Newsletter
Stephens Lawyers & Consultants

February 2004

Legal Risks Associated With Email and Internet Use and Abuse by Employees

The potential for abuse of email and Internet facilities provided at the workplace is virtually limitless and could have severe legal ramifications for employers. Employers can be held vicariously liable for discriminatory, sexually harassing or victimising material sent by their employees under the *Equal Opportunity Act 1995 (Vic)*. There are additional risks in the area of copyright infringement and defamation. **(1.)**

Monitoring The Email And Internet Activities Of Your Employees?

Many employers monitor the email and Internet usage of their employees without recognising that there are privacy issues which can restrict the type of monitoring employers can perform. The *Privacy Act 1988 (Cth)* contains a set of National Privacy Principles which apply to all private sector businesses with a turnover of more than $3 million. **(2.)**

Do You Have An Email and Internet Policy?

A comprehensive email and Internet policy is essential where employees have access to email and the Internet. In the recent case of *Lulham v Shanahan, Watkins Steel and Others* [2003] QADT 11 , the court suggested that had the employer notified employees of their obligation not to sexually harass other employees, it may have resulted in the employer successfully defending the vicarious liability suit which ultimately cost them $26,000 in compensation.

In addition, an unfair dismissal claim was recently defeated by an employer due to an email and Internet policy being displayed on a pop-up screen when the employee logged on to their computer, as the employer was able to show that they took reasonable steps to inform staff of their policy. **(3.)**

(1.)

Legal Risks Associated With Email and Internet Use and Abuse By Employees

Legal Risks for Employers

There are a number of legal hazards that employers risk exposure to if their employees abuse email or Internet facilities provided to them in the workplace.

Vicarious Liability

Pursuant to the common law doctrine of vicarious liability, employers may be liable for acts of their employees where the employees have committed the acts in the course of their employment or while acting as an agent of the

employer. Employers have been successfully sued under this doctrine where their employees have harassed other employees in the workplace, leading to the payment of fines and damages.

Email and Internet availability increases the methods by which employees can be harassed or discriminated against. Compounding this, some workers perceive email as a more informal mode of communication, escalating the risk of inappropriate or offensive "jokes" being sent without consideration of the consequences.

The *Equal Opportunity Act (Vic)* prohibits sexual harassment, discrimination and victimisation in the workplace. Sections 102 & 103 establish that acts of sexual harassment, discrimination and victimisation by an employee in the workplace can constitute a vicarious act of the employer unless the employer took reasonable precautions to prevent it.

In practice, this means that if employees send or show offensive or harassing material to other employees and vicarious liability is established, the employer will be facing the harassment charges alongside the errant employees.

Lulham v Shanahan, Watkins Steel and Others [2003] QADT 11

In a case before the Queensland Anti-Discrimination Tribunal last year, an employer was held vicariously liable for the sexual harassment of one employee carried out by two other employees.

The court held that the employer failed to show that it had taken reasonable steps to prevent staff contravening the *Anti-Discrimination Act (Qld)* (Equivalent to the Victorian *Equal Opportunity Act*). The fact that the employer had an 'open door' policy for complaints was considered insufficient to defend the vicarious liability suit.

An alarming aspect of the decision was the court's declaration that it was irrelevant that the victim had failed to inform the employer of the sexual harassment as actual knowledge was unnecessary.

While this case did not involve harassment via the Internet or email, when a court is determining the liability of the employer for the acts of employees, it is likely to be immaterial how the sexually harassing act was perpetrated. Thus if a similar case arose where the harassment was executed via an email, a similar outcome could be expected.

Legal Liability Hazards under Copyright Law

An employer who merely provides the electronic means for an employee to infringe copyright and fails to prevent the employee doing so, could face legal action for copyright infringement.

