbound or outbound) or access to all or certain websites provided:[20]

- the employer has a policy on email and internet access that has been notified to its employees in advance in such a way that it is reasonable to say that the employee is aware of and understands the policy;
- the employer acts in accordance with that policy; and
- where there is an email filter, the employee is notified (by a "prevent delivery notice") as soon as it is practicable that a delivery of an email sent by or to them has been prevented (for example, by the use of an instant

email notification from the mail server).

The Act provides a number of exceptions relieving employers from these notification requirements. Notification is not required where:[21]

- the email is a commercial electronic message (or spam) under the *Spam Act 2003 (Cwlth)*;
- the content of the email or attachment would or might have resulted in unauthorised interference with or damage to a computer or network of the employer, or any program running or data stored on such a computer or network (for example, computer viruses and "nukes"); or
- the email or its attachment would have been regarded by a reasonable person in all the circumstances as offensive, menacing or harassing (for example, emails of a sexually suggestive nature or emails containing racial or religious abuse).

The Act specifically refers to a further prohibition on employers limiting access to emails or websites in the case of industrial matters,[22] in that an employer cannot prohibit delivery of emails or access to websites merely because the content concerns industrial matters.[23] In other words, an employer cannot add industrial matter websites (and emails) to a "black list" of blocked sites/emails merely because they relate to industrial matters. However, this section does not provide special protection for industrial matter related websites or emails where the employer has a total or complete no email/website policy (that is, no accessing of any emails or the internet is permitted).

Compliance issues

Our experience to date is that many employers, particularly those in large corporate groups or with experienced HR departments, already have some form of policy in place dealing with computer and internet use. However, in many cases when these policies are closely scrutinised they do not quite meet the specific requirements of the Act, especially with respect to notified surveillance.

There is a need for all employers and IT administrators to review their policies in light of the Act. Failure to do so could result in substantial problems and consequences for employers. This is particularly the case in employee disciplinary matters and investigations - employers may be prevented from using computer evidence available to them due to non-compliance with the requirements of the Act.

Employers have sought to comply with the Act by amending or creating computer surveillance policies and notifying their employees of these policies. A common (and sensible) approach being adopted by employers is to incorporate notification of computer use/surveillance policies into the standard form employment contract so that employees are given notice before they start employment and enter the workplace.

We note that despite our comments regarding the potential level of non-compliance with the Act we are not aware of any successful prosecution under the Act to date (see our comments further below on this).

Unresolved issues concerning the application of the Act

Potential conflict with the Telecommunications (Interception and Access) Act 1979 (Cwlth)

Although appearing to provide safeguards for employee privacy whilst providing a right for employers to conduct surveillance of their employees, being a recent piece of legislation, the Act has yet to be tested in the courts. One issue which is perhaps of more than purely academic concern is the interaction between the *Telecommunications (Interception and Access) Act 1979 (Cwlth)* ("**TIA**") and the *Workplace Surveillance Act 2005 (NSW)* ('**the Act**").

Under the TIA listening to or recording a communication (which now includes emails) passing over a telecommunication system without knowledge of either the person sending or receiving the communication is prohibited.[24] Depending on when an email communication is monitored (that is, while being sent/transmitted or after the email has been stored), the Commonwealth Attorney General has stated that an employer may still be committing an offence under the TIA where they have not notified the sender and receiver that they are intercepting incoming and/or outgoing emails (while such emails are 'passing over' a telecommunication system).[25] This offence would still occur despite any covert surveillance authority being granted by a Magistrate under the Act due to the fact that, under section 109 of the Constitution, State laws that are inconsistent with Commonwealth laws on the same matter are invalid to the extent of any inconsistency.

The Attorney General did recognise that although the TIA may have priority over the Act in this respect, where emails have ceased to 'pass over' the telecommunications system and are stored, any surveillance of the stored material would be subject to the NSW Act.

Until such conflict has been tested in the Courts, the preferred option for employers and IT administrators regarding computer surveillance of emails would be to examine these emails after they have been sent and stored rather than intercept them while they are being sent.

Federal agencies

The first prosecution to occur under the Act was discontinued in March 2006 when the Prosecution decided it wasn't sure whether the Act would apply to federal agencies (in this case, Centrelink).[26] This was due to concerns that a piece of State legislation could not operate to bind a Federal agency. This seems to be a legitimate concern regarding the scope of the Act.

Geographical application

It is not clear how the Act applies in cases where IT departments or employers conduct computer surveillance of NSW employees (such as monitoring of emails) either in another State or offshore. This is significant for employers who have IT departments or servers located offshore. In our view, applying the general principles regarding the extraterritorial operation of legislation, there are reasonable arguments to say

that the offences created under the Act do not apply to surveillance conducted outside the State of New South Wales.

