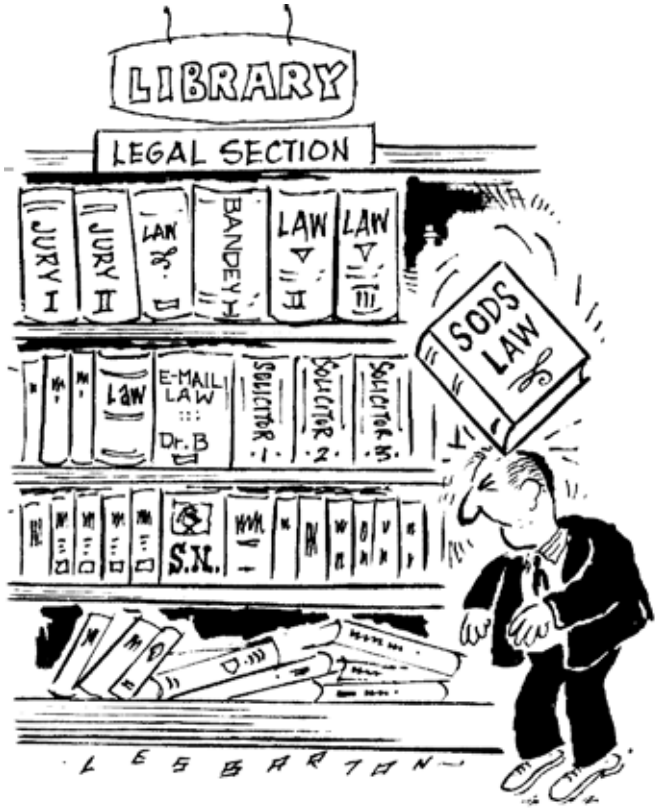
A Briefing Paper On The Principles Of Corporate Legal Exposure Arising By Virtue Of Employee Misuse Of E-Mail, Instant Messaging And Internet Access

Contents

The purpose of this Briefing Paper is to provide an initial entrée into the classes of Legal Exposure which can arise for corporate entities when their employees misuse Email, Instant Messaging and Internet Access facilities provided for them.

Author: Dr Brian Bandey

MARSHAL
Secure. Protect. Comply.



1. INTRODUCTION

The purpose of this Briefing Paper is to provide an initial entrée into the classes of Legal Exposure which can arise for corporate entities when their employees misuse E-Mail, Instant Messaging and Internet Access facilities provided for them. Although the intention behind the production of this Briefing Paper is to provide the reader with an understanding of how the employer organisation can become legally exposed in this particular sphere; it is important to similarly understand the limitations of a short document such as this. They are:

(i) this is an English Law (EU Law Context) only analysis;

(ii) it is confined to employer-employee relationships;

(iii) it will treat Instant Messaging and Web-Based Mail as "E-Mail"[1] ; and

(iv) it is an "Overview" of the position only.

So if these are this Briefing Paper's limitations, what is its utility? To answer that question, it is first of all necessary to understand that there is no single, cohesive area, theory or doctrine of law which applies in this area. Rather, the activity of Corporate E-Mail and Internet Access Misuse occupies a space at the intersection of a number of significant, well-established and important theories of law. What this Briefing Paper can do therefore is (including real-life examples) identify the types of 'misuse' that arise and describe the applicable Law in broad terms.

2. SPECIES OF MISUSE AND APPLICABLE DOCTRINES OF LAW

When addressing the consequences of corporate employees 'misusing' E-Mail and Internet Access, this Briefing Paper will not generally differentiate between undesirable activity which is brought about intentionally (for example, a group of employees writing and sending sexually explicit E-Mails about another employee) and undesirable activity which is brought about unintentionally (for example, a medical secretary mistakenly E-Mailing confidential patient information to an unintended recipient).

Similarly, this Briefing Paper will seek to identify areas of potential legal liability and exposure that arise not only through the purely internal activities of corporate employees, but also identify how liability can arise flowing from the employer

1 Since the legal rules of ownership apply equally to all forms of messaging, and since all messaging involves a form of TCP/IP packetised protocols always involving, at least, a transient copy of the message existing on the employer's computer system, it is argued that it is a proper position to treat all messaging as "E-Mail" for the purposes of this Briefing Paper.

MARSHAL
Secure. Protect. Comply.

to the employee when inappropriate material makes its way into the corporate e-environment from the outside.

The areas of Law which intersect over the space of E-Messaging and Internet Access Misuse include:

The Law of Confidence
The Law of Contract
The Law of Copyright
The Law of Torts
Data Protection Law
Criminal Law
Human Rights Law
Employment Law

For ease of reference, this 'activity area', this 'space' (so to speak) of misusing E-Mails and Internet Access over which and through which so many important, settled and significant areas of Law intersect will be referred to in this Briefing Paper as the "HazardSphere[2]".

Classes of "Misuse" to be addressed by this Briefing Paper include:

Harassment by E-Mail
Indirect Harassment via Internet Access
Unlawful Discrimination
Defamation by E-Mail
Distribution of Confidential Information
Infringement of Copyright
Distribution of Obscene Material

This Briefing Paper will further address the Legal Exposure that may arise to an employer who permits employees to be exposed to Spam E-Mail containing pornographic or inappropriate content.

3. A WORD CONCERNING THE SOURCE OF THE PROBLEM

This is a Briefing Paper directed solely to the Legal Exposure that may arise for Corporate Employers out of the HazardSphere and is not a paper directed to the sociological source of the behaviour sets which go to produce these forms of Legal Exposure. However, it is suggested, that a very brief discussion of the behavioural and attitude-based causes of the mischief at the heart of the HazardSphere is relevant.

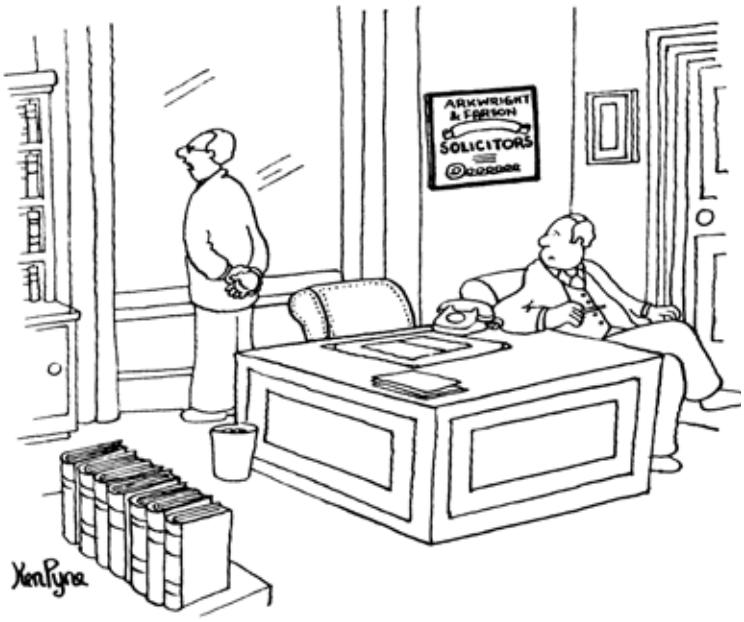
It is suggested that it must be recognised that many employees will assume, in the absence of receiving express rules to the contrary, that they may make use of their employer's E-Mail and Internet Access systems for personal and private use at their sole and entire discretion. Clearly employees who make this assumption will spend (from the employer's perspective) unacceptable amounts of their employer's time engaging in their own private activities. It is difficult to apportion legal blame to employees who use E-Mail and Internet Access for personal purposes

2 "HazardSphere" is a trade mark of Mailogic Limited and is used herein with their kind permission.

in circumstances where their employer has not issued guidelines on where the boundaries of their permitted use lie.

Sending an E-Mail has often been likened to sending a postcard. Many employees continue to be unable to grasp that the E-Mails they send are neither secure nor confidential. They further often do not understand that as soon as an E-Mail is sent, a permanent digital-computer record is created of what was written, the name of the person who wrote it, the time and date of creation and transmission, and the name of the employer. Overarching this state of ignorance is a modern attitude towards E-Mail of presumed informality that crosses all hierarchical boundaries within organisations. A custom has evolved that the style of communication used in E-Mails can and indeed should be informal. However, the great deal of difference that exists between the informal and sloppy, the rude and flippant is similarly unrecognised. The lack of appreciation of this distinction based against this attitude of presumed informality has fuelled the litigation over the misuse of E-Mail and Internet Access.

It should be understood that it will be the responsibility of the employer to define and communicate what is and is not appropriate. At the very least, guidelines should exist which specify that minimum standards of professionalism must be applied to every E-Mail, whether sent internally or externally. Employees should be encouraged to understand that both the content and style of their E-Mails will reflect the perceived professionalism and reputation of both themselves and their employer.[3]



"Be ever mindful, Farson, that not only must justice be done—it must be paid to be done."