Subject to the fair dealing exceptions contained in the *Copyright Act* 1958, copyright is infringed by a person who, not being the owner of the copyright and without the licence of the owner of the copyright, does ***or authorises the doing of*** *in Australia any act comprised in copyright* [1] . Sections 31, 85(1) and 86 of the *Copyright Act 1968* set out the acts comprised in copyright. [2]

If a person authorises the doing of any of the acts comprised in copyright of a protected work without the licence of the copyright owner, they themselves infringe the copyright in that work. In determining whether a person has authorised the doing of an act comprised in copyright without the licence of the copyright owner, the following matters have to be taken into account:

- the extent of the person's power to prevent the doing of the act concerned
- the nature of any relationship existing between the person and the person who did the act concerned
- whether the person took any reasonable steps to prevent or avoid the doing of the act including complying with any industry codes of practice.

(Sections 36 (1A) and 101(1A) *Copyright Act 1968*).

Examples of where Australian courts have found cases of authorisation of copyright infringement include a hotel hosting a band which plays copyright protected songs and a University which provides photocopiers for students who are infringing copyright by photocopying too much of a textbook.

In the High Court case of *University of NSW v Moorhouse* (1975) 133 CLR 1, the University was held to have authorised infringement of copyright when a student made a copy of a book on a University library photocopier. The High Court declared that the University had authorised the infringement because the University provided the photocopying machines used to reproduce the book, allowed unsupervised access to the machines and took no reasonable steps to prevent the infringement. This was held despite the fact that the student was making the copy for himself alone and the University was unaware of his copyright infringement. The Court interpreted "authorise" to mean "sanction, approve, countenance".

Where an employer provides Internet access to employees and those employees then infringe copyright by downloading music or video onto a company's computers, the employer faces the risk of being sued for authorising copyright infringement if the employer has not taken reasonable steps to prevent or avoid the infringement by its employees. Devices that may assist companies avoiding a copyright infringement claim include Internet usage policies, electronic warnings, employee training and electronic filtering.

Defamation

Defamation is a common law tort whereby a communication occurs between two or more people which tends to cause a third party's reputation to be negatively affected. This communication could be expressed verbally, in writing or as pictures, such as a cartoon or doctored photograph.

A defamatory communication can be identified by its tendency to lower a party in the eyes of others or injure the reputation of a party. It is easy to imagine how a "joke" email authored by an employee could contain material which disparages a colleague, customer or business rival. It is still easier to imagine such an email being forwarded through an entire organization within minutes. In this scenario, what may have begun as a thoughtless comment or joke about someone's work or personal life within a social email between colleagues could reach the person who is the subject of the comment and quickly develop into a defamation action.

Defamation in the Workplace

Although the primary responsibility for a defamatory publication falls on the publisher, a party who authorises the publication is also liable. An employer can be held vicariously liable for the defamatory publication of its employees where it is held to have authorised the publication or where the publication was made in the normal course of employment. Knowingly allowing employees to regularly send "joke" emails of an offensive or defamatory nature could be interpreted by a court as authorising such emails, leaving employers open to vicarious liability suits for defamation.

Defamatory publications made in the normal course of employment could also lead to employer liability for defamation. Publications made in the normal course of employment could conceivably include employees creating or updating intranet or external internet pages. Employers must be careful to implement a policy which strictly governs what material employees place on intranet pages or the employer's external internet site and monitor the content of these regularly.

(2.)

Monitoring of Employee Use of Internet and Email

Employers may wish to monitor the on-line activities of employees for a number of reasons, for example:

- to keep a log of emails sent and Internet sites viewed by employees
- to detect employees sending offensive, defamatory, confidential or copyright material via company networks
- to deter employees from accessing and downloading inappropriate material from the Internet

It is important to recognise that simply monitoring abuses of email and Internet systems will not address all legal hazards. Email is notoriously difficult to retract once it is sent and a mere record of unauthorised email and Internet use will not be sufficient to deflect legal liability.

Privacy Implications of Monitoring for Private Sector Businesses

Although there is no constitutional or common law right to privacy, the *Privacy Act* 1988 (Cth) imposes privacy principles on the private sector. Businesses with an annual turnover of less than $3 million are exempted, but are subject to restrictions relating to the commercial use of personal records. This includes the prohibition on selling any material contained in employee emails where the information allows the individual to be identified.

Private sector organisations with an annual turnover of more than $3 million along with all health service providers regardless of turnover have the option of either adopting the National Privacy Principles or developing a privacy code of their own.

