A Perspective Of The Legal Exposure That Arises For Companies When Employees Misuse The Workplace Internet And E-Mail Systems (UK Law)

1. INTRODUCTION

It is a commercial necessity in the 21st Century for every organisation to give its employees access to e-mail and the Internet for use in the course of their employment. It is now a given fact that some employees will abuse that access – and use the technology not only to harass each other and the employees of third parties, but to discriminate against each other and introduce material (some illegal) into the workplace causing it to become hostile.

This perspective seeks to introduce, at the very highest level and in the most general of terms, some of the key legal structures which expose the corporation when its employees misuse the workplace Internet & E-Mail Systems.

2. SUMMARY

2.1 Corporate Liability for Employee Misuse of Employer IT Infrastructure

- Companies are being sued by Employees who have been ***sexually harassed or bullied*** both through exposure to IIM[1], and in respect of co-workers misusing corporate E-Mail[2] and Internet Access facilities in the workplace.
- Companies can avail themselves of ***statutory defences*** when sued by an Employee who have been sexually or racially harassed through the use of IIM in the workplace by taking ***all reasonably practical measures*** to avoid the act complained of. Content Filtering and Image Interdiction Technologies are a reasonably practical measure.
- Companies are ***Vicariously Liable*** to an Employee who has been Harassed by another Employee.
- Companies are ***Vicariously Liable*** to a Third Party for an Employee holding of Paedophilic Pornography on the Employer's IT Infrastructure.
- A Companies' ***only*** defence where is it Vicariously Liable for an Employee's misdeeds is ***Interdiction*** (preventing the harassment via the e-mailing in the first place).
- Companies are being sued by Employees who have been exposed to ***Pornographic Internet Content*** being accessed by their co-workers.
- Companies' highly valuable ***Intellectual Property and Confidential Information*** are being released through E-Mail Use Errors (often placing them in ***Breach of Contract*** with their Trading Partners).
- Companies have found themselves liable for hundreds of thousands of pounds worth of damages when their Employees ***libel a competitor via E-Mail***.
- Credibility in the market-place is being ***seriously lost*** when it becomes public that Employees engage in Inappropriate Internet Use which involve IIM.
- Companies may suffer ***Criminal Prosecution*** when employees disseminate Pornography using the employer IT infrastructure
- Companies may suffer ***Criminal Prosecution*** if they neglect to prevent Employees from downloading Child Pornography into the workplace from the Internet using the employer IT infrastructure.

2.2 Personal Liability for Employee Misuse

- Individual Executives may ***personally*** suffer ***Criminal Prosecution*** if they neglect to prevent Employees from downloading Child Pornography into the workplace from the Internet using the employer IT infrastructure.

1 IIM means "Inappropriate Image Material". This ranges from soft pornography to hard pornography and on to extreme pornographic images, indecent photographs and indecent pseudo-photographs of children.

2 This Paper treats all form of Instant Messaging, Web Mail and E-Mail as being "E-Mail".

3. SOME LAW

3.1 IIM and E-Mails as a Vehicle for Harassment

What Amounts to Harassment?

Any form of sexual harassment is capable of amounting to unlawful discrimination for which the employer will be liable. Harassment by E-Mail text, E-Mails containing Explicit Images or the showing of Explicit Images, for example sexual images 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 content or image to be amusing or otherwise inoffensive; the point is that if an employee finds the content or image offensive, and if the material in it is sexual, then it becomes unlawful harassment.

Where harassment is sexual in nature, the victim would be able to take a claim of unlawful discrimination to an employment tribunal and these Courts have taken the view consistently over a period of many years that sexual harassment is capable of causing a injury to the employee and is thus a form of unlawful discrimination. The same principles apply to racial and disability harassment.

What is the definition of Sexual Harassment?

The legislation expressly states that sexual harassment is unlawful and 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.

For example – 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.

For example – an employee sending pornographic images to another by e-mail would fall within this definition.

(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.

For example – a manager failing to give an employee an opportunity for promotion because they complained of his lewd e-mail which contained Explicit Images.

A little known legal truth is that the ***Prevention*** of an event which *would* otherwise give rise to a legal right to sue is far, far better than defending the action later.

The new generation of E-Mail Content and Image Interception Technologies permit, for the first time, the prevention of sexual harassment through digital means.

What if Sexual Harassment wasn't intended?

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. When assessing whether the 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.

It can be seen from this that the question of whether or not particular behaviour when using ICT constitutes sexual harassment is

a subjective one. This means 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 thinks that the conduct is not offensive or unreasonable.