4. THE NATURE AND CONSEQUENCES OF LEGAL EXPOSURE

As made out above, the primary purpose of this Briefing Paper is to identify the technical legal sources of Legal Exposure that arise for the corporate entity from the HazardSphere. But what exactly is 'Legal Exposure' in this context? In this Briefing Paper the term 'Legal Exposure' is used to describe a circumstance where a corporate entity or organisation has been placed in the position where another person (be it individual, employee or another organisation) has a legal cause of action against it. Having a 'cause of action' gives an individual a right to commence legal proceedings against another.

3 In Dunn v IBM United Kingdom Ltd [1998], an employment tribunal held that an employer had acted unfairly in dismissing an employee who had misused the employer's computer facilities by downloading pornography from the Internet. The employer failed in defending itself because it had no policy that forbade such activities and the employee had not been told that this type of conduct would lead to his dismissal.

MARSHAL
Secure. Protect. Comply.

Now that we have a simple understanding of the meaning of Legal Exposure, it is suggested it would be useful to briefly examine the consequences of it. At the very least, legal proceedings may be formally threatened but do not result in actual litigation being commenced. However, a very great deal of management time may be taken up and, perhaps, a financial settlement reached. It is often the practice in these more litigious times for the plaintiff (the party commencing civil legal proceedings) to sue straightaway, establish the strength of their case and their resolve, and then see if a settlement can be reached.[4] But the 'bottom line' is this, when a defendant (the party being sued) faces an aggressive and well-motivated plaintiff (as is very often the case if it is an ex-employee suing) with a reasonably well founded case such as those examples described in the remainder of this Briefing Paper, some or all of the following consequences will inevitably ensue:

(i) A significant management overhead arises as managers address the litigation amongst themselves, fact find and then address the matter with their lawyers. In addition, an immediate Opportunity Cost arises – what could these managers be achieving for the business if they were not spending very significant amounts of time responding to the law suit?

(ii) The managers and other staff involved, especially if they are eventually called to give evidence before a Tribunal or Court of Law, will find this experience particularly stressful and unpleasant.

(iii) The managers and other staff involved, especially if they are eventually called to give evidence before a Tribunal or Court of Law, will be anxious that their careers (both in the short and long term) will be adversely affected by the clinical, critical and unsympathetic legal examination of their acts and omissions. Such careers are often negatively affected by litigation.

(iv) In an action founded in Employment Law, a settlement with the plaintiff may be in the tens of thousands of pounds sterling. However, the ex-employer will also have to bear its own legal costs (also in the tens of thousands of pounds sterling), recruit a replacement employee to the plaintiff and train them and, quite possibly, discipline or terminate the employment of other employees who gave rise to the plaintiff's cause of action with all of those attendant costs.[5]

(v) The overhead for dealing with lawyers will be high both in terms of time and financial costs. Simple Employment Law cases might mean costs of tens of thousands of pounds but complex intellectual property cases may cost hundred of thousands of pounds in legal costs.

(vi) In addition to legal costs and depending on the type of action, damages awarded may be between tens of thousands and hundreds upon hundreds of thousand of pounds sterling.

(vii) It is difficult to articulate how desperately difficult (in both a business

---

4 See the £10,000 settlement reached in the Holden Meehan Independent Financial Advisers Limited case below in Section 5.

5 In the Holden Meehan Independent Financial Advisers Limited case below in Section 5. Bradford and Bingley, who acquired them in June 2003, confirmed that the nine persons who harassed the plaintiff were all dismissed.

and an organisational sense) and unpleasant corporations find it when coordinating and cooperating with the local CID or uniformed police force as they investigate the holding of obscene material on that corporation's servers.

(viii) In 'real-life', litigation and criminal investigation have a truly uncanny habit of taking on a life of their own. In factually and technologically complex cases where there is some but not total wrongdoing on the defendant's part; the process can only be managed but cannot be truly controlled.

5. THE EMAIL AS A VEHICLE FOR HARASSMENT AND BULLYING

Any form of sexual or racial harassment, or harassment on grounds that are related to an individual's disability, is capable of amounting to unlawful discrimination for which the employer will be liable. Harassment by E-Mail, for example sexual innuendoes or racially biased jokes sent in an E-Mail, fall squarely into this arena. The key element that dictates whether or not conduct amounts to harassment is whether the victim finds the conduct in question unwelcome. Thus it is irrelevant if another employee considers the same E-Mail to be amusing or otherwise inoffensive; the point is that if an employee finds an E-Mail offensive, and if the material in it is sexual, sexist, racial, racist or disability-related in nature, then it becomes unlawful harassment.

Where harassment is sexual or racial in nature, or is on grounds related to an employee's disability, the victim would be able to take a claim of unlawful discrimination to an employment tribunal under the Sex Discrimination Act 1975, the Race Relations Act 1976 or the Disability Discrimination Act 1995 as appropriate. Courts have held consistently over a period of many years that sexual harassment is capable of causing a detriment to the employee and is thus a form of unlawful discrimination. The same principles apply to racial and disability harassment.

Harassment can take many forms. There is no definition of "Harassment" under English Law but the European Commission's Code of Practice on Measures to Combat Sexual Harassment has defined sexual harassment as 'unwanted conduct of a sexual nature or other conduct based on sex affecting the dignity of women and men at work' . The Code goes on to state that sexual harassment may include physical, verbal or non-verbal conduct and that such conduct will amount to sexual harassment where it is 'unwanted, unreasonable and offensive to the recipient'. There is also a paragraph that states 'it is for each individual to determine what behaviour is acceptable to him or her and what he/she regards as offensive'.

It can be seen from this that the question of whether or not particular conduct constitutes sexual harassment is a subjective one, by this meaning if a particular employee finds a colleague's conduct offensive, and if the conduct is sexual in nature, then it is by definition unlawful sex discrimination. It is irrelevant whether anyone else takes the view that the conduct is not offensive or unreasonable. It follows that anyone dealing with complaints of harassment should not substitute their own personal view of the incident in question for that of the person making the complaint, nor assume that the person is over-reacting.

A similar approach is taken by the Commission for Racial Equality towards racial harassment, and by extension, the courts would interpret harassment on grounds of an employee's disability in the same way.

MARSHAL
Secure. Protect. Comply.

Here is a recent real-life example of sexual harassment by E-Mail occurring in the workplace:[6]

"Gossiping or slating colleagues behind their backs might be a common, if unfortunate, workplace occurrence but doing it on email could have serious repercussions, as one employer found out last week. A woman who discovered nine of her colleagues had circulated offensive emails about her has received £10,000 compensation after settling a sexual harassment case against her former employer.

While working at Holden Meehan Independent Financial Advisers Ltd, the sales support administrator and PA discovered the emails inadvertently after she was given access to a colleague's email folder while he was on extended leave. She made a formal complaint, but felt she was not treated seriously. Eventually she felt she had no option other than to resign.

"I was really shocked and upset when I came across a series of unpleasant emails about me," said the unnamed woman. "When my complaint didn't seem to be taken seriously I lost confidence in my employer and felt I couldn't carry on working for Holden Meehan."

Julie Mellor, chair of the Equal Opportunities Commission, expressed concern that despite a number of high-profile cases in the media, employers are still failing to get to grips with the dangers of email misuse.

"Robinson! You call this an E-Mail Disclaimer! Why, damn it, it's as plain as a pikestaff!!"

"All employers should make their staff aware that sexual harassment can take many forms and can be deeply distressing for the person on the receiving end," said Mellor.

"The fact that comments are made by email doesn't mean they should be treated any less seriously than if they were spoken or written down.""

In another, but less recent, case concerning a black secretary who worked for a firm of city solicitors, the secretary complained of race and sex discrimination on account of an E-Mail sent by one of the firm's principal lawyers to another saying he wanted a "real fit busty blonde" to replace her (the secretary had only recently resigned). The employee was distressed and disturbed by the incident and stated before an employment tribunal that she found "the content and tone of the E-Mail to be both racist and sexist". She won her case.

The Chairman of the Employment Lawyers Association's Working Party on workplace privacy said at the time: "Time and time again employees are putting things in E-Mails they would not dream of writing down. But it is a written record that can come back to haunt them. The danger is getting

6 Reported on 23rd August 2003 in the Register and the Bristol Evening Post.

through to people surprisingly slowly. We are regularly acting in cases where emails have played an important part".[7]

The number of cases where the inappropriate content of e-mails in the workplace that are regularly before Employment Tribunals are legion and go far beyond the scope of this Briefing Paper's ability to enumerate.

However, the following example[8] is typical of the opportunity cost, time and money that is regularly spent by corporations in controlling ex post facto their staff's misuse of their information technology infrastructure:

"Worker sacked over e-mail – An office worker sacked for sending inappropriate e-mails to friends and colleagues has lost his fight to get his job back."

Hilary Miseroy, 40, from, took his former employers Barclaycard to an employment tribunal claiming he was unfairly dismissed in September 2002. He said his dismissal after 15 years working in fraud prevention at the company headquarters in Northampton was too harsh as other workers had been given written warnings.

