

# Privacy Update

## Employment Focus

September 2004

## The Spam Act – Employer Considerations and Obligations

Employers need to be aware that the *Spam Act 2003* (Cth) goes beyond just protecting consumers against bulk offensive commercial electronic messages. Businesses need to consider their day to day operations and must introduce or update their policies and procedures to ensure compliance with the *Spam Act*.

The *Spam Act* prohibits the sending of commercial electronic messages unless the relevant electronic account-holder has consented to the sending of the message or an exemption applies. To fall within the prohibition, the message must be an "electronic message" and it must be "commercial".

A message is an electronic message if it is sent by email, SMS or by using an Internet based instant messaging service. Facsimiles and voice communications are specifically

excluded from being electronic messages. For a message to be "commercial", it must be for a specified commercial purpose such as offering, promoting or advertising goods, services, investments or land.

In addition, the commercial electronic message must also have an "Australian link". In broad terms this means it must be sent from Australia or be accessed in Australia.

The *Spam Act* contains exemptions which allow commercial electronic messages to be sent to a party without their consent if certain requirements are met. For many employers the most relevant exemption is the "factual information" exemption.

The *Spam Act* contains substantial penalties for breach. If an organisation fails to comply with the provisions in the *Spam Act*, it can be fined in excess of \$1 million per day.

### Compliance issues

There are a number of issues that employers need to consider to ensure compliance with the *Spam Act*. Companies need to conduct a review of existing email and privacy policies and procedures which regulate the use of company email and other electronic resources, consider any existing databases and how these databases operate, review email templates, client

The Spam Act – Employer Considerations and Obligations	1
Bad Connection: Union Breaches Privacy and Copyright Laws	2
Surveillance In The Victorian Workplace	3
Use of Surveillance Evidence	4
Privacy Issues – The Provision of Employee Information During Due Diligence	4
Privacy and Pre-Employment Medicals	5
Use of Medical Information Obtained by Self Insurer	6
Checking References	7
Email and Internet Use	7

## Key Points

- Review existing email, Internet and privacy policies for compliance with the *Spam Act*.
- Review advertising and marketing strategies (including databases) and electronic distribution of information to clients and change the existing practices, where required to comply with the *Spam Act*.
- Conduct a review of existing client databases or client contact details to assess any consent provided by clients to the receipt of commercial electronic messages.
- Implement updated policies which comply with the *Spam Act* and inform and train employees on these policies.

lists and the process adopted in the collection and use of electronic address details. International companies must also review overseas operations and consider adopting company-wide electronic resources and privacy policies.

Unlike the *Privacy Act 1988* (Cth), the *Spam Act* applies to all Australian companies, no matter what size they are. Therefore, all Australian organisations must ensure that employee use of email, Internet and other electronic resources complies with the *Spam Act*.

Jan Dransfield, Partner, Sydney  
jan.dransfield@bdw.com

Bridget Maguire, Lawyer, Sydney  
bridget.maguire@bdw.com

# Bad Connection: Union Breaches Privacy and Copyright Laws

A single judge of the Federal Court has awarded damages to the Seven Network after a union breached the *Privacy Act 1988* (Cth) and the *Copyright Act 1968* (Cth) during negotiations about a workplace agreement. The union used a list of employees' phone numbers compiled by Seven to contact employees about the proposed agreement: *Seven Network (Operations) Limited v Media Entertainment and Arts Alliance* [2004] FCA 637.

## Background

The Seven Network had been unsuccessfully engaged in negotiations with the Media Entertainment and Arts Alliance (MEAA) for an enterprise bargaining agreement. The MEAA had obtained information about Seven's employees in the form of a document which included telephone contact numbers and job position titles. Seven did not provide the information, or consent to its disclosure. The MEAA claimed the document had been sent to them anonymously in the mail. The footer had been cut off the document, probably to avoid disclosing the identity of the person who had provided the document to the MEAA.

The MEAA used the information to arrange for a call centre (Connect) to contact employees and find out their views about the proposed agreement. After Connect had collected the data, they relayed it back to the MEAA.

Seven alleged that the MEAA had acted with intent to coerce its employees to vote against the proposed agreement in breach of section 170NC of the *Workplace Relations Act 1996* (Cth). In addition, Seven claimed that the receipt and use of the document by the MEAA meant it had breached the National Privacy Principles (contrary to the *Privacy Act*). Seven also argued that the use of a telephone contact list prepared by, and belonging to, Seven constituted a breach of the *Copyright Act 1968* (Cth).