Conclusion

The introduction of the *Workplace Surveillance Act 2005 (NSW)* has resulted in greater transparency in the workplace regarding computer surveillance. By expanding the definitions of employee and workplace, employees rights to privacy have increased as it is an offence for employers to carry out computer surveillance on their employees without complying with the Act. Although the requirements of the Act do not impose onerous burdens on employers, employers in NSW that wish to monitor computer use by their employees must:

- develop a written policy on computer surveillance and bring that policy to the attention of employees as soon as possible. To avoid restricting themselves to limited types of computer surveillance, employers should seek to ensure the terms of their computer surveillance policies are as broad as possible while still meeting the minimum notice and other requirements under the Act. This might include mentioning that computer surveillance might be carried out by third parties and confirming that all forms of electronic storage/communication devices may be monitored;
- notify employees of any intended (or changes in) computer surveillance procedures at least 14 days before such surveillance commences (the Act provides that notice by email is sufficient). Such notice should include details of the type of surveillance that may be carried out, how the surveillance will be carried out, when the surveillance will start and whether the surveillance will be for a specified limited period or ongoing; and
- ensure that if employers deliberately block delivery of particular emails there are procedures in place to ensure that employee-recipients of such blocked emails are notified as soon as practicable of the blocked email.

In addition, it may also be prudent for employers to include a provision in contracts of employment for new employees allowing for surveillance in accordance with the employer's surveillance policy from the commencement of employment. Some employers have also adopted the approach of using pop up messages where employees log on to their computers to get confirmation of their acceptance to the terms of any IT use policy (including computer surveillance policies). Given the requirement that employers need to be able to say that their employees are aware of any computer surveillance policy, it is preferable that employers regularly bring their IT/computer surveillance policies to the attention of their employees rather that these policies being 'dead letters' put in a HR manual and never to be reviewed again.

Employers and IT administrators should also keep an eye on this area of law generally and, in particular, how the legislation is interpreted by the Courts. The issue of workplace surveillance is also being reviewed by the legislators in States other than NSW and there may be similar legislation introduced in other States in the future.

---

[1] Cripps, A., *Workplace Surveillance*, New South Wales Council for Civil Liberties, November 2004, p10.

[2] Schulman, A. "Computer and Internet Surveillance in the Workplace" (2001) 8(3) *Privacy Law and Policy Reporter* 31.

[3] 'Email files and internet browsing', ¶51-744, *Australian Employment Law Guide*, CCH online.

[4] Sempill, J., 'Under the Lens: Electronic Workplace Surveillance', (2001) 14 *Australian Journal of Labour Law* 111.

[5] Second Reading Speech - Mr Bob Debus, NSW Legislative Assembly Hansard, 4 May 2005

[6] *Giller v Procopets* [2004] VSC 113 at paragraphs 187-189

[7] Note 5.

[8] Note 5

[9] Section 3 *Workplace Surveillance Act* 2005 (NSW)

[10] Section 3 *Workplace Surveillance Act* 2005 (NSW)

[11] Section 43 *Workplace Surveillance Act* 2005 (NSW)

[12] Section 3 *Workplace Surveillance Act* 2005 (NSW)

[13] Section 18 *Workplace Surveillance Act* 2005 (NSW)

[14] Sections 10(2) & (3) *Workplace Surveillance Act* 2005 (NSW)

[15] Section 10(4) *Workplace Surveillance Act* 2005 (NSW)

[16] Section 12 *Workplace Surveillance Act* 2005 (NSW)

[17] Section 3 *Workplace Surveillance Act* 2005 (NSW)

[18] Sections 20 & 22 *Workplace Surveillance Act* 2005 (NSW)

[19] Note 5 and section 29 *Workplace Surveillance Act* 2005 (NSW)

[20] Section 17(1) *Workplace Surveillance Act* 2005 (NSW)

[21] Section 17(2) *Workplace Surveillance Act* 2005 (NSW)

[22] Section 17(4) *Workplace Surveillance Act* 2005 (NSW)

[23] Concern over industrial matters in emails is not restricted to after the commencement of the Act. In *ASU v Ansett Australia Ltd [2000] FCA 441*, the Federal Court found that the dismissal of an employee for using their work email and IT system to distribute union related material to other union members was unlawful.

[24] Sections 6 & 7 *Telecommunications (Interception and Access) Act* 1979 (Cwlth). Under recent amendments to the Act, Chapter 3, Part 3-1 of the Act also now prohibits access to "stored communications" without notice. However, the definition of "stored communications" is limited to communications stored on equipment operated by a 'carrier' (as defined under the Act, ie, a holder of a carrier licence) so this prohibition does not apply to most employers.

[25] 'Private Parts', (2006) 11(8) *Privacy Law and Policy Reporter* 244

[26] *First NSW workplace surveillance prosecution dropped*, www.workplaceexpress.com.au, 1 March 2006.