But after a two-day hearing, the tribunal in Bedford decided the company had acted properly. Barclaycard dismissed Mr Miseroy after a disciplinary hearing following a company investigation last summer. The company found he had made derogatory remarks about co-workers in emails to colleagues. Solicitor Lisa Bryson, for Barclaycard, said the company dismissed Mr Miseroy on the grounds of misconduct after finding he had divulged confidential information to someone who worked at Citibank. However, Mr Miseroy said in the witness box his use of e-mail was "quite modest". He said he did not believe he had divulged confidential information as the person with whom he had corresponded was a former Barclaycard employee and a friend.

Mr Miseroy argued it was common practice for fraud investigators in different institutions to share information. However, tribunal chairman Michael Kay QC said the company's investigation had followed correct procedures and the dismissal had been a "reasonable response".

It seems therefore that the behavioural truth of the matter is this. No matter what "Acceptable Use Policies" are put into place; human behaviour in the modern workplace is such that these incidents will invariably occur, costing employers tens of thousands of pounds in legal and human resource advice costs. How much better it would be to interdict this behaviour – especially as it often leads to other employees being distressed and having legal causes of action against their employers, in addition to the misconduct issue arising in the first place. Commenting on a survey undertaken by the United Kingdom Equal Opportunities Commission in 2005-2006, Caroline Slocock, Chief Executive of the EOC, said:

"While technology has improved our lives and changed the way we work, it has also opened up a new forum for sexual harassment - one that can fall below the radar screen of even the most vigilant employers. Based on complaints to our helpline, we know e-mail can be used for a range of activities, from sending lewd jokes around

7 The bold emphasis has been added by the author.

8 Taking place in March 2003 and reported by the BBC

the office, to more insidious and targeted harassment, including sending e-mails to individuals laden with sexual innuendo…...

In the modern workplace, this is a significant new issue for employers, who have a real interest in protecting their employees - their most valuable asset - from unwelcome harassment. It is important for employers to have clear and well communicated policies regarding the appropriate use of IT, and to take complaints seriously."

The Equal Opportunities Commission report ranked victims of e-mail sexual harassment in the workplace as one of the top five callers in 2005-6. These ranged from complaints about a manager emailing the caller with sexual innuendos, a colleague at the workplace circulating email to all employees that said "All women should shut up!" to bosses sending offensive sexual content, and more. Interestingly, many of the complainants were men, said the report.

In addition to the well-known activities of sexual harassment, the office e-mail has also become a preferred weapon of choice for the office bully. In a survey conducted in 2006[9] it was found that one in six workers in the UK has been bullied via e-mail. The poll showed that e-mail bullying in the workplace is increasing with those in the south west and London suffering most from cyber criticism. Perhaps surprisingly, the higher up the career/office ladder people are, the more likely they are to be targeted by e-bullies. While just 15% of secretaries claim to be the victim of such attacks, 28% of their managers are being harassed via the corporate e-mail inbox. Examples of such bullying range from unfair comments sent by managers keen to avoid face-to-face confrontations to unwelcome personal remarks.

"I was bullied by my boss who would send me insults and belittle me by e-mail…" complained one female administrator from London. "In the end, I resigned."" she added. The Report indicated that the problem is likely to affect productivity – finding that some people find such bullying so distressing they need time off work, although nearly a third confront the bully and 22% talk the problem through with friends or managers.

In Section 8. this Briefing Paper explains how, in Law, employers become directly and legally liable for the behaviour of their employees in the course of their employment.

6. INTERNET ACCESS AS A VEHICLE FOR HARASSMENT

The use by employees of their ability to access the Internet during the course of their employment can lead to actions citing sexual harassment. In one case[10] a female employee was subjected indirectly to sexually explicit material which her male colleagues regularly downloaded from the Internet. Such downloading was not part of their employment but was conducted for their personal 'enjoyment'. She eventually resigned and brought a claim to a Tribunal for unlawful sex discrimination, arguing that the activities in the open-plan office where she had worked amounted to sexual harassment.

---

9 By the Internet business subsidiary of the UK Employment Agency – Reed Employment

10 Morse v Future Reality Ltd [1999]

Despite the fact that the activities that went on were not directed at her personally, and despite the fact she had not previously raised any complaint with management, the employee won her case. The tribunal held that the working environment was uncomfortable for the employee as a woman on account of the sexually explicit material being circulated and that this had caused her a detriment. The employer was held liable because they had taken no action to prevent such activities.

The Employment Equality (Sex Discrimination) Regulations 2005 came into force on 1st October 2005, introducing a number of amendments to existing sex discrimination legislation. One of the most publicised of these was the introduction of a statutory definition of sexual harassment. Before these Regulations, claims for sexual harassment have had to be made under then existing sex discrimination law which outlawed less favourable treatment on the grounds of sex. The new legislation expressly states that sexual harassment is unlawful. The new legislation provides that a person subjects another to harassment if:

(i) on the ground of sex, a person engages in unwanted conduct that has the purpose or effect of violating the other person's dignity or of creating an intimidating, hostile, degrading, humiliating or offensive environment (e.g. an employee regularly downloading pornographic pictures of women onto his computer could have the effect of creating a degrading environment for a woman to work in);

(ii) a person engages in any form of unwanted verbal, non-verbal or physical conduct of a sexual nature that has the purpose or effect of violating the other person's dignity or of creating an intimidating, hostile, degrading, humiliating or offensive environment (e.g. an employee making sexually suggestive comments to another by e-maul would fall within this definition); or

(iii) on the ground of the other person's rejection of or submission to unwanted conduct of the kind set out in (i) or (ii) above, a person treats another less favourably than they would have treated him/her had s/he not rejected, or submitted to, the conduct (e.g. a manager failing to give an employee an opportunity for promotion because she rejected his or her e-mailed sexual advances).

It is important to note, in the context of discussing the misuse of e-mail and Internet access technology in the workplace, that conduct can have the 'effect' of creating an intimidating, hostile, degrading, humiliating or offensive environment even if creating such an environment was not the intention of the person carrying out the conduct complained of. When assessing whether conduct has this effect, a tribunal will consider all the circumstances, including the complainant's perception of the alleged harassment and whether it is reasonable to consider the conduct as being a form of harassment.

7. THE INESCAPABLE EXPOSURE ASSOCIATED WITH DISCRIMINATION

All of the United Kingdom Discrimination Acts[11] contain a provision that ensures that employers are to be held liable for their workers' actions in the course of their employment, whether or not the actions in question were done with the employer's knowledge or approval. This means that the employer cannot escape liability for discrimination by:

11 Sex Discrimination Act 1975, Race Relations Act 1976, Disability Discrimination Act 1995

(i) Pleading ignorance of the fact that harassment was being suffered by an employee;

(ii) Arguing that there was no intent to cause offence - courts and tribunals have consistently held that lack of intent or motive on the part of the person undertaking the harassment will not remove the employer's liability for acts of sexual or racial harassment;

(iii) Blaming the employee for failing to complain formally to management about the alleged harassment.

From the case law on this subject, it is suggested that a regular circumstance, arising from a variety of reasons, is that employees suffering harassment may not come forward to a member of management to complain about the harassment they apprehend. They may feel embarrassed about what is happening to them, fear that they will not be believed or taken seriously, or worry that a complaint will lead to negative repercussions for them in the longer term.

It follows logically, and in any event it is clear from both statute and case law that the responsibility lies squarely with employers to take all reasonable steps to prevent discrimination (including harassment) from occurring.

As a matter of Law, if an employer takes all reasonably practical measures to prevent discrimination (including harassment) from occurring in the workplace, this will provide a statutory defence in the event that they are litigated against following an allegation of harassment. There is, it is suggested, a strong parallel here with health and safety law. Under health and safety law - where an employer can show that they took all steps that were reasonably practicable to prevent injuries or damage to health at work, but an injury nevertheless did occur, the employer may be able to escape liability or, at the very least, significantly mitigate their damage.

A little known legal truth is that the Prevention of an event which would otherwise give rise to a cause of action in Law is far, far better than defending the action later. The new generation of Content Security & Image Interdiction Technology permits, for the first time, the prevention of sexual harassment through digital means.

On this point, the Employment Appeal Tribunal held[12] that an employer who had devised and implemented a policy on racial awareness, had made every employee fully aware of the need to abide by the policy, and had carried out training on racial and sexual awareness, had taken such steps as were reasonably practicable to prevent discrimination from occurring. The Tribunal concluded that the provisions the employer had put in place to ensure racial equality fulfilled the statutory defence and they were therefore not to be held liable for a derogatory and racially discriminatory remark that had been made in the presence of an employee of Iraqi-Arabic ethnic origin.

8. UNDERSTANDING THE EMPLOYER'S LIABILITY FOR THE ACTS AND OMISSIONS OF ITS EMPLOYEES

In broad legal terms, employers are responsible for the actions and omissions of

12 Haringey Council v Al-Azzawi [2002]

their employees in the course of their employment. This is known as the Doctrine of Vicarious Liability. It follows that any misdeeds committed by workers in the course of their employment can lead to legal claims being successfully taken against the employer by the injured party. This area of this Briefing Paper will explore three possible areas of legal liability that could arise in relation to the employers vicarious liability for its employee's misuse of E-Mail at work - namely pornography in the workplace, defamatory statements made in E-Mails and infringement of copyright.

