

News

October 2005

Litigation Newsletter

In this issue we will outline the following topics:

- Workplace Surveillance Act 2005 (NSW)
- Silence during contractual negotiations
- A note about blogs
- The infallibility of fingerprints

1. Workplace Surveillance Act 2005 (NSW)

The new *Workplace Surveillance Act 2005* (**Act**) commenced on 7 October 2005. The Act regulates surveillance of employees at work in relation to electronic equipment used by both employers and employees. The Act covers two types of surveillance, namely:

- (a) "notified" or overt surveillance, in respect of which employers are required to provide specific notice; and
- (b) covert surveillance, which can only be used to investigate unlawful activities at work and may not be used to monitor an employee's work performance. Covert surveillance may only be carried out pursuant to a "Covert Surveillance Authority" which is granted by a Magistrate of the Local Court.

In this article, we shall concentrate on overt surveillance of employees. The Act covers surveillance of employees "at work" using video cameras and tracking devices (ie, devices that have the primary purpose of monitoring or recording the location or movement of an employee, such as global positioning systems). In addition, the Act also contains provisions dealing with surveillance of employees' emails and their internet usage. The Act permits, in certain circumstances, surveillance of employees "at work" which includes:

- (a) the workplace of an employer, whether the employee is performing work or not; and
- (b) any other place where the employee may be performing work. For example, an employee using an employer's laptop computer at home may be subject to surveillance.

MAKINSON & d'APICE

— L A W Y E R S —

Level 12 135 King Street Sydney NSW 2000 • GPO Box 495 Sydney 2001 • DX 296 Sydney
Telephone 02 9233 7788 • Facsimile 02 9233 1550 • Email mail@makdap.com.au • www.makdap.com.au

Camera surveillance of an employee must not be carried out unless the surveillance cameras are clearly visible and there are clearly visible signs at each entrance to the workplace notifying people that they may be under surveillance.

Computer surveillance of an employee must not be carried out unless the surveillance is conducted in accordance with the policy of the employer and the employee has been notified in advance of that policy. In these circumstances, it must be reasonable to assume that the employee is aware of and understands the policy. A "pop up" notice on an employee's computer screen where the employee must positively acknowledge and accept the policy before being permitted to log on is an effective means of communicating the policy.

Thirdly, tracking surveillance of an employee involving the tracking of a vehicle or "other thing" (eg. laptop computers) must not be carried out unless there is a notice clearly visible on the vehicle or thing indicating that it is the subject of tracking surveillance.

Overt surveillance is prohibited in the following circumstances (breaches of which will constitute an offence punishable by a maximum penalty of 50 penalty units - currently \$5,500):

- (a) change rooms and toilet, shower and bathing facilities;
- (b) surveillance of an employee using a work surveillance device when the employee is not at work unless it involves computer surveillance of the employee's use of equipment or resources provided by the employer or at the employer's expense; and
- (c) the blocking of emails or internet access. Such blocking may not occur unless appropriate advance notice has been given to the employee and the employee is also sent a "prevented delivery notice" regarding the blocking of an email as soon as possible after it has occurred. Spam email, emails that are potentially damaging to the computer network, and emails that are reasonably considered to be menacing, harassing or offensive are exceptions to this provision. Furthermore, a prevented delivery notice is not required if the employer is not capable of identifying the addressee of the email. Emails from employees' industrial organisations may not be blocked, nor access to internet sites relating to such organisations, merely because of the fact that those emails and internet sites relate to employees' industrial organisations.

The results of any overt surveillance must not be used or disclosed unless it is for:

- (a) a legitimate purpose relating to the employment of employees or business activities/functions of the employer (including work performance);
- (b) law enforcement purposes;
- (c) for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings; or
- (d) where the use or disclosure is reasonably believed to be necessary to avert an imminent threat of serious violence or substantial damage to property.

Breach of this provision carries a maximum penalty of 20 penalty units (currently \$2,200).

An employee must be notified in writing at least 14 days before the surveillance is implemented unless the employee agrees to a lesser period. For new employees, the notice may be given before the employee starts work. The employer must set out in its policy:

- (a) the kind of surveillance being carried out;
- (b) how the surveillance is being carried out;

- (c) when the surveillance will commence;
- (d) whether the surveillance will be continuous or intermittent; and
- (e) whether the surveillance will be for a specified period or ongoing.

