Communications Law BULLETIN
CAMLA
Communications & Media Law Association Incorporated

Print Post Approved PP 234093/00049

The New Workplace Surveillance Act: Impacts On Media Organisations

Sophie Dawson and Arthur Artinian look at some of the implications of the new *Workplace Surveillance Act* and its consequences for media reporting.

The *Workplace Surveillance Act* 2005 (NSW) "(**Act**)" was passed by both Houses of Parliament on 21 June 2005 and was assented to on 23 June 2005, but has not yet commenced. The Act regulates the surveillance of employees in the workplace with reference to computer, camera and tracking surveillance. It also operates to restrict the ability of employers and others from disclosing and using surveillance records.

In view of the expected commencement of the Act and the notice requirements under the Act, all NSW employers (including media organisations) should now take steps to ensure compliance with the Act.

Impact on Media Organisations

The Act has two important implications for media organisations. First, as employers and heavy users of computer and communications technologies, media organisations will be required to comply with the notification requirements under the Act for surveillance of employees who are at work and will be subject to the restrictions on covert surveillance.

Second, and perhaps more importantly, the Act is likely to limit the extent to which media organisations can obtain and publish material obtained through workplace surveillance. This has the potential to have an adverse impact on investigative journalism. The extent of this impact will to a large extent depend on the way which courts interpret "computer surveillance" and the exceptions to the prohibition on use and disclosure of notified surveillance.

Media organisations as employers

Media organisations will need to move quickly to reassess their current surveillance practices, including notices to employees and review of the measures they use to control employees' use of company computer systems. This may include entering into agreements with a suitable employee organisation, meeting the notification requirements which are specified in the Act or both. It will also involve putting in place appropriate compliance policies and reviewing internet and email policies and practices.

The Act makes it an offence for an employer to carry out any surveillance by camera, computer or tracking when an employee is not "at work". This applies whenever an employee is not in the workplace and is not performing work for the employer elsewhere. There is a limited exception to this offence where an employer conducts computer surveillance of "equipment or resources provided by or at the expense of the employer". The Act also makes it an offence to carry out surveillance in any change room, toilet facility, shower or other bathing facility at work.