The doctrine of vicarious liability has evolved as part of the common law as a result of court decisions over many years. Under the principles of vicarious liability, any party that suffers a civil wrong[13] as a result of an individual's transgressions or negligence during the course of their employment may sue that individual's employer and seek damages. In theory the employer could then sue the negligent employee, although this rarely happens in practice.

Determining whether an employee's actions or omissions have occurred "in the course of employment" has caused difficulties of interpretation for Courts and Tribunals over the years. Broadly, whenever there is a close connection between the employee's actions and the nature of the employee's job duties, the employer may be held liable. It follows that as a matter of Law, where the employer has provided the employee with a computer and with access to E-Mail, they will be liable for any abuse of the computer system perpetrated by that employee.

In a landmark case in 2006 by the House of Lords [14] (the highest Court of Appeal in the United Kingdom) on the subject of bullying in the workplace; the law changed so as to make employers liable for workplace harassment even if they were not in any way negligent.

The decision was based on anti-stalking legislation which was used by an NHS employee to hold his employer responsible for a superior's treatment of him. The law in question is 1997's Protection from Harassment Act. The Act does not define harassment, which has enabled courts to permit it to mean tabloid newspaper campaigns and the behaviour of animal rights activists. However, in this case the claim of William Majrowski was originally summarily struck out by the Central London County Court by Judge Collins. "He held that the 1997 Act was not designed to create another level of liability in employment law. Employees are already adequately protected by the common law," said this House of Lords judgment. The Court of Appeal overturned that decision.

The House of Lords decided that the Act covers the behaviour of employees at work even when the employer has not caused or failed to prevent the offending behaviour. Those employers now have vicarious liability for the acts of employees. Previously employees had to prove that the employer was negligent in not stopping bullying taking place and that it had caused them psychological damage. The new ruling means that companies can be sued even if the company can not be expected to have known about the bullying.

---

13 Different theories of liability and doctrines of law concerning "civil wrongs", being wrongs perpetrated on one party by another, without a contractual relationship and in the absence of criminal liability, is called The Law of Torts.

14 Majrowski v. Guy's and St. Thomas' NHS Trust [2006] UKHL 34.

There can be no doubt that this decision has serious implications for employers as it gives employees who are bullied or harassed at work a further basis on which to claim compensation from their employers. Moreover, some of the existing limitations and defences will not be available. For example, an employer has a defence under existing discrimination legislation if it can show that it took all reasonably practicable steps to prevent discriminatory harassment occurring – this defence was recently made out where an employer had implemented an effective harassment policy. This would not help an employer facing a claim that it was vicariously liable for an employee's harassment under the Act.

Indeed, it seems that the only avenue forward for employers in avoiding the breadth of this decision is to technologically interdict the harassment so as to stop it reaching the intended target.

Vicarious Liability is the no-fault liability where the Blameless Employer is liable in law for the acts of the Blameworthy Employee. We know ICT is an instrument used to bully and harass in the workplace. The Interdiction of such use is the ONLY defence available in law.

Majrowski worked for Guy's and St Thomas' NHS Trust in London and claimed that his superior, Sandra Freeman, was rude and abusive to him in front of colleagues. Majrowski, who is gay, claimed that the abuse was fuelled by homophobia. Under this new interpretation of the law; it will be necessary to show that an offence under the Act has been committed – this involves showing a course of conduct, defined as conduct on at least two occasions, by an employee amounting to harassment, so a single act will not be sufficient. It is also necessary to show a sufficient connection between the harassment and the employment if the employer is to be vicariously liable. However this is widely construed and any bullying or harassment taking place at work will almost certainly be covered.

In the Court's judgement. Lord Nicholls of Birkenhead spelt out the effect for employers where he said:

"As to the terms of the legislation, by section 3 Parliament created a new cause of action, a new civil wrong. Damages are one of the remedies for this wrong, although they are not the primary remedy. Parliament has spelled out some particular features of this new wrong: anxiety is a head of damage, the limitation period is six years, and so on. These features do not in themselves indicate an intention to exclude vicarious liability. Vicarious liability arises only if the new wrong is committed by an employee in the course of his employment, as already described. The acts of the employee must meet the 'close connection' test. If an employee's acts of harassment meet this test, I am at a loss to see why these particular features of this newly created wrong should be thought to place this wrong in a special category in which an employer is exempt from vicarious liability. It is true that this new wrong usually comprises conduct of an intensely personal character between two individuals. But this feature may also be present with other wrongs which attract vicarious liability, such as assault."

Essentially then, when one employee bullies and harasses another (within the meaning of Protection of Harassment Act 1997) persistently through e-mail in the workplace, then the employer will become automatically liable for the damage caused by the bullying employee (including anxiety, nervous shock, psychiatric and psychological problems, loss of earnings and so on.) The bullied and harassed employee will sue the employer, NOT the bully.

MARSHAL
Secure. Protect. Comply.

9. EMPLOYEES, PORNOGRAPHY AND OBSCENE MATERIAL

One of the most common and difficult problems an employer may face is the discovery that an employee has been using their computer system to access, view, download or transmit pornographic or sexually explicit material. Although the possession or downloading of adult pornography is not a criminal offence under English Law (unless it is obscene or of a paedophilic nature), the transmission or distribution of such material is illegal under the Obscene Publications Act 1959. Thus for example, an employee who transmits a pornographic picture to a colleague within the employing organisation or to someone outside the organisation as an E-Mail attachment is committing a criminal offence.

It should also be borne in mind (as explained above) sexually explicit material[15] enerated, displayed or transmitted by the employer computer system may amount to sexual harassment of an employee who finds the material offensive. It should further be borne in mind that misconduct proceedings and dismissals in respect of the use, handling and dissemination of pornographic images and text are common. Here are two recent examples:

Example #1 – The Finance Services Group "Merrill Lynch" dismiss 13 staff.[16]

Merrill Lynch sacked 13 of the 20 Dublin staff it told to stay away from work as part of an inquiry into the sending of pornographic e-mails. The remaining seven have been given written warnings and returned to work. A spokesman for the multinational financial services group said that "of the 20, 13 have been terminated and seven have received written warnings. The seven can return to work….. All have the right to appeal."

Those told to stay away from work included both male and female staff, according to a source, though the spokesman would not confirm this. The sacking of the 13 staff members for inappropriate use of the company's e-mail system brings to 15 the number of staff sacked in recent times from Merrill Lynch's 600-job operation in Dublin.

According to the source, two members of staff sent a pornographic e-mail to a client of the company and this led to their being sacked. While the company was searching through computers or e-mails at Merrill Lynch in the aftermath of that incident, further instances of inappropriate use of e-mail emerged. This led to 20 staff being told on Monday to stay away from work and another 10 being given written warnings.

Those given written warnings must now do retraining on internet and e-mail use but will not suffer any financial penalty

---

15 The downloading of pornography from the Internet in the workplace by employees seems to be endemic in modern times. Such activity appears to cut across the usual organisational and hierarchical boundaries and the expectations associated with them. See for example, the case of a Personnel Officer working for Hillingdon London Borough being dismissed for downloading pornographic images whilst at work:- Hillingdon London Borough v. Thomas EAT/1317/01/MAA [2002].

16 Reported in the "Irish Times" – 24th June 2006

Example #2 – The Government Agency Driver and Vehicle Licensing Agency ('DVLA') dismissed 14 employees following e-mail pornography causing a deterioration in its IT Infrastructure's performance.[17]

Fourteen staff at the Driver and Vehicle Licensing Agency in Swansea, United Kingdom have been sacked and 101 disciplined after they swapped so many pornographic e-mails that it affected the organisations mainframe computer. The action was taken after a three-month inquiry into the controversy. The 14 employees, including one higher executive officer, were dismissed for sending obscene e-mails to people outside the DVLA. The others, who were given various degrees of reprimand including final warnings, had sent the material to colleagues within the building.

The DVLA, which has 6,000 staff, handles all of the United Kingdom's driver and vehicle records. A spokeswoman said that the pornography had been downloaded from the internet by staff during working hours. The images were then attached to e-mails that were sent around the 20-storey building in Morriston, Swansea.

Trouble began when computers started slowing down because of the size and number of images being sent. Other members of staff, unaware of what was going on, complained that obscene material was being attached to innocent-looking e-mails. Bosses ordered the investigation and the IT department was able to pinpoint the computers involved.

The spokeswoman said that those who sent images to people outside the building risked bringing the DVLA into disrepute. She added: "Following an investigation, DVLA has started dismissal proceedings against 14 members of staff for gross misconduct." The staff concerned were found to have used the agency's electronic systems to send pornographic e-mail attachments out of the agency, in direct contravention of DVLA's code of conduct. She said that tighter controls had been introduced which would monitor all e-mails with images attached.

