



UNDERSTANDING AND MANAGING
THE LEGAL AND SOCIAL ISSUES CAUSED BY
ILLCIT IMAGERY IN THE WORKPLACE
~ A LEGAL PERSPECTIVE ~

1. **SUMMARY**

1.1 **Corporate Liability for Employee Misuse of Employer IT Infrastructure**

- ➔ Corporations are being sued by Employees who have been *sexually harassed or bullied* through exposure to IIM¹ in the workplace by their co-workers.
- ➔ Corporation 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. Image Interdiction Technology is a reasonably practical measure.
- ➔ Corporations are *Vicariously Liable* to an Employee who has been Harassed by another Employee under the Protection from Harassment Act 1997.
- ➔ A Corporation's *only* defence where is it Vicariously Liable for an Employee's misdeeds is *Interdiction (preventing the harassment in the first place)*.
- ➔ Corporations are being sued by Employees who have been exposed to *Pornographic Internet Content* being accessed by their co-workers.
- ➔ Credibility in the market-place is being *seriously lost* when it becomes public that Employees engage in Inappropriate Internet Use which involve IIM.
- ➔ Corporations may suffer *Criminal Prosecution* when employees disseminate Pornography using the employer IT infrastructure.
- ➔ Corporations 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.

1.2 **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.

2. **SOME LAW**

2.1 **IIM as a Vehicle for Harassment**

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

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



UNDERSTANDING AND MANAGING
THE LEGAL AND SOCIAL ISSUES CAUSED BY
ILLCIT IMAGERY IN THE WORKPLACE
~ ~ ~ **A LEGAL PERSPECTIVE** ~ ~ ~

Where harassment is sexual in nature, the victim would be able to take a claim of unlawful discrimination to an employment tribunal under the *Sex Discrimination Act 1975*. 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.

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 sending pornographic images to another by e-mail 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 complained of his lewd e-mail which contained IIM).

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.

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 Image Interdiction Technology permits, for the first time, the prevention of sexual harassment through graphical digital means.

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.



UNDERSTANDING AND MANAGING
THE LEGAL AND SOCIAL ISSUES CAUSED BY
ILLCIT IMAGERY IN THE WORKPLACE
~ A LEGAL PERSPECTIVE ~

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.

2.2 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 case² 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.

In *Morse v. Future Reality Limited* (see footnote 2.) – no cause of action would have arisen to be used against the Employer *if* downloading pornography into the workplace was prevented technologically.

Thus, all of the costs, damages and loss of reputation in this case would have been completely avoided.

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 (including IIM) 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. If they could have, and did implement Image Interdiction Technology, they would not have been liable.

2.3 The Inescapable Exposure associated with Discrimination

All of the United Kingdom Discrimination Acts³ 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:

- (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.

² *Morse v Future Reality Ltd [1999]*

³ *Sex Discrimination Act 1975, Race Relations Act 1976, Disability Discrimination Act 1995*



UNDERSTANDING AND MANAGING THE LEGAL AND SOCIAL ISSUES CAUSED BY ILLCIT IMAGERY IN THE WORKPLACE ~ ~ ~ A LEGAL PERSPECTIVE ~ ~ ~

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. Where IIM is involved they may 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 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.

To use the Statutory Defence against harassment and discrimination, the Employer must show they have taken *all reasonably practical measures* to prevent it.

Image Interdiction Technology is the newest reasonably practical measure which **MUST** be taken. Without it – the defence is more likely to fail completely.

On this point, the Employment Appeal Tribunal held⁴ 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.

2.4 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.

In a landmark case in 2006 by the House of Lords⁵ (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 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 and this ruling is certainly wide enough to include the use of IIM as the vehicle for e-bullying.

⁴ *Haringey Council v Al-Azzawi* [2002]

⁵ *Majrowski v. Guy's and St. Thomas' NHS Trust* [2006] UKHL 34.



UNDERSTANDING AND MANAGING
THE LEGAL AND SOCIAL ISSUES CAUSED BY
ILLCIT IMAGERY IN THE WORKPLACE
~ A LEGAL PERSPECTIVE ~

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.

Vicarious Liability is the no-fault liability where the *Blameless Employer* is *liable* in law for the acts of the *Blameworthy Employee*.

We know digital Pornography is an instrument used to bully and harass in the workplace.

The Interdiction of such use is the ONLY defence available in law.

As we know that harassment takes place in the workplace through the use of pornographic images,⁶ it seems that the only avenue forward for employers in avoiding the breadth of this decision is to technologically interdict the harassment and the IIM employed therein so as to stop it reaching the intended target.

2.5 **Employees, Pornography and Obscene Material in General**

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.⁷ 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.

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.

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.

⁶ *Spencer v Primetime Recruitment Limited* EAT 2 March 2006

⁷ 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].