## Federal Court decision

Seven's claim that the MEAA campaign amounted to coercion failed because Justice Gyles found that telephoning employees to ask their views about the proposed agreement did not demonstrate an intent to coerce their vote.

In relation to the *Privacy Act* claim, Justice Gyles found that the MEAA's receipt of the telephone list constituted "collection of personal information" within the ordinary meaning of the words. However, the court could not tell if the MEAA had "collected" the information after 21 December 2001 being the date on which the *Privacy*

*Act* commenced. Because there was a chance the telephone information was collected before 21 December 2001, Seven could not prove such a collection breached the *Privacy Act*.

However, a separate breach of the *Privacy Act* was made out in relation to the survey information received by the MEAA from Connect. The survey information contained details of employees with an interest in the MEAA and of those wishing to receive more information about the MEAA. The Court took the view that this information was not necessary for the MEAA's functions regardless of how useful or desirable it was to the MEAA. In these circumstances the Court held that the MEAA breached the *Privacy Act* by unnecessarily collecting this personal information.

In relation to the actions of Connect in contacting employees to obtain personal information (at the behest of the MEAA), the Court found that it was the MEAA that had to justify collection of the information. The result was that Seven got its injunctions against the MEAA, despite the fact that it was Connect who actually undertook the research.

However, it was on the basis of breach of copyright that Seven was most successful. Both the MEAA's and Connect's use of the phone directory was found to constitute a breach of copyright. Damages of \$10,000 were awarded against the MEAA, and damages of \$2,500 were awarded against Connect.

Timothy Lange, Senior Associate, Melbourne  
timothy.lange@bdw.com

Vanessa Swannie, Articled Clerk, Melbourne  
vanessa.swannie@bdw.com

## Key Points

- Confidential employee records, including basic information such as phone numbers or addresses, should be kept secure.
- An action for breach of the *Privacy Act* may be brought directly in the Federal Court, bypassing any Privacy Commissioner ruling.
- In future, union demands that certified agreements include an obligation on the employer to supply information about new employees may become much more hard-fought.



# Surveillance in the Victorian Workplace

**An employee of your business has made three complaints in the past two weeks to Human Resources about an unknown person placing flowers on his car. He finds it creepy.**

The car is parked in the work car park located in the basement of the work building. Only employees of your business have access to this car park by electronic pass.

## What do you do?

One approach may be to covertly install a camera in the car park in order to identify the unknown individual. Surveillance in Victoria is regulated by the *Surveillance Devices Act 1999* (Vic). This Act prohibits the installation or use of a camera in the car park if it will be used to record a "private activity".

"Private activity" means "an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include: (a) an activity carried on outside a building; or (b) an activity carried on in any circumstances in which the parties to it ought reasonably to expect that it may be observed by someone else."

As other employees have free access to this car park, it is unlikely that activities taking place there will be considered to be "private". If the activities were "private", however, consent of the users of the car park would be required prior to the installation and use of the camera.

## The camera is installed and the person is caught

The law is likely to change as a result of new legislation being mooted in Victoria.

On 5 March 2002 the Victorian Attorney General launched the Victorian Law Reform Commission's reference into workplace privacy and surveillance. This reference is at an advanced stage and an Options Paper will be released shortly for consultation with various interest groups including employers. Similar reviews have been occurring in other States.

**Sarah Rey, Special Counsel, Melbourne**  
sarah.rey@bdw.com

**Michael Tamvakologos, Lawyer, Melbourne**  
michael.tamvakologos@bdw.com

## Key Points

- Workplace surveillance is a powerful tool when used appropriately. Employers should be careful, however, to only use it where it is necessary to do so and does not infringe the law.
- The installation, use or maintenance of a surveillance device is prohibited where a "private conversation" or "private activity" is being recorded in some way.
- Employers need to keep track of legislative amendments impacting on the right to use surveillance equipment in the workplace.

Employers need to be careful to use surveillance only when it is necessary and to ensure it does not infringe the law.



## Use of Surveillance Evidence

In an unfair dismissal case, the NSW Industrial Relations Commission ordered that nine security officers previously employed by Western Sydney Area Health Services should be reinstated with back pay: *Staal, Tupene and Health and Research Employees' Association of NSW (on behalf of Nagy and Ors) v Western Sydney Area Health Service* [2004] NSWIRComm 27 (11 March 2004, Sams DP).

The security officers had been dismissed, or forced to resign, after the employer's investigation found they had engaged in serious misconduct.