A woman worker who did not want to be named said: "Boredom is a major problem in this place. The work can be very tedious and people find ways of livening up their days. The early stuff was pretty innocent, a joke really. A very boring document would have a picture of a naked woman attached, for example. I suppose it was bound to get out of hand. The stuff became more outrageous and then some of the men started sending ordinary e-mails to female colleagues and then watching their reaction when they opened the attachment. There are a lot of girls up here and some took it as a laugh, and even got involved themselves, but it only takes a couple of complaints and everyone gets into trouble".

However, offensive and pornographic material can make its way into the workplace as Spam. In this way, unsuspecting employees may be exposed to obscene and pornographic material (sometimes as an isolated case but, more importantly, repetitively) which may cause the employee distress, anxiety and stress.

Undoubtedly, the most important aspect of an employer's duty to its employees which is implied by Law is the duty to take reasonable care to ensure the safety of its employees. There are a number of common law rules which determine the extent of that duty, and in addition there are certain statutory provisions designed to ensure

17 Reported in the "The Times" – 22nd June 2006

the employee's safety which, if broken or not observed by the employer, may lead to an action for damages by an injured employee based on a breach of statutory duties.

Frequently, the two actions are run together, so that an employee may succeed for breach of the common law duty and/or a breach of the statutory duty, though, of course, only one set of damages will be awarded. The purpose of the common law rules is to compensate for injuries incurred as a result of the employers negligence; the object of the Statute will be accident prevention enforced by criminal penalties, but with a potential liability for compensation as well.

But as Goddard L.J. said in Hutchinson v. London and North Eastern Railway Company:

"The real incentive for the observance by employers of their statutory duties … is not their liability to substantial fines, but the possibility of heavy claims for damages."

The duty owed by the employer is in respect of the employee's physical and mental health, including ill-health caused by overwork [18], psychiatric illness,[19] and stress and anxiety caused thereby.[20] But if the employers do not know of the risk, or if, having knowledge, they take such steps as are reasonable in the circumstances to minimise the risk, or provide appropriate health care, no liability arises.[21]

A subject for the most part beyond the scope of this Briefing Paper is the liability of the Corporate Employer itself for the Criminal Acts of its Employees. It is an important, complex and emergent area of modern Criminal Law. However it can be said that as a general principle of Criminal Law a Company can be convicted of any offence provided that the sentence can be in the nature of a fine.

The Company can be held liable by what is known as the doctrine of identification, also know in Criminal Law as the alter ego doctrine. [22] What this means is that in each Company a Court of Law will recognise certain senior individuals as being the Company itself and the acts of these individuals when acting in the company's business are treated as the acts of the Company.

It is suggested that the holding of obscene material or obscene images contrary to the Obscene Publications Act 1959 on an organisation's computer system or the holding of indecent photographs or indecent pseudo-photographs of a child contrary to Section 1 of the Protection of Children Act 1978 on the organisation's computer system may expose the corporation itself (and possibly senior individuals within it) to

---

18 Johnstone v. Bloomsbury Health Authority

19 Frost v. Chief Constable of South Yorkshire Police

20 Walker v. Northumberland County Council

21 Petch v. Customs and Excise Commissioners

22 See generally, C. Wells, "Corporations: Culture, Risk and Criminal Liability" [1993] Crim.L.R. 551. This new form of liability, distinct from vicarious liability, was based on the concept of the company itself being identified with the acts of senior officers, rather than being accountable for the transgressions of employees. See also A. Reed & P. Seago "Criminal Law".

criminal prosecution.[23]

Lord Reid, when giving a legal decision of the House of Lords (the highest Court of Appeal in the United Kingdom) described the identification principle of liability in the following terms:[24]

"A living person has a mind which can have knowledge or intention or be negligent and he has hands to carry out his instructions. A corporation has none of these: it must act through living persons, though not always one or the same person. Then the person who acts is not speaking or acting for the company. He is speaking as the company and his mind which directs his acts is the mind of the company. There is no question of the company being vicariously liable. He is not acting as a servant, representative, agent or delegate. He is the embodiment of the company, one could say, he hears and speaks through the persona of the company, within his appropriate sphere, and his mind is the mind of the company. If it is a guilty mind then that guilt is the guilt of the company."

As indicated above in this Section, the possession or downloading of adult pornography is not a criminal offence. However, it is suggested that the downloading of pornography in the workplace and the downloading of obscene material or paedophilic material in the workplace can be seen, it is argued, as behaviour on the same spectrum of activity – merely existing at very different ends of such a spectrum. In the recent case of an Australian Bank Manager stealing 19 Million Australian Dollars from his employer to feed his Internet Gambling Addiction,[25] there was evidence to show that the nature of the Bank Manager's uncontrollable addiction was fuelled by the unrestrained access he had to his online bookmaker in working hours through his employer's Internet Access System.

There seems prima facie evidence available therefore, which goes to suggest that dysfunctional individuals who express that dysfunction through Internet use, will find a continuance and an exacerbation of their dysfunction by having unrestricted access to the Internet at their workplace. It is suggested that it is unarguable that prudent employer's should interdict such behaviour at it's source since no amount of work-orientated training can restrain an individual from such a behavioural characteristic.

Forwarding Pornographic E-Mails and Attachments

As made out above, one of the most common and difficult problems an employer may face is the discovery that an employee has been using their computer system to access, view, download or transmit pornographic or sexually explicit material.[26]

---

23 Section 160 of The Criminal Justice Act 1988 made the simple possession of indecent photographs of children a criminal offence. Section 3.(1) of the Protection of Children Act 1978 has the capacity to make not only Corporations criminally liable, but also such Corporation's officers and managers personally criminally liable if, through neglect, indecent photographs of children or indecent pseudo-photographs of children are downloaded onto the organisation's computer storage systems.

24 Tesco Supermarkets Limited v. Nattrass [1972] A.C. 153 at 170.

25 Reported in the Asia Pacific News on 29 October 2003

26 The downloading of pornography from the Internet in the workplace by employees

Although the possession or downloading of adult pornography is not a criminal offence under English Law (unless it is obscene or of a paedophilic nature), the transmission or distribution of such material is illegal under the Obscene Publications Act 1959.

Thus for example, an employee who transmits a pornographic picture to a colleague within the employing organisation or to someone outside the organisation as an e-mail attachment is committing a criminal offence.

Vicarious Liability and Grossly Offensive or Obscene E-Mailing

In addition, it is illegal to send indecent or grossly offensive material in order to cause the recipient distress or anxiety under the Malicious Communications Act 1988. [27] A similar offensive exists under the Communications Act 2003 where it is an offence to send over a public electronic communications network a message that is of a "…grossly offensive or of an indecent, obscene or menacing character".[28] After the House of Lords decision in 2006 by the House of Lords[29] with respect to the Prevention of Harassment Act, the likelihood of an employer being vicariously liable for an employee's breach of either the Communications Act 2003 or the Malicious Communications Act 1988 must be very considerably higher.

Indecent E-Mails in the Workplace and the Sex Offenders Register

What damage will be done to an Employer when an Employee's Indecent E-Mails causes them to be entered on the Sex Offenders' Register?

What are the Vicarious Liability Issues here?

Once again – Interdiction is the ONLY realistic answer.

The sending of e-mails of a sexual nature could earn the sender a place on the Sex Offenders' Register under changes to existing legislation that came into force in February 2007. An Order[30] amended the Sexual Offences Act of 2003 to make it possible for offences which are not primarily sexual in nature to be punishable by a Sexual Offences Prevention Order (often referred to as a "SOPO").

---

seems to be endemic in modern times. Such activity appears to cut across the usual organisational and hierarchical boundaries and the expectations associated with them. See for example, the case of a Personnel Officer working for Hillingdon London Borough being dismissed for downloading pornographic images whilst at work:- Hillingdon London Borough v. Thomas EAT/1317/01/MAA [2002].

27 Sections 1(1)(b) Communications Act 2003. See especially the House of Lords decision in DPP v. Collins [2006] UKHL 40.

28 Section 127(1)(a)s 1(1)(b) and 4. Malicious Communications Act 1988. See especially Veronica Connolly v. DPP [2007] EWHC (Hearing Date: 23rd January 2007] who sent photographs of aborted foetuses to pharmacies who stocked the 'morning after' contraceptive.

29 Majrowski v. Guy's and St. Thomas' NHS Trust [2006] UKHL 34.

30 Sexual Offences Act 2003 (Amendment of Schedules 3 and 5) Order 2007 (Statutory Instrument 2007 No.296) coming into force on 19th February 2007. Made by the Secretary of State pursuant to Section 130 Sexual Offences act 2003. The Order does not apply in Scotland.

Improper use of a public communications network is forbidden already by the Communications Act 2003. It defines improper use as sending a message that is "grossly offensive or of an indecent, obscene or menacing character". The amendment to the Sexual Offences Act add that offence to the list of others that qualify for a SOPO and covers such activities as nuisance phone calls, obscene messages and harassment emails of a sexual nature.

Anyone issued with a SOPO is subject to its conditions. A SOPO bans a person from certain behaviour for a fixed period which must be five years or more. People issued with a SOPO are added to the Sex Offenders' Register. The Register is designed to monitor and control the behaviour of, and therefore the risk posed by, sex offenders. The amendments now made are designed to include acts which are not in themselves sexual in nature but which relate to sex offences.