The Truth of Employee Behaviour

From recent case law and studying the misuse of ICT at work, it seems therefore that the truth of the matter is this. No matter what "Acceptable Use Policies" are put into place; human behaviour in the modern workplace means that these incidents will invariably occur, costing employers tens of thousands of pounds in legal costs and human resource time. How much better it would be to intercept this behaviour – especially as it often leads to other employees being distressed and being able to sue their employers.

How can Internet Access Amount to Harassment?

Uncontrolled Internet access routinely leads employees into misbehaviour which is, in legal terms, ***sexual harassment***. For example, in one case that went to Court a female employee, who worked in an open-plan office, saw sexually explicit material which her male colleagues regularly downloaded from the Internet and displayed on their workstation monitors. This downloading was not part of their employment but was conducted for their personal 'enjoyment'. She resigned and sued her employer for sex discrimination and sexual harassment.

Even though the activities she complained of were not directed at her personally, and despite the fact she had not previously raised any complaint with management, she won her case. The Court said that the working environment was hostile to her as a woman due to the sexually explicit material being circulated. In this real-life situation, if the employer had implemented a modern Content Security System the pornography may have been blocked – a valuable employee kept who was never exposed to the pornography, and training initiated for those trying to download. Even if the porn filter had let the images through – the employer may very well have had a ***total legal defence***. That is that they had taken all reasonable and practical measures to prevent the harassment.

*A little known legal truth is that the **Prevention** of an event which would otherwise give rise to a legal right to sue is far, far better than defending the action later.*

How is the Employer to Blame for this type of Employee Behaviour?

All of the UK Law dealing with discrimination contain makes employers legally 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 by:

- pleading ignorance of the fact that harassment was being suffered by an employee;
- arguing that there was no intent to cause offence to the person affected;
- blaming the employee for failing to complain formally to management about the alleged harassment.

Often the employees who is suffering the harassment may not come forward to a member of management to complain. Where unacceptable e-mail content or images are concerned they often feel particularly embarrassed about what is happening to them, fear that they will not be believed or taken seriously, or worry that a complaint will just cause problems for themselves.

How does the Employer defend itself?

The Law says that the responsibility lies squarely with employers to take all reasonable steps to prevent discrimination (including harassment) from occurring.

To use the Statutory Defence against a case where the Employer is being sued for harassment and discrimination, the Employer must show they have taken ***all reasonably practical measures*** to prevent it.

E-Mail Content Scanning and Image Scanning Technologies are the newest reasonably practical measures which MUST be taken. Without them – use of the Statutory Defence is more likely to fail completely.

So legally, if an employer takes all ***reasonably practical measures*** to prevent discrimination (including harassment) from occurring in the workplace, this will provide what is called a **Statutory Defence** in the event that they are sued following an allegation of harassment.

Employers escaping legal liability can be seen to work completely in real life.

In one piece of litigation, the Court decided a case where one of the employees had made racially discriminatory remarks in the presence of another employee who was of Iraqi-Arabic ethnic origin. However, the employer involved 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.

*If an employer takes all **reasonably practical measures** to prevent discrimination (including harassment) from occurring in the workplace, this will provide what is called a **Statutory Defence** in the event that they are sued following an allegation of harassment.*

Because of this action, the Court decided that the employer had taken such steps as were reasonably practicable to prevent discrimination from occurring. The Court concluded that the provisions the employer had put in place to ensure racial equality fulfilled the statutory defence and they were therefore not liable at all.

How can Technology Help Provide a Legal Defence?

To use the Statutory Defence against a case where the Employer is being sued for harassment and discrimination, the reasonably practical measures taken ***do not have to be perfect or infallible***.

No technology is 100% accurate or available 24–7. The Law understand this – merely requires its implementation as a reasonably practical measure and that the implementation is not merely for show.

We have seen the that Statutory Defence is only available to the Employer if they can show that they have taken all reasonably practical steps to avoid the harassment. One modern and now common-place step to be taken is the implementation of a modern Content Security System whereby the software checks e-mails for profanity and indecent or obscene pictures. The Employer must be able to show that if an implementation of this type of technology is reasonably practical in order to protect employees, than they have done so. Thus an implementation of this technology (which is not just for show) will substantially improve an Employer's ability to access this defence.

*To use the Statutory Defence against a case where the Employer is being sued for harassment and discrimination, the reasonably practical measures taken **do not have to be perfect or infallible.***

What about SPAM?