The employer's investigation relied on covert video surveillance gathered by external agents. The *Workplace Video Surveillance Act 1998* (NSW) (*Surveillance Act*) requires employers undertaking such surveillance to obtain an authority from a Magistrate.

Although the employer obtained this authority, it was held that the employer had breached the *Surveillance Act* by conducting most of the surveillance before the authority was obtained, and then, once the authority was obtained, conducting the surveillance outside its specifications.

The Commission found that "The surveillance was clumsy, incomplete, inaccurate and had the hallmarks of a Keystone Cops episode." It criticised the surveillance operator and stated that "a surveillance operation should only report what it observes, not make subjective conclusions as to whether a particular activity constituted gross misconduct or corrupt practices".

The Commission criticised the employer for over reliance on the surveillance operator's report and for not testing the report's findings before making a decision to dismiss the security guards.

Mary-Jane Ierodionou, Senior Associate,  
Melbourne  
mary-jane.ierodionou@bdw.com

Trent Sebbens, Lawyer, Sydney  
trent.sebbens@bdw.com

## Key Points

- Establish a written brief for the surveillance agent on the work to be undertaken including the duration, location and persons to be under surveillance.
- Obtain an order from a Magistrate prior to the agent conducting covert surveillance at the workplace, and ensure that the agent is aware of, and complies with, the terms of the order. Reports should also be provided to the Magistrate as required under the *Surveillance Act*.
- Undertake a rigorous review of the report, notes and video provided by the agent, including interviewing the agent to ensure the veracity and consistency of the evidence provided.
- Conduct further investigations to establish corroboration (or otherwise) for the evidence provided by the surveillance, especially where this evidence is being relied upon as justification for the dismissal of an employee.

## Privacy Issues – The Provision of Employee Information During Due Diligence

During a sale of business due diligence investigation, prospective purchaser organisations and their advisers will often review information relating to the business of the vendor organisation, including information about the employees of the business. If this is personal information, the parties to the sale of business should consider their obligations under the *Privacy Act 1988* (Cth).

The Privacy Commissioner has published an Information Sheet making a number of suggestions about how vendor and purchaser organisations should proceed to deal with personal information in the context of a due diligence exercise (*Information Sheet 16 – Application of Key NPPs to Due Diligence and*

*Completion When Buying and Selling a Business*). In relation to a vendor organisation it suggests that, wherever possible, personal information be aggregated and de-identified before being disclosed. In many cases such information will be adequate for the purchaser's purposes. Where it is not, further consideration should be given

## Key Points

- Vendor and purchaser organisations must carefully consider their obligations under the *Privacy Act* before disclosing or collecting personal information about employees in the context of a sale of business.
- Wherever possible, information should be released in an aggregated and de-identified form.
- Protocols concerning the review and collection of personal information should be established and implemented.

to whether the provision of more detailed information is appropriate.

Regarding a prospective purchaser organisation, the Privacy Commissioner recommends that:

- where appropriate, the information be inspected, rather than collected;
- only information necessary to the due diligence investigation be inspected or collected;
- copies not be taken;
- access be restricted to those people who need to make the investigation;
- the information collected only be used for due diligence purposes until the sale of business is completed; and
- if the sale of business is not completed, the information be destroyed or returned to the vendor.

The Privacy Commissioner also recommends that the vendor require the purchaser to follow these protocols.

**Nereda Thomas, Senior Associate, Melbourne**  
nereda.thomas@bdw.com

**Arianna Levy, Lawyer, Melbourne**  
arianna.levy@bdw.com

## Privacy and Pre-Employment Medicals

Many employers require prospective employees to undergo a pre-employment medical examination as part of the company's process of recruitment. Employers should be aware of privacy laws in their collection and use of pre-employment medical examinations.

For example, the *Health Records Act 2001 (Vic)* applies to any health information relating to employees in Victoria, whether past, current or prospective employees. Employers who hold any health information relating to individuals, such as that collected during a pre-employment medical, are bound by this Act and must comply with the Health Privacy Principles contained in the Act.

Under the *Health Records Act*, an individual has a general right of access to health information relating to that individual, held by an employer. This right of access may be exercised by inspecting the health information and having the opportunity to take notes of its contents, or by receiving a copy or a summary of the health information, or viewing the health information and having its contents explained.