10. DEFAMATION

From the evidence to hand it is suggested that many employees regard E-Mail in much the same way as they would regard an informal telephone conversation. They therefore take a relaxed approach to what they communicate and assume a degree of informality which can lead to legal repercussions. Occasionally, however, this relaxed approach may stray over into E-Mail gossip, and, with human nature being what it is, uncomplimentary or even derogatory statements about another individual or organisation may occasionally be included within the text of an E-Mail, perhaps as part of routine office gossip, or perhaps even as a joke.

"This is treachery—they've stolen our deceptive wording that gets round the Trade Description Act."

An E-Mail is defamatory if it is untrue and is of such a nature that it would tend to lower a person in the estimation of right-thinking members of society generally. It is possible to defame a corporation as well as an individual. Statements that are true cannot lead to successful claims for defamation. Nevertheless, it is suggested that is not in the employer's interests to allow employees to write derogatory statements about others in E-Mails, whether true or untrue.

The Law of Defamation does not distinguish between text written in an E-Mail and text contained in a written letter, journal or newspaper. If the text of an E-Mail contains material about an individual, or another organisation, that is defamatory, then both the employee who sent the message and their employer may be sued by the injured party for substantial sums of money. Realistically, it is much more likely that an individual whose reputation has been tarnished by the content of an E-Mail would sue the employer rather than the employee who is the author of the offending message. Clearly an employer is more likely than an individual employee to be in a financial position to pay any damages that a court may award.

MARSHAL
Secure. Protect. Comply.

The employer will be potentially vicariously liable for any defamatory statements made in their employees' E-Mails when sent from the employee's workplace computer system (and not from their home computer except where that home computer is provided for use in the course of their employment). This is because the employer may be regarded in law as either the author or the publisher of the E-Mail, and the Defamation Act 1996 states that:

"Employees or agents of an author, editor or publisher are in the same position as their employer or principal to the extent that they are responsible for the content of the statement or the decision to publish it."

One of the most high-profile defamation cases in the employment arena came before the courts in 1997 when the company Western Provident Association sued one of their competitors, Norwich Union, on account of the content of an E-Mail that had been widely circulated amongst staff at Norwich Union.

The E-Mail contained untrue statements about Western Provident, alleging they were in financial difficulties and under investigation by the DTI. The outcome for Norwich Union was a £450,000 bill for damages. Another important element in this case was that the court ordered Norwich Union to preserve and hand over all the offending E-Mails in the normal litigation procedure known as "discovery".[31]

11. INFRINGEMENT OF COPYRIGHT

Whenever employees have access to E-Mail and in particular, the Internet, a risk will arise that the employee will infringe a third party's Copyright whether deliberately or unintentionally. Activities that could give rise to a infringement of copyright include (for example):

(i) Unauthorised use of material that has been downloaded from the Internet;

(ii) Downloading music and video files;

(iii) Copying a document or computer program downloaded from the Internet for a colleague's use;

(iv) The display of a third party screen-saver in a public office;

(v) Forwarding copyright material (documents, pictures, photographs, drawings, music, sound recordings, films) to colleagues or persons outside the organisation as an E-Mail attachment;

(vi) Transferring copyright-protected material from one computer to another (for example an employee may load copyrighted material that they have obtained elsewhere on to their workplace computer);

(vii) The use of pirated software at work.

The Copyright, Designs and Patents Act 1988 states that material can be copied only

31 The Courts of Law are now well versed in considering the defamatory content of e-mails. See, merely as an example, the Court of Appeal (Civil Division) in Spencer v. Sillitoe [2003] EMLR 207.

with the permission of its owner. Copyright automatically accrues to the author of the material without the need for it to be registered. Copyright then lasts for the lifetime of the owner plus 70 years without any requirement for renewal.

The Copyright, Designs and Patents Act applies to material communicated by E-Mail in the same way as it applies to printed material. It protects the owner of material published on the Internet, including documents, web-pages, graphics, screen-savers, computer games, video, sound files and software. Thus, an employee who transmits such material as an E-Mail attachment may be infringing the copyright of the owner which is not only a civil wrong but a criminal offence.

The fact that material is readily available on the Internet, or has been published in a book or newspaper, does not prevent it from being a copyright work and protected. Thus, even though material may be freely available on the Internet to read or download, this does not necessarily mean that it can be copied or distributed to others, unless permission from the owner is first obtained.

As in other areas of law, employers can be held vicariously liable for infringement of copyright on account of the transgressions of one of their employees in the course of employment. It will not be a defence against liability to argue ignorance of the infringement. The employer is the party that is responsible for taking preventative measures to ensure that none of their employees commits an infringement in the course of their employment.

12. BREACH OF CONFIDENCE

Organisations need to bear in mind that the HazardSphere that they occupy contains a network of confidences and secrets. The organisation as an employer will owe obligations of confidentiality to its employees as a matter of Employment Law and Data Protection Law. The organisation may also hold personal data on third parties to whom it also owes obligations under the Data Protection Act.

As a trading organisation, and not as an employer, the organisation is likely to owe obligations of confidentiality that it has assumed by virtue of its Contracts with others. Indeed those contracts may very well contain express and complex obligations of confidentiality the breach of which may not be subject to the limitation of liability mechanisms usually and commonly expressed in modern contracts.

Employees have the capacity to disseminate such information and place the employer in Breach of Confidence with a third party. Such dissemination may take place intentionally or unintentionally.

An example of threatened intentional disclosure concerned an employee of the Inland Revenue.[32] The Employee in question was employed as a tax valuation officer by the Inland Revenue. His employers discovered that he had written a letter to a right-wing group, the National Socialist Alliance, offering to supply sensitive data from the Revenue's computer that would be of assistance to the NSA. That discovery led to the employee's dismissal for misconduct on the grounds of threatened disclosure of confidential information from records held on the employers' computer. The Revenue's rules on confidentiality provided that information acquired by employees

32 Winder v The Commissioners of Inland Revenue – Ashford employment tribunal (20.4.98, Case No. 1101770/97)

in the course of their work must not be misused or discussed outside the Revenue. A tribunal dismissed the employee's claim of unfair dismissal. Although he had not actually disclosed confidential information to the NSA, the employers were entitled to conclude that an offer to use computer facilities to acquire such information was a breach of the duty to maintain confidence. The employee's intention to disclose protected information at the time of writing the letter was clear and unambiguous.

A recent example of a serious but unintentional disclosure of highly sensitive and confidential information (but taking place outside of the United Kingdom) was reported in October 2003. The Psychiatric Hospital of Århus forwarded a non-encrypted email containing sensitive information about a patient to the private email address of a specialist employed at the hospital. Because of an IT virus, and it is suggested, the negligence of an employee, the email was forwarded to a number of other email addresses. The Psychiatric Hospital of Århus entered into a number of difficult and sensitive negotiations with the patient, the patient's family, the Hospital Trustees and the Danish Data Protection Registrar.

13. CORPORATE LEGAL EXPOSURE IN RESPECT OF BLOGGING, WEB 2.0 AND USER-GENERATED CONTENT

Corporate Blogging can, in one generalised activity, generate Legal Exposure for the unwary Corporation across a number of Legal Theories of Liability. Consequently, Content Security Technology must be an essential component in every Corporation's Blogging strategy.

13.1 Corporate Blogging: An Introduction

Many major companies have seized the opportunities presented by blogging. They have recognised the benefits which internal blogs bring to communication and culture across a corporation, or in the case of external corporate blogs, the scope for improved marketing, branding and PR. High profile users of corporate blogs include: General Electric, McDonald's, PwC and Time Warner. In Sun Microsystems, the CEO and the General Counsel are among the company's 2,000 bloggers. IBM has even more.

Corporate blogs can be an effective means of providing commentary or news on a company and its products. The instantaneous nature of blogging can allow companies to react quickly to breaking news stories, helping them to manage publicity, both good and bad. Blogging is also seen as a way of humanising a company, allowing the personality of employees to emerge in an informal setting.

The best-known example of how a blog can improve a company's image is Robert Scoble's Scobleizer blog, begun when Scoble was an employee of Microsoft. He is credited with changing the public view of Microsoft by his blogging on life and events inside and outside Microsoft, becoming its unofficial corporate voice. Scobleizer is widely seen as helping to humanise Microsoft and shift its stance from arrogant and aloof to one which is more inclusive and accepting of criticism. One of the keys to achieving this softer image was Scoble's neutrality and readiness to point out Microsoft's mistakes, as well as praise for its rivals. (Scoble has since left Microsoft for a start-up, but continues Scobleizer).

In contrast, a blog created by Vichy, a division of cosmetics giant L'Oreal, initially backfired. The blog was part of a marketing campaign for a new anti-ageing product.

It was based on the diaries of a flawless-looking character called Clare who lamented the onset of age. Clare's youthful looks turned out to be too good to be true: Clare was a character invented by the advertising agency. Vichy narrowly escaped a PR disaster by admitting its mistake, apologising and introducing the real Vichy team. Customers were invited to post unedited comments about their experiences of the Vichy product on the blog.