Employers should ensure that the following steps are taken where overt surveillance is to be undertaken:

- (a) all email and internet policies should be reviewed and updated where appropriate;
- (b) employees should be notified in writing of any revisions to the existing policies;
- (c) new employees should be informed that their email and internet usage will be subject to surveillance; and
- (d) current employees must be given 14 days' written notice of any intended surveillance. The surveillance should not commence until after that notice period expires.

2. Silence during contractual negotiations

The decision of the Victorian Court of Appeal in *CCP Australian Airships Limited & Ors v Primus Telecommunications Pty Limited* [2004] VSCA 232 is a timely reminder that silence during contractual negotiations can sometimes constitute misleading conduct under the *Trade Practices Act* and under common law.

Primus entered into negotiations with CCP in relation to a licence for the exclusive use of an airship for advertising and promotional purposes. A representation was made by CCP on 16 February 2000 that the airship, which had not then been manufactured, would be available to Primus for promotional purposes during the Sydney Olympic Games.

On 1 March 2000, CCP stated that unless a deposit of \$400,000.00 was paid by 3 March 2000, CCP could not guarantee delivery of the airship in time for the Sydney Olympics. Primus subsequently paid the deposit which, under the agreement entered into between the parties, was described as being "non-refundable". CCP subsequently failed to supply the airship, thereby repudiating the agreement. At the time the agreement was made, CCP did not itself own an airship and the evidence adduced during the case indicated that it did not have the funds or the ability to acquire an airship. Therefore, CCP could not have made available to Primus an airship for the Sydney Olympics.

Primus brought claims against CCP for return of the deposit both by reason of CCP's misleading and deceptive conduct under the *Trade Practices Act* and also at common law.

The main issue in the case was whether CCP's representation (that unless a deposit of \$400,000.00 was paid by 3 March it could not guarantee delivery of the airship in time for the Sydney Olympics) constituted a guarantee that the airship would be available for the Sydney Olympics if the deposit was paid.

The Victorian Court of Appeal held that a negative stipulation implied a positive covenant that if the deposit was paid, CCP would be able to guarantee delivery in time for the Olympics. The Court found that CCP's financial situation was poor and that at no time did it have any basis for believing that it could raise the funds with which to complete the project.

In essence, the Court found that CCP's silence constituted misleading and deceptive conduct under section 52 of the *Trade Practices Act*. The Court found that, once CCP made the representation on 16 February 2000 that the airship would be available to Primus for promotional purposes during the Sydney Olympics, it had a duty to correct that representation if subsequent events meant that the

position would be altered. The Court found that, by saying nothing thereafter, CCP was guilty of misleading conduct.

Furthermore, the Court found that at common law there was a total failure of consideration on CCP's part and that Primus was able to recover its deposit notwithstanding that the contract stated the deposit was "non-refundable". CCP was ordered to return the deposit.

The case illustrates the onerous nature of duties owed by parties when negotiating with one another, particularly in relation to matters which go to the very core of the contract.

3. A note about blogs

A weblog or "blog" is basically a personal internet journal cum bulletin board. An unrestricted weblog or "blog" is an internet website which enables anyone with internet access to post comments. A restricted weblog permits the posting of comments only by authorised users.

Although blogs are a relatively new phenomenon, they have grown like topsy in the recent past. Some reports put the current number of blogs at in excess of 15 million, up from 7.8 million a mere 6 months ago. These days, a brief surf of the internet will turn up blogs on just about any subject.

However, just because they are relatively new and cyberspace-based doesn't mean that blogs are immune from the law of the land.

The operator of a motor vehicle dealership was recently able to obtain an injunction in the Supreme Court of New South Wales against a blogger (the operator of a blog) who had set up a blog apparently specifically to disparage the dealership (the blogger's car having been stolen from the dealership). The motor vehicle dealer claimed that the name (www.hunterholdensucks.com) and content (uncomplimentary allegations) of the domain amounted to injurious falsehood, namely false statements concerning his business which were calculated to induce others not to deal with him. The injunction precluded the blogger from maintaining the offending domain name or displaying the material contained in that domain or similar material on any Internet website. The blogger was also ordered immediately to shut down the offending domain.

Defamation actions based on the content of blogs will undoubtedly become quite common in the future. However, injunctions restraining publication of allegedly defamatory material are only granted in the very clearest cases, so as to interfere as little as possible with the community's right to discuss in an open forum matters of public interest.

Blogs have given rise to other issues aside from the obvious concerns about injurious falsehood and defamation. Breach of copyright and theft of intellectual property are others another. Most bloggers are neither trained lawyers nor journalists. They are generally less attuned to the legal niceties which preclude the liberal use of others' work and claiming it as their own.

