

# Compliance with the new NSW Workplace Surveillance Act: Don't assume – act new

Keeping tabs on employees' computer use in the workplace just a little more complex.  
Carrie Peterson reports on what employers need to know if they are to monitor usage legally

New South Wales' recently passed *Workplace Surveillance Act* comes into operation today, 7 October 2005, with important implications for employers who keep track of their employees' electronic "footprints".

Prudent employers should consider the changes coming into force as in some instances, failure to comply may amount to a criminal offence.

The Act introduces new restrictions on the use and disclosure of surveillance records and expands the definition of employee to include, among others, independent contractors.

The charges directly reflect the increased need to protect the rights of employees to confidentiality in the workplace.

In most businesses, the crucial changes relate to computer surveillance. The Act regulates employers' previously unrestrained capacity to block emails to and from employees or to prevent employees from accessing websites. Previous NSW workplace surveillance laws regulated how an employer could use video cameras, as well as the conduct of their employees, but did not regulate the use of tracking devices for monitoring, for example, employees' internet and computer use.

The Act requires that an employer either notify employees before surveillance can be

carried out, or obtain a covert surveillance authority. A key requirement is that employers must notify employees at least 14 days before the commencement of the surveillance.

Furthermore, the employer may only carry out computer surveillance in accordance with a policy when they have advised the employee in advance and it is reasonable to assume that the employee is aware of and understands it. An employer may continue to block delivery of emails or access to certain websites provided it is acting in accordance with that policy and if an employer is blocking delivery of an email, the employee is immediately notified that the email has not been delivered (section 17).

The Act will require employers to formulate carefully worded policies and procedures relating to workplace surveillance. Obviously, there are consequences for an employer who breaches the Act, which include being unable to rely on evidence during unfair dismissal proceedings or being unable to use evidence in proceedings relating to the misuse of the employer's confidential information.

The basic implications for employers are that they should:

- Conduct an audit of the workplace surveillance they currently have in place and identify any procedures or policies

that may need to be implemented as a result of the new Act;

- Review their email and internet use policies to ensure compliance with the new Act;
- Ensure employees are aware of, and understand, those policies;
- Make sure that employees are aware of any future changes that result whenever the policies are renewed or amended; and
- Ensure that contractors and agency staff are also aware of surveillance policies.

The Notice requirements in Part 2 of the Act do not, however, require the employer to notify the employees every time that an employee logs onto their computer.

The United Kingdom has issued a Code of Practice on workplace monitoring to guide employers on compliance with privacy laws. In Canada and New Zealand, where privacy laws applied to workplaces no such regulatory provisions have yet been introduced. The EU has recently proposed a directive on the protection of employees' data. And in the United States, there have been in two previous legislation proposals to require the matters of monitoring but they both failed to be introduced in at least two US states.