The National Privacy Principles deal with the collection, handling and storage of personal data and are designed to ensure that personal information held by private sector organisations is managed in a reasonable and suitable manner.

The first, and most relevant privacy principle, concerns the collection of personal information and requires that the collection of personal information be carried out by lawful and fair means. The Federal Privacy Commissioner refers to this principle in the Guideline on Workplace Email, Web Browsing and Privacy, and concludes that where the logging of employee network activities occurs without employee knowledge, it could be considered unfair and thus in breach of the privacy principle.

In *Halford v UK* [1997] IRLR 471, a case heard before the European Court of Human Rights, an employer who monitored an employee's telephone calls without her knowledge was ordered to pay compensation. The court found that private telephone calls were covered by a concept of 'private life' and therefore the employee had a reasonable expectation of privacy. It is conceivable that the monitoring of employee emails without their knowledge could be viewed in the same way.

Consequently, if monitoring is going to occur in your workplace, employees must be informed that monitoring will take place and should be informed of the nature of the monitoring activities.

(3.)

Email and Internet Policy

Adopting an Email and Internet Usage Policy

A well-drafted email and Internet policy which is communicated to each employee, preferably upon induction, and which is updated and brought to the attention of employees regularly may avoid legal risks associated with employee email and Internet abuse.

However, the mere existence of an Internet and email policy on its own will not be sufficient for an employer to successfully defend a legal claim based on vicarious liability, defamation or copyright infringement. All breaches of the policy must be met with an appropriate level of disciplinary action by the employer.

Employers have successfully used email and Internet facility policies to defend claims for unfair dismissal where an employee's employment has been terminated for misuse of the Internet in the workplace.

In the recent case of *Bassam Darwich and Kaal Kaal Australia Limited* (U2002/4250) , the Australian Industrial Relations Commission found that an employer was justified in dismissing an employee who had stored inappropriate and offensive material on the company's computer. The Commission held that the employee was deemed to be aware of the company computer policy due to a 'pop-up' screen which contained the policy. The Commission considered that the employer had taken reasonable steps to bring the relevant policy to the attention of employees and upheld the dismissal.

Content of Policy

There are no rules or regulations which set out the content of an email and Internet policy. The policy can and should be tailored to your individual workplace. The most important aspect of creating an effective policy is to ensure that it is clear and any key terms are explained.

In the Federal Court, the case of *Australian Municipal, Administrative, Clerical and Services Union (ASU) v Ansett* [2000] FCA 441, highlighted the importance of having a clear policy.

Ansett dismissed an employee who distributed an ASU bulletin on Ansett's internal email system. Ansett claimed this was a breach of the Ansett IT policy which permitted email use "for the purpose of performing authorised lawful business activities". The Federal Court found that the distribution of union bulletins on Ansett's email system fell within "authorised, lawful business activities" and in the decision Justice Merkel emphasised:

"the desirability of employees having been made aware, in clear terms of the criteria establishing the circumstances that constitute acceptable and unacceptable use of their employer's email or IT system."

[1] Section 36(1) - Infringement of copyright in literary, dramatic, musical or artistic works.

Section 101(1) - Infringement of copyright in subject matter other than works (sound recordings, cinematograph films, television and sound broadcasts).

[2] For a literary, dramatic or musical work, copyright is the exclusive right to:

- reproduce the work in a material form
- publish the work
- perform the work in public
- communicate the work to the public
- make an adaptation of the work

(Section 31(1)(a))

For an artistic work, copyright is the exclusive right to:

- reproduce the work in a material form
- publish the work
- communicate the work to the public

(Section 31(1)(b))

For a sound recording, copyright is the exclusive right to:

- make a copy of the sound recording
- cause the recording to be heard in public
- communicate the recording to the public
- enter into a commercial rental agreement in respect of the recording

(Section 85(1))

For a cinematograph film, the copyright is the exclusive right to:

- make a copy of the film
- cause the film, insofar as it consists of visual images, to be seen in public, or, insofar as it consists of sounds, to be heard in public
- communicate the film to the public

(Section 86)