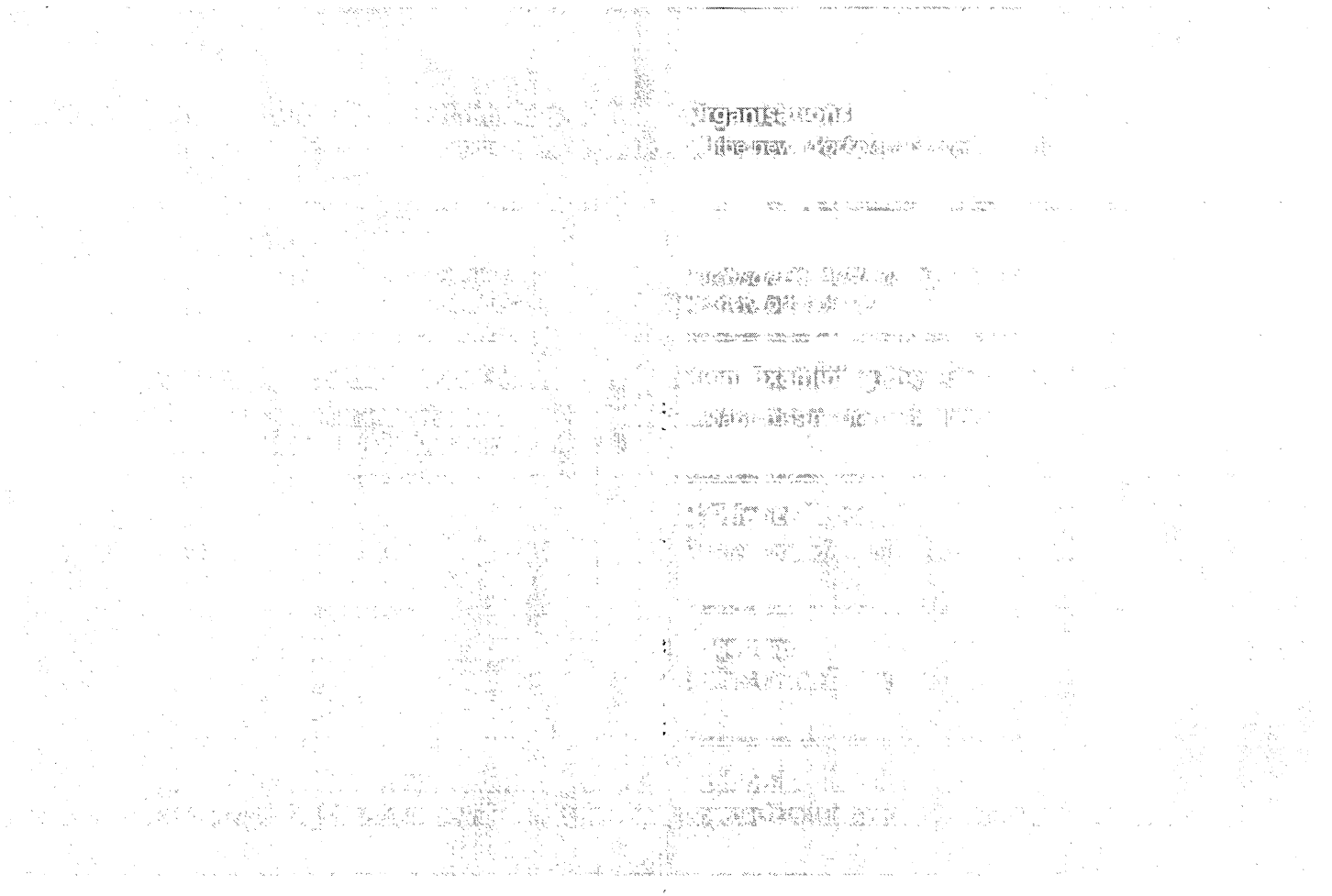
Surveillance

Notified Surveillance

The Act allows employers to conduct surveillance if they meet a general notice requirement and specific requirements for each type of surveillance.

Employees must be given notice in writing 14 days prior to the commencement of any surveillance, unless an employee agrees to a lesser period of notice ("**General Notice Requirement**"). The General Notice

Volume 24 No 2
September 2005



Requirement does not apply to camera surveillance when an employee is working at a location that is not their usual workplace, for example where an employee attends a meeting or training off-site.

Surveillance of an employee will be taken to comply with notification requirements in the Act if the surveillance is for a purpose other than surveillance of employees and the employer has entered into an appropriate agreement with the employee or with a body representing a substantial number of employees at the relevant workplace.

Camera surveillance

Camera surveillance may only be used where the employer meets the General Notice Requirement and where:

- cameras (or camera casings or other equipment indicating the presence of a camera) are clearly visible in the place where the surveillance is taking place; and
- signs which notify people that they may be under surveillance are clearly visible at each entrance to that place.

Computer surveillance

Computer surveillance of an employee is defined as the surveillance of an employee through:

> *"monitoring or recording by means of software or other equipment that monitors or records the information input or output, or other use of, a computer (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites)".*

This definition has a potentially broad application. This will depend upon how broadly courts interpret "surveillance".

Computer surveillance can be used where the General Notice Requirement and both of the following requirements are met:

- the surveillance is carried out in accordance with a policy of the employer on computer surveillance of employees at work; and
- the employee has been notified in advance of that policy in such a way that it is reasonable to assume that the employee is aware of and understands the policy.

In view of the expected commencement of the Act and the notice requirements under the Act, all NSW employers (including media organisations) should now take steps to ensure compliance with the Act.

Covert Surveillance

Covert surveillance is all surveillance other than Notified Surveillance. The Act generally makes it an offence for an employer to carry out covert surveillance at work unless the surveillance is carried out solely for the purpose of establishing whether or not an employee is involved in any unlawful activity at work and it is authorised by a covert surveillance authority or the defence below applies. There are exceptions for law enforcement agencies, correctional centres, courts and casinos.

The Act provides a defence to a prosecution for covert surveillance where an employer can show that:

- surveillance was conducted for security purposes;
- there was a real and significant likelihood of security being jeopardised in the absence of covert surveillance; and

- the employees (or a body representing a substantial number of employees) were notified in writing prior to the surveillance commencing.