The handling of employees' personal information in the private sector is also regulated by the *Privacy Act 1988 (Cth)*. This does not currently apply to information held by an employer about its current and former employees, where the information is used or disclosed for a purpose directly related to the employment

relationship. However, the employee records exemption is currently under review. Further, the employee records exemption does not apply to personal information about unsuccessful job applicants, for example, it does not cover pre-employment medical examination information.

Under both the *Health Records Act* and *Privacy Act*, employers should tell prospective employees, amongst other details, how the medical examination results will be used and to whom they will be disclosed. Employers should not use results for any other purpose, and particularly not for an unlawful discriminatory purpose. Equal opportunity laws specifically prevent the request of information for any discriminatory purpose.

**Mary-Jane Ierodiaconou, Senior Associate, Melbourne**  
mary-jane.ierodiaconou@bdw.com

**Lisa Jarrett, Articled Clerk, Melbourne**  
lisa.jarrett@bdw.com

### Key Points

- Pre-employment medical examinations must relate to the candidate's capacity to undertake the essential requirements of the job.
- Candidates undertaking a pre-employment medical examination should be given a privacy notice explaining the purpose of the examination, how the examination results will be used and disclosed, and how they may access the results.



# Use of Medical Information Obtained by Self Insurer

In a recent decision in the Queensland Industrial Relations Commission, a Woolworths' employee dismissed on the basis of medical information supplied to the employee's manager by Woolworths self-insurance division, RISK, was reinstated. In the decision, the Commission was critical of RISK's disclosure of the medical information to the employee's manager: *Shop, Distributive and Allied Employees Association (Queensland Branch) Union of Employees and Woolworths Limited (Fruitex – Richlands) 176 QGIG 147*.

The Commission found that medical information about the employee obtained for the purpose of the employee's workers compensation claim should only have been disclosed to the employee's manager to assist with the employee's rehabilitation. It should not have been used for the purposes of assessing the employee's fitness for work or dismissing the employee. The Commission also found that RISK had breached the confidentiality of the medical report by providing details of it to the employee's manager without the employee's consent.

Woolworths appealed the decision. President Hall dismissed the appeal

after considering the medical evidence on which the decision to dismiss was based.

President Hall found it unnecessary to reach any conclusions about the "inappropriate use of the medical report". However, he considered the Commission's comments in this regard and said that "the Commission was not obviously correct". He suggested that "the debate about the confidentiality of information obtained during rehabilitation" raised issues which would be "better resolved by policy makers than by lawyers".

Sonya Greaves, Senior Associate, Brisbane  
sonya.greaves@bdw.com

## Key Points

- Employers may be liable under occupational health and safety laws if they fail to act on information about an employee's fitness for duty. The knowledge of an employer's workers compensation unit may be imputed to the rest of the business.
- Self insurers should, however, exercise caution when disclosing medical evidence to an employee's manager for a purpose unrelated to the employee's workers compensation claim (eg the purpose of considering an employee's fitness for duty).
- When obtaining medical information about an employee to support a workers compensation claim, a self insurer should seek the employee's consent to use the information for other purposes (eg assessing the employee's fitness for work).
- At least in Queensland, there has been a call for Parliament to enact a law dealing with the disclosure of medical information by a self insurer. Self insurers should watch out for changes in this area.

medical records

## Checking References

Many employers remain unclear about their obligations under the *Privacy Act 1988* (Cth) in relation to obtaining and giving references for potential, current and past employees. Some employers have erred on the side of caution and have implemented a blanket policy of not providing references at all. However, if the employer is careful about the type of information that is disclosed, there may be circumstances where an employer can disclose certain information without breaching the *Privacy Act*.

A way to minimise the risk of breaching the *Privacy Act* is for a current or past employer to obtain consent from an individual to disclose certain personal information to a prospective employer.

For example, in *C v Commonwealth Agency* [2003] PrivCmrA 1, an employee asked a supervisor to be a referee for an application for a position with another Commonwealth agency. In providing a reference, the supervisor told the interview panel that the employee suffered from epilepsy and depression, had been on sick leave and did not cope well under stress.

The Privacy Commissioner found that an individual may imply consent to the disclosure of a range of personal information relating to skills, work experience and personal attributes related to a particular position. The disclosure of susceptibility to stress was something the employee imply consented to as it is relevant in an employment context.

However, the disclosure of information about medical conditions and past sick leave taken could not be construed as being within the scope of that implied consent. As a result of the Privacy Commissioner's

## Key Points

- Employers should be careful not to provide incorrect or irrelevant information in breach of the *Privacy Act* when providing employee references.
- An employee may imply consent to the disclosure of some personal information but this may not include medical information or details about sick leave taken.

investigation, the agency apologised to the complainant and paid compensation of \$7,000.