UNDERSTANDING AND MANAGING
THE LEGAL AND SOCIAL ISSUES CAUSED BY
ILLCIT IMAGERY IN THE WORKPLACE
~ A LEGAL PERSPECTIVE ~

The duty owed by the employer is in respect of the employee's physical and mental health, including ill-health caused by overwork⁸, psychiatric illness,⁹ and stress and anxiety caused thereby.¹⁰ ***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.***¹¹

2.6. 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 known in Criminal Law as the *alter ego* doctrine.¹² 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 criminal prosecution.¹³

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 employers should interdict such behaviour at its source since no amount of work-orientated training can restrain an individual from such a behavioural characteristic.

Before addressing the evidence of employees downloading paedophilic images into the work-place, it will be helpful to review the actual legislation involved:

Section 3, Subsection 1 of Protection of Children Act 1978 tells us.

“Where a body corporate is guilty of an offence under this Act and it is proved that the offence occurred with the consent or connivance of, or was attributable to any neglect on the part of, any director, manager, secretary, or other officer of the body, or any other person who was purporting to act in any such capacity he, as well as the body corporate, shall be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.”

⁸ *Johnstone v. Bloomsbury Health Authority*

⁹ *Frost v. Chief Constable of South Yorkshire Police*

¹⁰ *Walker v. Northumberland County Council*

¹¹ *Petch v. Customs and Excise Commissioners*

¹² 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”.

¹³ 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.



UNDERSTANDING AND MANAGING THE LEGAL AND SOCIAL ISSUES CAUSED BY ILLCIT IMAGERY IN THE WORKPLACE ~ ~ ~ A LEGAL PERSPECTIVE ~ ~ ~

It should be noted that the Criminal Liability attaches not only to the body corporate itself¹⁴ 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.

In a relevant case before it¹⁵, the Court of Appeal held that the purpose of imposing criminal liability on Managers was “...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”.

Possession of indecent photographs of children and indecent pseudo photographs of children is also an offence by virtue of Section 160 of the Criminal Justice Act 1998. The offence of ‘possession’ is not one of strict liability and the Courts of Law have held¹⁶ that: “...the offence of possession under s 160 of the 1988 Act was not committed unless the defendant knew that he had, or had once had, the photographs in his possession. Accordingly, an accused could not be convicted where, as in [this] case, he could not be shown to have been aware of the existence of a [temporary Internet Explorer] cache of photographs in the first place.”¹⁷

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 Corporation 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 in place that will inhibit or stop the making of indecent photographs and indecent pseudo-photographs of children by employees using the Corporation’s IT

Directors and Managers are **required** by the Law **NOT** to be Neglectful with respect to the entry points for Child Pornography making its way into their IT Infrastructure.

We **know** paedophiles download and keep child pornography in the workplace. The cases tell us so.

Consequently, Image Interdiction Technology must be an **essential** component in every Corporation’s legal protection strategy.

infrastructure. It is further suggested that the availability of software tools designed to interdict the entry of pornographic images into the Corporate IT Structure has now made the threshold of “Neglect” as used in the Protection of Children Act 1978 lower. It is suggested that Corporations and Executives will have to put forward sound reasoning, based on legal rules and legal analysis, as to why no “Neglect” had taken place in circumstances where an employee was making (downloading or copying) indecent photographs and/or indecent pseudo-photographs of children using the employer computer system where no IIM interdiction tool was present.

¹⁴ This term will include private limited companies, limited liability partnerships, public limited companies, trusts, local government authorities, charities and other incorporated bodies depending on the nature of their incorporation.
¹⁵ *R v. Boal* [Court of Appeal] [1992] Q B 591
¹⁶ *Atkins v. Director of Public Prosecutions* [Queen’s Bench Division, Divisional Court] [2000] 2 All ER 425, [2000] 1 WLR 1427, [2000] 2 Cr App Rep 248; *R v Buswell* [1972] 1 All ER 75 and *R v Steele* [1993] Crim LR 298 distinguished.
¹⁷ Un-italicised text in square brackets have been added by the author.



3. **SOME “REAL-LIFE” EXAMPLES**

3.1 **The Finance Services Group “Merrill Lynch” dismiss 13 staff.**¹⁸

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

3.2 **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.**¹⁹

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.

¹⁸ Reported in the “Irish Times” – 24th June 2006

¹⁹ Reported in the “The Times” – 22nd June 2006



UNDERSTANDING AND MANAGING
THE LEGAL AND SOCIAL ISSUES CAUSED BY
ILLCIT IMAGERY IN THE WORKPLACE
~ ~ ~ **A LEGAL PERSPECTIVE** ~ ~ ~

That investigation continued. It was reported that 65 workers at the Driver and Vehicle Licensing Agency (DVLA) in Swansea now face disciplinary action over the "inappropriate use" of e-mail.²⁰ The DVLA said the action followed a "*continuing investigation*" which has already led to the sacking of 14 staff who circulated pornographic e-mails. Some of the employees involved have unsuccessfully challenged the decision. But the agency said staff would be given the opportunity to respond to the gross misconduct charges.

A DVLA spokeswoman said: "*As a result of DVLA's continuing investigation into the inappropriate use of its e-mail facility, 65 employees have been charged with gross misconduct....The investigation will follow our normal procedures, and all concerned will have the opportunity to respond to the charge....All servers have been scrutinised, with no exceptions.*"

²⁰ Reported by the BBC Online – 13th November 2006