A great deal of SPAM is rude, lewd or may contain indecent images. Once again the Employee has a right not to work in a hostile workplace where their health is not negatively affected. SPAM can create a hostile workplace as easily as any form of sexual or racial discrimination.

3.2 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 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.

The legal theory of Vicarious Liability even extends to workplace bullying and Employers are liable for workplace harassment even

if they were not in any way negligent. With a new generation of workers entering the workplace – who are used to texting, instant messaging and e-mailing; bullying using these digital means is bound to rise.

Previously employees had to prove that the employer was negligent in not stopping bullying taking place and that it had caused them psychological damage. But the law has changed on this point and it means that companies can be sued even if the company cannot be expected to have known about the bullying and this law is certainly wide enough to include the use of Explicit Images and E-Mailing as vehicles for e-bullying.

Are there Defences to Vicarious Liability in this Context?

There can be no doubt that this new interpretation of UK law has serious implications for employers as it gives employees who are bullied or harassed at work an additional way 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 would not help an employer facing a claim that it was vicariously liable for an employee's harassment under the Act.

As we know that harassment takes place in the workplace through the use of pornographic images and obscene and bullying e-mails, it seems that the only avenue forward for employers in avoiding the breadth of this area of law is to use every means, including technology, to try to intercept e-harassment and the E-Mails or the Explicit Images used by the workplace bully so as to stop it reaching the intended victim.

3.3 Employees, Pornography and Obscene Material in General

What if Employees are Forwarding Pornographic E-Mails and Attachments?

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.

Thus for example, an employee who transmits a pornographic picture to a co-worker or to someone outside the organisation as an E-Mail attachment is committing a criminal offence.

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 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.

*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.*

What other alternative is available to technologically interdict the behaviour which uses the Employer's ICT as its vector?

What about Offensive or Obscene E-Mails which aren't Pornographic?

It is illegal to send indecent or grossly offensive material in order to cause the recipient distress or anxiety. It is also a criminal offence send over a public electronic communications network a message that is of a *"…grossly offensive or of an indecent, obscene or menacing character"*. This includes the Internet.

Following the expansion of the Doctrine of Vicarious Liability – 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 (which produce the crimes just mentioned) must be very considerably higher.

Is it true that Indecent E-Mails in the Workplace can be a Criminal Offence?

Yes – the sending of e-mails of a sexual nature could earn the sender a place on the Sex Offenders' Register offences which are not primarily sexual in nature to be punishable by a Sexual Offences Prevention Order (often referred to as a "SOPO").

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.

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. Therefore an employee who sent e-mails, via the Internet, to others could be put on the public UK Register together with rapists and paedophiles.

3.4 Employees and Paedophilic Images

An important, complex and emergent area of modern Criminal Law is the liability of the Corporate Employer *itself* for the Criminal Acts of its Employees. 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[3]. What this means is that in each Company a Court of Law will recognize 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.

Do Paedophiles Download and Keep these Images at Work?

The existence of child pornography on an organisation's computer system may expose the corporation itself (and possibly senior individuals within it) to criminal prosecution. There is now substantial evidence available which shows that the dysfunctional individuals who engage in the downloading and keeping of child pornography, are likely to do that at work also if given unrestricted access to the Internet at their workplace. Prudent employers should do their best to intercept such behaviour at it's source since no amount of work-orientated training can restrain an individual from such a behavioural characteristic.

Can the Employer be Liable?

If management (and therefore the corporate employers) are shown to have been 'neglectful' in allowing child pornography into their IT structure; Criminal Liability attaches not only to the company itself but also to its officers and directors (which will be a matter of record). Additionally it applies to "Managers" and persons purporting to act in such a senior capacity. The question of whether or not a person is a "Manager" is a question of Law.

Why are Directors personally exposed to Criminal Prosecution?

As the purpose of the Law is *"… to fix with criminal liability only those who are in a position of real authority, the decision-makers within the company who have both the power and responsibility to decide corporate policy and strategy. It is to catch those responsible for putting proper procedures in place; it is not meant to strike at underlings"* it is constructed so that it is able not only to catch the Employer itself, but is capable of catching those Corporate Officers and their IT Directors, Security Directors and Senior Managers who decide corporate policy and are responsible for putting the proper procedures that will help prevent child pornography infecting their systems.

Remember – these systems that protect the Employer's systems ***do not have to be 100% effective***. Rather, implementing sensible training and technology-based systems go to show that the Employer has not been 'Neglectful'.

3 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".

Copyright Information