Craig Taylor, Senior Associate, Perth  
craig.taylor@bdw.com

## Email and Internet Use

The growth in email and Internet use at work has presented employers with a range of significant management challenges. Key amongst these is the need to take disciplinary action, including possible termination of an employee's employment, for misuse of an employer's email or Internet network.

While each case will need to be assessed on its own merits, a review of the authorities provides significant guidance to what will be considered by industrial tribunals when assessing the fairness of a termination of an employee's employment for misuse of emails and/or the Internet.

The Office of the Federal Privacy Commissioner has also issued draft guidelines on workplace email, web browsing and privacy.

## Key Points

- It is important to have a clear policy in place for the use and monitoring of emails and Internet browsing.
- Development of the policy needs to take into account privacy law as well as employment and industrial considerations.
- A failure to properly deal with this area may expose an employer to significant risk and liability.



If an employer fails to properly deal with the misuse of emails and the Internet, significant liabilities can arise. For example, employers have significant duties and liabilities under anti-discrimination laws and a failure to properly deal with misuse of emails and the Internet may leave an employer badly exposed.

Similarly, employers have duties under workplace health and safety laws to provide a safe place of work. This

duty will not be satisfied if an employer allows email and the Internet to be used in a way which may cause stress, hurt and humiliation to its employees. Depending upon the character of the material being accessed or distributed, it is possible that breaches of criminal laws may also be committed.

**Ian Humphreys, Partner, Brisbane**  
ian.humphreys@bdw.com

## Key learnings

Set out below is a summary of the key learnings from the authorities and the Federal Privacy Commissioner's guidelines:

1. **Employers should have a clear policy in relation to the use and misuse of the Internet and email in the workplace, which:**
  - a) **sets out in clear terms what is a permitted and a proper use of the network; and**
  - b) **has been clearly communicated to, and understood by, employees. Training and the use of a "pop-up", which reinforces the policy each time an employee logs on to his or her computer, can be very helpful in satisfying a tribunal about this.**
2. **Employers must apply the policy in a fair and consistent manner, particularly where there have been several breaches of the policy.**
3. **Employers must follow a fair procedure for dealing with an employee's breach of the policy before any decision to dismiss the employee is made.**
4. **The policy should clearly set out what information is logged by the employer and who in the employer's business has rights to access the logs and content of employees' emails and browsing activities and in what circumstances this will occur.**
5. **The policy should refer to the employer's network security policy and that improper use may impact upon network security.**
6. **The policy should be reviewed regularly to ensure it properly reflects advances in technology.**
7. **Any penalty imposed on an employee for breach of the policy should be proportionate and take into account, for example, the employee's level of culpability and the number of times the misuse has occurred and the type of material involved.**
8. **Dismissal will be difficult to justify in circumstances where the culture of the workplace condoned improper use, such as downloading pornographic material, and the employer knew about the culture but failed to put a stop to it.**

### BDW Contact Details:

<b>Sydney</b>	Tim Brookes Jan Dransfield	(02) 9258 5770 (02) 9258 6533	<b>Brisbane</b>	David Wenck Ian Humphreys	(07) 3259 7219 (07) 3259 7180
<b>Melbourne</b>	Gordon Hughes Vince Rogers Kent Davey Mary-Jane Ierodionou	(03) 9679 3395 (03) 9679 3522 (03) 9679 3762 (03) 9679 3372	<b>Perth</b>	Anthony Willinge Tony Davies	(08) 9366 8165 (08) 9366 8767
			<b>Canberra</b>	Ian Oi Paul Vane-Tempest	(02) 6234 4000 (02) 6234 4036
			<b>London</b>	Geoff Hone	(44 20) 7600 3030

This publication is authorised by Blake Dawson Waldron. The firm can be contacted by emailing [marketing@bdw.com](mailto:marketing@bdw.com)

**Subscription Maintenance** – If you would like to unsubscribe or modify your electronic subscription please go to <http://www.bdw.com/subscriptions>

**Privacy Policy** – You can find our Privacy Policy on our website at <http://www.bdw.com>

*Where applicable, liability limited by the Solicitors' Scheme, approved under the Professional Standards Act 1994 (NSW). This publication is intended only to provide a summary of the subject matter covered. It does not purport to be comprehensive or to render legal advice. No reader should act on the basis of any matter contained in this publication without first obtaining specific professional advice.*