These two examples demonstrate one of the keys to successful corporate blogging: authenticity. The blog posts must be genuine – a key part of blogging's success has been the fact that people believe it side-steps the "spin" that permeates marketing material, or the reporting of news. The authors must also be allowed at least a degree of autonomy in generating and selecting content. However, in fostering authenticity in a blog companies undoubtedly introduce risks to the process.

13.2 Risks of Corporate Blogging

The main risks of external corporate blogging (some of which will be common to internal blogging) are:

(i) Damage to an Individual's or Company's Reputation

This typically arises if a blogger says something which tarnishes the reputation of the company in the eyes of the reader. It could be an inappropriate comment, or it could be that they criticise the company directly.

(ii) Liability for Infringement of Intellectual Property Rights

The biggest risk here is that the blogger copies content for the blog post from another source without permission. It could be that they copy the text of an article, or include a photograph or logo belonging to another party.

(iii) Liability for Defamation or Illegal Content

Defamation is perhaps one of the greatest risks to corporate blogs – especially if authors are given a free reign. It is probably natural that employees would want to put down the competition, and fair comparisons are fine. The risk arises when authors cross the line, and opinion becomes defamation.

(iv) Leaking Confidential Information

Internal losses are as much of a concern as external liability. Not all employees will realise what is and is not appropriate to disclose – meaning that confidential information can easily leak out of the business. This could be details of a new product launch, or disclosure of poor financial figures. Commercial damage and breach of insider trading rules are just two of the risks.

(v) Harassment

Employers have a duty to protect all of their employees, so it is important that blogs are not used as a way of harassing others. The employer could become liable for allowing one employee's blogging to amount to harassment of another.

(vi) Failing to Recognise a Statutory Grievance

A statutory grievance is any complaint which is capable of forming a claim before an employment tribunal, discussed further below.

Liability may arise from content posted by the company's employees or, where a site is more widely accessible, from comments posted by members of the public using the website. A company's risks and exposure to liability will depend on the type of blog which the company operates and the capacity in which its employees are posting to that blog. A company may set up a blog as a marketing tool, under which employees post material during the course of their employment, in their capacity as employees of the company and on behalf of the company. In this case the company and the employee will be treated as one and the same and the company will be responsible for the statements made by the employee as if they had been made by the company itself. This is vicarious liability (as explained above) and it makes the employer liable for the actions of its employees made in the course of their employment.

Some companies provide employees with the ability to create individual blogs, without them being specifically tied to a particular product or marketing campaign. IBM, for example, has over 3,000 employees who blog. Many of them use their blogs to explain a technology they are working on or to discuss issues faced by the business. Others simply use their blogs to comment on the state of the industry, or to discuss day-to-day aspects of their jobs. These type of blogs aren't typically used by the company to promote any particular products. However, like the Scobleizer blog, they can help generally improve the image of the company.

In these situations, even though the employee is not writing "on behalf of the company", the fact that the blog is hosted or funded by the company may still make it liable for the content of the posts. Of course, this raises some difficult practical issues: no company has the resource to supervise 3,000 blogs.

It is possible that an employee could make what is known as a statutory grievance whilst blogging which would require the employer to follow the statutory grievance procedure. This is most likely on an internal blog – i.e. one used and read only by staff. A statutory grievance is any complaint which is capable of forming a claim before an employment tribunal when it has been put in writing and sent to the employer. This definition of a statutory grievance was drafted very widely in the legislation and has been interpreted very widely by employment tribunals largely on policy grounds as an individual can be barred from bringing a claim if they have not first raised a grievance internally.

Arguably if an employee posts a complaint on an internal corporate blog which relates to an unlawful act, such as discrimination or bullying, then this could amount to a statutory grievance, which has been sent to the employer when posted on the blog. The employer would then be required by law to invite the employee to a meeting to discuss the grievance, within a reasonable time. Following the meeting the employer is obliged to write to the employee communicating the outcome of the meeting or any decision reached. The employee must also be offered an appeal against any decision. The employee is entitled to be accompanied to both the grievance meeting and the appeal by a trade union representative or a workplace colleague.

If the employer misses the very existence of the statutory grievance, because it does not monitor the content of the blog and an employee subsequently took a case to an employment tribunal and was successful the tribunal must award an uplift in

damages of between 10% and 50% for the employer's failure to follow the statutory procedure.

14. EMPLOYEES AND PERSONAL BLOGGING

When an employee maintains a personal blog, the employer is unlikely to incur liability for its content unless there is some connection between the personal blog and the blogger's work. The boundary is sometimes unclear and will be determined by the particular facts in each case. There may be occasions when the employee is using his or her personal blog in a way which could be said to bring the company into disrepute even though they use it outside of working hours. An employer may wish to use disciplinary sanctions against the employee in these circumstances. The extent to which this is possible will also turn on the particular facts.

Waterstone's employee Joe Gordon was dismissed in 2005 because he made critical remarks about his boss and the bookseller on his personal blog, called the 'Woolamaloo Gazette'. He referred to Waterstone's as 'Bastardstone's' and to a character called 'Evil Boss' whom he compared to the Pointy-Haired Boss in Scott Adams' Dilbert cartoons. An inquiry led to a disciplinary hearing and he was sacked for gross misconduct. The company argued that he brought it into disrepute. With the help of a trades union representative from the Retail Book Association, Gordon successfully appealed against the dismissal and was offered reinstatement.

In France, an English secretary brought a case under French labour law after being sacked for allegedly bringing her employers, British accountancy firm Dixon Wilson into disrepute by writing a "Bridget Jones in Paris" blog describing her everyday life living and working in Paris. Writing under the pseudonym "La Petite Anglaise" the secretary kept an online diary about everyday events in her work and personal life which built up quite a following amongst the public. When speaking about work the secretary described a quintessential English office atmosphere complete with a senior partner who is 'very old school' prone to donning braces and sock suspenders. The secretary maintains that stories such as the 'unwritten rule' of never pulling a cracker at the Christmas party before the senior partner or his wife have pulled theirs were harmless anecdotes. Dixon Wilson did not agree and dismissed her even though she never once identified her own name or the identity of her employers. She did however publish photographs of herself on the blog which the company maintain could be sufficient to identify her employers.

Initially Dixon Wilson tried to rely on gross misconduct as the grounds for dismissal but later dropped this justification and alleged a 'loss of confidence' and 'dismissal with real and serious cause' maintaining that the blog 'brought the firm into disrepute'.

She won her unfair dismissal claim in a case that tested the boundaries between freedom of speech and the duty of loyalty which is included in most employment contracts in France. A similar duty of trust and confidence is implied into every employment contract formed in the UK. The secretary maintained that Dixon Wilson's internal policy regarding personal use of email and internet was not watertight and was prepared to fight her case on principle. She used the same blog which lost her her job to inform the public of the progress of her case.

Increasing numbers of people have personal blogs. Some may think that they can say what they like when they are blogging on their own time; but that is not always

the case. As a general rule, conduct committed outside employment can potentially justify disciplinary action depending on the conduct, the nature of the employee's job and the potential damage to the employer's reputation. Many factors will be relevant, including the terms of an employee's contract and any applicable policy. In order to rely on an applicable policy an employer must ensure that there are appropriate procedures in place to ensure that all staff are aware of the policy and understand it otherwise the policy may provide little protection for the company seeking to rely on it.

More than a third of employees who keep personal blogs are posting information about their employer, workplace or colleagues and risk dismissal, according to new research.[33]

Human resources firm Croner commissioned YouGov to ask employees if they kept a personal blog and, if so, what information they post. Of those who keep a blog, 39% admitted that they had posted details which could be potentially sensitive or damaging about their place of work, employer or a colleague.

Gillian Dowling, technical consultant at Croner, said that the problem is similar to that of the early days of email use. "In the 1990s when emails were introduced as a new means of communication employees were lulled into a false sense of security by the informality that this type of communication brings," she said. "Many recipients received rude, angry or otherwise inflammatory emails which had been written and sent in the heat of the moment," she continued. "Back then it was common to train staff on the use of emails which included advising employees not to send inappropriately worded emails in haste. Employees were advised that the use of emails was the equivalent of sending or dictating a letter, and just as binding. These concepts remain in email or internet policies today," she said.

"With blogging, the employee, sitting in front of his computer screen, experiences the same lack of embarrassment as there is no face-to-face contact. An employee can be lulled into a false sense of security and sound off about his bad day at work on a blog without fully considering the impact such a posting may have."

"If there is a negative impact on the organisation's corporate image which is so serious that it breaches the implied term of mutual trust and confidence, the employee could be dismissed for gross misconduct," she added. "The blog could also be evidence of other conduct issues or reveal workplace discrimination or bullying. Confidential secrets could be disclosed including financial information or new product development, or whistle blowing all of which could have a negative impact on the business. Employers need to ensure that they carefully consider the impact of blogging on their organisation and take appropriate steps to minimise any potential risk," said Dowling.