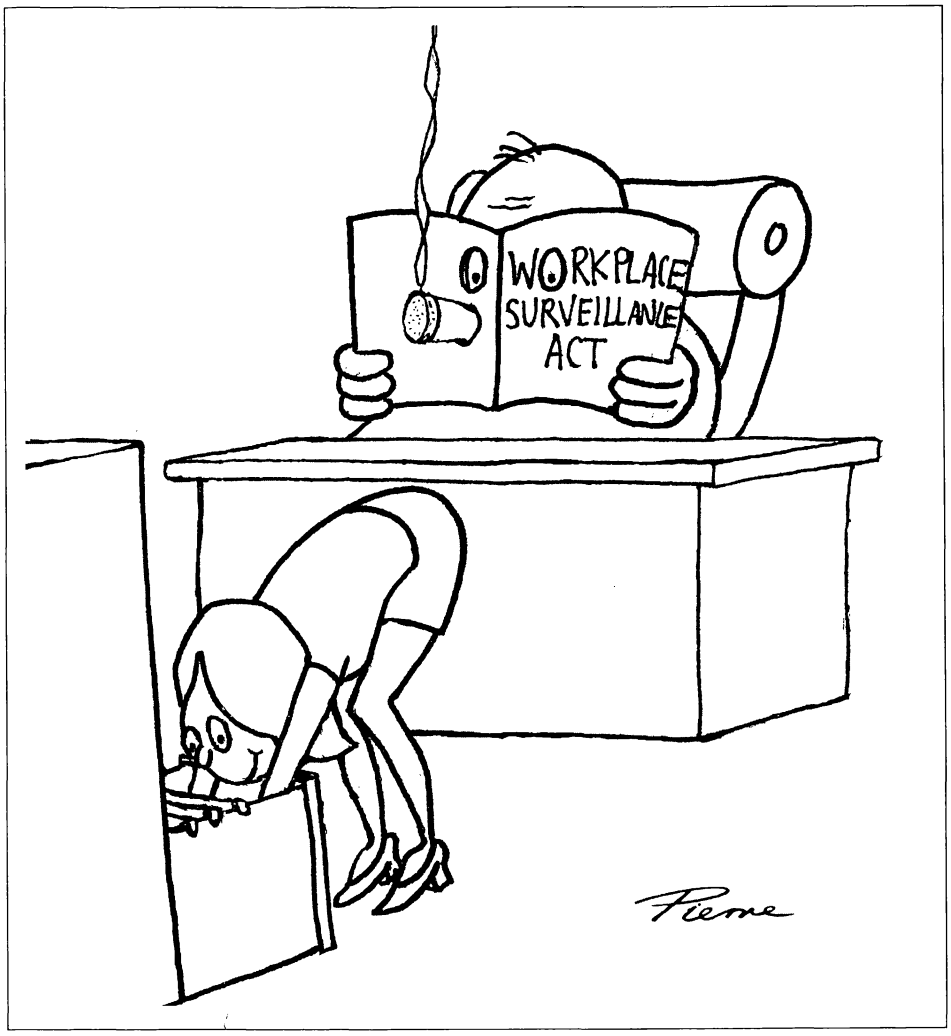
The Act prohibits use or disclosure of information obtained, recorded, monitored or observed and of records made as a direct or indirect consequence of covert surveillance of an employee. This prohibition is subject to narrow exceptions, such as where the use is for purposes of law enforcement. This is discussed below.

Publication of surveillance records

The Act prohibits "persons" generally from using or disclosing information or a surveillance record where there is reasonable cause to suspect the record or information results directly or indirectly from covert surveillance. Practically, this means that any person or organisation risks committing an offence if they obtain and publish surveillance material such as camera footage, photographs or computer records from an employer unless they know the notification requirements discussed above have been met or one of the limited exceptions to the prohibition applies. In the case of covert surveillance carried out without a covert surveillance authority, the exceptions are very limited and all relate to law enforcement. The exceptions are slightly broader where a covert surveillance authority has been obtained but are still broadly limited to law enforcement, employment and security purposes and purposes permitted under a covert surveillance authority. Importantly, there are no public interest exceptions to the prohibition.

These provisions are likely to significantly restrict the information and footage which media organisations can obtain and publish where notification requirements have not been complied with by employers. For example, publication of footage or still photographs obtained from an employer following a hold-up in a shop will be prohibited where there are reasons to suspect that surveillance was conducted without notification. The same will be true for "undercover" or hidden camera investigations which often appear on current affairs television programs where cameras have been used covertly by an employer to prove theft, fraud or other unacceptable conduct without notification.

The fact that the Act extends to computer surveillance also potentially means that computer files which have been obtained through the surveillance of an employee using an employer's computer systems in the absence of the required notification would not be able to be published by the media. If courts interpret "computer surveillance" widely, this may seriously impact on the business reporting of large companies and organisations where compliance with the notification requirements under the Act cannot be demonstrated.



Employers' disclosure of notified surveillance records

The Act was recently amended to limit use and disclosure by employers of surveillance records where notification requirements are met. The new "use and disclosure" clause provides that, in the case of notified surveillance, an employer must ensure that surveillance is not used or disclosed unless that use or disclosure is:

- for a legitimate purpose of employment or a legitimate business activity or function of the employer;
- to a law enforcement agency as part of that agency's legitimate function;
- directly or indirectly related to the taking of civil or criminal proceedings; or
- reasonably believed to be necessary to assert an imminent threat of serious violence to persons or a substantial damage to property.

Depending on the interpretation of the first of these exceptions, this prohibition could prevent employers from providing notified surveillance records (which, it must be remembered, will include at least some computer records and may, for example, include email) to the media. The question in each case will be whether releasing such information is a "legitimate business activity or function" of the employer.

Conclusion

The Act is likely to have significant impact on media organisations both as employers and as publishers. The extent of that impact will depend upon interpretation by the courts of "computer surveillance" and of what is a "legitimate business activity or function" of a NSW employer. It is to be hoped that the courts will interpret these terms so as to still allow the media to obtain and communicate to the public information relating to matters of genuine public interest.

Sophie Dawson is a partner and Arthur Artinian is a lawyer in the Sydney Office of Blake Dawson Waldron.