Yet another concern is potential breach of confidentiality. If an employee maintains a blog, there is always a concern that he or she may, even inadvertently, make public information about the employer's business which should remain private. Obviously such things happen all the time in everyday life, but there is a significant difference between gossiping about company business with one or two friends over a beer, and publishing that same gossip as fact on the worldwide web.

A few blogs of interest:

<http://www.froststreet.net/> - The Culinary Adventures of a New York City Lawyer

<http://www.legalunderground.com/> - A blog that asks the questions--can lawyers be entertaining?

<http://www.texasbar.com/saywhat/weblog/index.html> - A weblog of classic humor from U.S. District Court Judge Jerry Buchmeyer

4. The infallibility of fingerprints

Given that the brave new world of biometrics is gearing itself up to be the next level of authentication, it is interesting to note that the reliability of fingerprinting as evidence in criminal hearings in the US is under new scrutiny as reported in *New Scientist* magazine.

The Daubert ruling of the US Supreme Court in 1993 established five criteria for admitting expert testimony. One criteria is that forensic techniques must have a known error rate.

It appears an error rate for fingerprinting has never been established.

A high profile fingerprinting error was the identification of a Portland lawyer, Brandon Mayfield, from finger prints taken in relation to the Madrid bombings on 11 March 2004. Spanish authorities eventually matched the prints to an Algerian despite three FBI examiners and an independent expert agreeing on the original identification.

Where there is a clear fingerprint the chances of that image being mistaken for another are 1 in 10⁹⁷ according to a study by Stephen Meagher of the FBI's Latent Fingerprint Section in Quantico, Virginia.

The problem arises in genuine crime scenes where the latent finger print is incomplete and messy.

In these circumstances a study by Itiel Dror and Ailsa Peron at the University of Southampton , UK, suggest subjective bias can influence the results – for example where fingerprint examiners are asked to verify conclusions already reached by colleagues. Dror and Peron recommend that finger print examiners be distributed work anonymously.

Biometrics which is all about authentication. The idea that your thumbprint, iris, retina, paw print, or facial dimensions can help authenticate you. The idea of multi-factor authentication is that you can use:

1. Something you know (like a password or PIN).
2. Something you have (like a smart card, credit card, driver's license or passport).
3. Something you are (like your finger prints).

On 31 March 2005 News.com.au carried a report from the *New Straits Times* that criminals chopped off the tip of a man's finger in Malaysia to override a high-tech security feature that required his fingerprint to start his luxury car. An Accountant was walking towards his 300,000 ringgit (\$102,584) S-Class Mercedes Benz in a Kuala Lumpur suburb when he was knocked down from behind by a car and subsequently had his index finger cut off when he told thieves the car wouldn't start without his fingerprint.

Not only are there concerns about such scenarios in the brave new world but other issues such as privacy and compliance (in terms of secure data storage) are likely to keep legislators busy in the years to come and that is assuming that the new technology works effectively. By accounts coming out of the US it will be some time before it does and even then two-factor authentication appears preferable no matter what.

Assistance

If we are able to assist you in any of these areas, or other litigation or industrial matters, please contact one of our Litigation Practice Group Team:

- Alex Kohn - 9233 9036 or akohn@makdap.com.au
- Stewart Roberts - 9233 9041 or sroberts@makdap.com.au
- John Baxter - 9233 9037 or jbaxter@makdap.com.au
- Richard d'Apice - 9233 9011 or rdapice@makdap.com.au
- Indran Sinnadurai - 9233 9040 or isinnadurai@makdap.com.au
- Diane Barker - 9233 9034 or dbarker@makdap.com.au
- Marianna Tuccia - 9233 9039 or mtuccia@makdap.com.au
- Claire Mallon - 9233 9038 or cmallon@makdap.com.au
- Brian Trist - 9233 9053 or btrist@makdap.com.au
- Olympia Samolis - 9233 9032 or osamolis@makdap.com.au
- Emma Clarke - 9233 9048 or eclarke@makdap.com.au

Disclaimer

This newsletter is a non-comprehensive general outline of the law as at 25 October 2005. You should not act upon or rely on any information contained in this newsletter without obtaining specific legal advice.

This newsletter and other publications are available from our website www.makdap.com.au. If you would like to receive future issues of this newsletter by email or you wish to unsubscribe, please email mail@makdap.com.au or contact our privacy officer on (02) 9233 7788.

18507