Industry Survey on Web 2.0 security[34]

For the most part, the survey focused on Web 2.0 social media sites -- blogs, forums, Web mail, instant messaging, social networking sites, podcasts, online video sites, wikis, photo sharing sites and Second Life -- and employee's use of them during in

33 Reported in May 2007

34 Reported by Clearswift in May 2007

the work environment. More specifically, Clearswift's research, which was conducted online earlier this year with total sample size of 939 adults, found that:

34 percent of organizations don't monitor employees' use of the Internet.

51 percent of businesses don't know whether they've lost confidential information via social media outlets.

20 percent of IT and business decision-makers don't have a policy governing appropriate use of the internet, including social media sites.

20 percent of organizations do not allow blogging at work while 45 percent don't have a policy on it.

39 percent of IT and business decision-makers consider social media to be relevant to today's corporate environment, while 36 percent do not see social media as relevant to their businesses.

13 percent of organizations are not aware of social media and have no policy on it.

While most organizations do understand that 71 percent of their staff use Web mail, 62 percent use forums, and 56 percent use blogs, 36 percent of those surveyed do not see them as relevant to their business and have no plans on using them in the future.

While more than 73 percent of those surveyed felt that loss of confidential data was the number one security issue in terms of priority to the security of their organization, 51 percent are not aware if their company has ever lost confidential information through social media sites. The only security issue to rank higher than loss of confidential data was viruses/worms (77 percent), yet 96 percent of companies are already using anti-virus tools.

In addition to virus, worms, and losing confidential data, other security issues that survey responders consider "high importance" are spyware (54 percent) and pornography in the workplace (54 percent). At the bottom of the list of security issues in terms of priority were those related to social media, including security breaches via blogs and security breaches via forums, which were tied for last, edging out "employee time wasting" and security breaches via instant messaging, and security breaches via Web mail.

15. DIRECTORS, SHAREHOLDERS AND CONTENT SECURITY – BREAKING AND FUTURE RESEARCH

Officers already owe a network of Common Law obligations to Shareholders and other Stakeholders. Their ability to technologically protect the Company's goodwill and Reputation is already is part of this.

The new Companies Act 2006 places more obligations on Officers to protect their Shareholders interests through digital means.

The rules governing the duties directors owe their companies have been codified in the Companies Act 2006 (the Act), which will come into force by October 2008. The Act also introduces a new statutory right for shareholders to sue directors in the company's name in some circumstances (known as the 'derivative action'). At present,

the rules governing directors come from several sources. The general duties they owe their company are governed by the common law and have been developed over many years in case law. The Companies Act 1985 (in particular, Part X) sets out additional rules. There are also other statutes that govern directors' behaviour in specific circumstances (such as health and safety). The Act now sets out a new statutory statement of directors' duties – described as their 'general duties' – in place of the common law and replaces (and to some extent rewrites) Part X Companies Act 1985.

Although the statement of general duties has been described by the government as a codification, it is not exactly the same as the existing law. The explanatory notes published with the original version of the Act describe two deliberate changes to the rules on directors' conflicts (both are described in more detail below). However, much of the language in which the general duties are framed is different from the language used by the common law and may lead to differences in approach when the new rules are applied in practice.

There are seven general duties in the new statutory statement as follows:

(i) A duty to act in accordance with the company's constitution, and to use powers only for the purposes for which they were conferred. This replaces existing, similar duties.

(ii) A duty to promote the success of the company for the benefit of its members. This replaces the common law duty to act in good faith in the company's interests.

(iii) A duty to exercise independent judgment. There is no exactly equivalent duty at common law. However, directors are currently under an obligation not to fetter their discretion to act or to take decisions – this aspect of the general duty replaces this obligation.

(iv) A duty to exercise reasonable care, skill and diligence. This replaces the existing duty of care and skill.

(v) A duty to avoid conflicts of interest (except where they arise out of a proposed transaction or arrangement with the company – see below). At present, if a director allows his personal interests, or his duties to another person, to conflict with his duty to the company then, unless shareholders consent to the conflict: (i) the company can avoid any relevant contract and (ii) he must account to the company for any 'secret profit' he has made out of the arrangement. The new duty replaces this old rule.

(vi) A duty not to accept benefits from third parties. There is no express duty to this effect at common law. It appears to derive from the current duties to act in the company's interests and the rule dealing with conflicts of interest.

(vii) A duty to declare to the company's other directors any interest a director has in a proposed transaction or arrangement with the company. At present, a conflict of interest arising out of a transaction or arrangement with the company is dealt with by the general rule on conflicts of interest, described above. In future, such a conflict will be covered by this new duty of disclosure.

One of the most significant differences between the current regime and the new provisions is in the treatment of the directors' duty of loyalty to their company. The common law requires directors to act in good faith, in the interests of their company.

MARSHAL
Secure. Protect. Comply.

The new provisions oblige a director to "act in the way he considers, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole".

This new formulation raises many questions, especially in the area of Director's obligation to introduce technology-based methods of satisfying obligations (ii) and (iv) above, few of which have been answered by the government. In particular, it is not clear whether 'the company' will continue to have interests as an entity separate from its members or whether the interests of present members will always be paramount. Government spokesmen in the Lords and the Commons have referred to the directors' obligation under the new provisions as being to promote the success of the company for the benefit of members as a collective body. Lord Goldsmith (the government's spokesman on this part of the Act) also said that 'success', for a commercial company, will usually mean 'long term increase in value'. It is not clear how far it will be possible to rely on existing case law in interpreting these provisions. The Act provides that regard is to be had to the current common law rules in interpreting the new provisions: it may be that, although the new duty of loyalty is framed in very different terms from the current law, the courts will nonetheless apply it in a similar way.

In deciding how to promote the success of the company, the directors are required to have regard 'amongst other matters' to:

- the likely long term consequences of their decisions;
- the interests of the company's employees;
- the need to foster the company's business relationships with suppliers, customers and others;
- the impact of the company's operations on the community and the environment;
- the desirability of maintaining a reputation for high standards of business conduct; and
- the need to act fairly as between members of the company.

The introduction of this list has caused some concern. However, it seems that although all the listed factors must be considered, in many cases it will be enough for the board briefly to conclude that a particular factor is not relevant, and move on. Helpfully, the government has made clear that the new provision is not intended to impose additional bureaucratic burdens on companies, and is intended to reflect what is already widely regarded as good practice. Most companies are unlikely to need to make significant changes to present procedures in relation to directors' decision making, provided that they do the following.

Fears have been expressed that the new requirement for directors to exercise 'independent judgment' may prevent individual directors – particularly, non-executives – from relying on the judgment of others in areas in which they are not expert. The government confirmed in debate that directors will continue to be able to do this – and to delegate matters to committees – provided they exercise their own judgment in deciding whether to follow particular advice or to accept someone else's judgment on a matter.

Will the new Shareholder's Right to Sue include a new specie of lawsuit based on Directors filing to avoid a Loss of Reputation when a scandal or employment problem could have been avoided by the use of Content Security or Image Interdiction Technologies?

Prudent Officers must consider Information Security in the context of the new Act.

The Act introduces a new statutory right for shareholders to sue directors, in the company's name, to recover on its behalf loss it has suffered as a result of the directors' negligence, default, breach of duty or breach of trust. At present, shareholders have only very limited common law rights, subject to the fulfilment of strict conditions, to bring actions in their company's name. Under the new provisions, shareholders will be able to bring proceedings in the company's name against the directors in a wider range of circumstances than at present. They will also be able to claim against third parties implicated in any breach (again, in the company's name).

The new statutory right – or 'derivative action' – will undoubtedly make it easier for shareholders to take directors to court. Considerable concern has been expressed that this, taken together with the statutory statement of duties – particularly the detailed list of factors to which directors are to have regard – will lead to significant risks for directors.

The government has made some effort to respond to these concerns, by introducing a two stage process for derivative claims. First, a disgruntled shareholder will have to apply to the court for permission to make the claim – if the court considers that the evidence filed by the applicant does not make out a prima facie case, it will be required to dismiss the application ex parte at this stage. If an application survives this process, it will enter the second stage, during which the court will decide, based on the evidence of both sides, whether the claim should be allowed to proceed. At this stage a range of factors will be taken into account – including the views of independent shareholders with no personal interest in the matter. Companies may find it helpful to approach institutional shareholders for support. Only if the claimant is successful will the claim progress to the third stage – a full trial of the issues.

These changes – when looked at against the background of the courts' significantly increased powers of proactive case management, and the obligation on parties in dispute to litigate as a last resort – go some way to improving the likely position of companies and their boards. They should also reduce the risk that the new provisions will lead to a significant increase in time consuming and expensive litigation in relation to claims against directors that are ultimately unsuccessful.

Boards that take the steps we have outlined here should be able to minimise these risks still further. However, there is still a risk that activist shareholders and pressure groups will seek to use the new procedures at least to create publicity and put decisions of public company boards under even greater scrutiny. Directors may want to have in place a response plan if action is threatened.

MARSHAL
Secure. Protect. Comply.

Marshal's Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email: emea.sales@marshal.com

Americas
Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404-564-5800
Fax: +1 404-564-5801

Email: americas.sales@marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com

info@marshal.com | www.marshal.com