



# THE LEGAL EXPOSURE CAUSED BY INAPPROPRIATE DIGITAL IMAGERY IN THE WORKPLACE - A PERSPECTIVE ON DEFENCES AND INTERDICTION STRATEGIES

---

## Introduction

The Law provides an intensely complex network in which the unwary and unprepared employer can become trapped by its employee's misuse of its IT infrastructure. The legal exposure that arises ranges from loss of reputation, to actions for damages for sexual harassment even to the risk of criminal prosecution for the corporation and even, in some circumstances, its officers and key employees.

## This Paper

The purpose of this paper is to provide an initial entrée into the classes of Legal Exposure which can arise for corporate entities when their employees introduce inappropriate, lewd and pornographic images<sup>1</sup> into the work-place through their misuse of the ICT<sup>2</sup> facilities provided for them. Having made that entrée, an introduction will be made to methods and strategies which, once integrated, not only provide legal defences to the exposure that arises but also lends to mitigating the organisations loss and exposure overall to the complexities faced in constructing a response to the dangers and demands of the "HazardSphere". It is authored by Dr. Brian Bandey who is one of the United Kingdom's leading experts on IT Law, Internet and Computer Law. His experience in the global computer law environment spans more than a quarter of a century and he routinely advises on almost every specie of arrangement that the world computer software industry makes.

Dr. Bandey is the principal of the UK consultancy practice "PATRONUS" servicing specialist copyright/computer law advice throughout the world.

He is the author of a definitive legal practitioners textbook on "International Copyright in Computer Program Technology". This work is recognised as being the first definitive text which examines all of the principal technologies employed in the development, manufacture, use and general exploitation of all computer program types; thereafter applying the Law of Copyright (in the United Kingdom, USA and the European Union). A new edition to this work is in progress together with works on the Law of the Internet and E-Liability. "International Copyright in Computer Program Technology" has won international acclaim from practitioners and academics alike - for example, it is cited by William R. Cornish, QC. (Herchel Smith Professor of Intellectual Property Law at the University of Cambridge, England) in his work "Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights" (4<sup>th</sup> Ed.). It is also cited in "Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights" (5<sup>th</sup> Ed.) by Cornish and Llewelyn.

His legal opinions are regularly published throughout the world. For example, he has had articles published on "Multimedia Law" and "Computer-Generated Works" by the New Zealand Intellectual Property Journal and his commentaries on current legal issues are syndicated throughout the world by such organisations as the BBC and Washington Post.

Dr. Bandey is now well-advanced upon the unique route of studying for a second Doctorate of Law advancing the current state of the art in the Copyright in the Construction, Structure and Operation of Internet-based Technologies with St. Peter's College at the University of Oxford in England. He is a Research Associate of the Oxford Intellectual Property Research Centre ([www.oiprc.ox.ac.uk](http://www.oiprc.ox.ac.uk)) and advises the Open Source Software Advisory Service ([www.oss-watch.ac.uk](http://www.oss-watch.ac.uk)) on Intellectual Property matters.

His other current research interests include 'Internet Law' and 'Corporate Legal Liability arising by the Misuse of Employer IT Systems by Employees'.

---

<sup>1</sup> The abbreviation "IIM" will be employed to describe all forms of inappropriate, lewd, pornographic and unlawful or illegal graphic and image material ("Inappropriate Image Material"). The term "Image Material" is employed since the illegality of some images extends beyond photographs but to images which are similar to a photograph but which, in law, are not.

<sup>2</sup> Information Communication Technology



## THE LEGAL EXPOSURE CAUSED BY INAPPROPRIATE DIGITAL IMAGERY IN THE WORKPLACE - A PERSPECTIVE ON DEFENCES AND INTERDICTION STRATEGIES

---

### The “HazardSphere”

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

*The Law of Confidence*  
*Human Rights Law*

*Employment Law*  
*Data Protection Law*

*The Law of Copyright*  
*Criminal Law*

For ease of reference, this ‘activity area’, this ‘space’ (so to speak) of misusing E-Mails, Internet Access and Employer IT Systems over which and through which so many important, settled and significant areas of Law intersect will be referred to in this paper as the “HazardSphere”.<sup>3</sup>

Classes of “Misuse” to be addressed include:

*Harassment by E-Mail & IIM*  
*Distribution of Pornography*

*Indirect Harassment via Internet Access*  
*Distribution of Obscene Material*

*Unlawful Discrimination*  
*Paedophilic Image Material*

In doing so 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 EMail, Internet Access and IT System Misuse involving IIM occupies a space at the intersection of a number of significant, well-established and important theories of law. What we can do therefore is (including real-life examples) identify the types of ‘mis use’ that arise and describe the applicable Law in the broadest of terms.

Although this paper is 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 ICT 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 ICT for personal purposes in circumstances where their employer has not issued guidelines on where the boundaries of their permitted use lie.

Sending an EMail (together with IIM) 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, any IIM attached, and the name of the employer.

Overarching this state of ignorance is a modern attitude towards IT use 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 and that there is no perceived actual or moral difference between an employee using their own computer at home and using their employer’s computer system for identical purposes at work.

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), to every instance of Internet Access, and to what may be uploaded to the Corporate IT System by the employee.<sup>4</sup> Employees should be encouraged to understand that both the content and style of their Corporate IT System Use will reflect the perceived professionalism and reputation of both themselves and their employer.<sup>5</sup>

---

<sup>3</sup> “HazardSphere” is a trade mark of Dr. Brian Bandey.

<sup>4</sup> It should always be borne in mind that employees are able to upload IIM to the employer system through the use of floppy diskettes, CDs, DVDs and Memory Sticks.

<sup>5</sup> 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



## THE LEGAL EXPOSURE CAUSED BY INAPPROPRIATE DIGITAL IMAGERY IN THE WORKPLACE - A PERSPECTIVE ON DEFENCES AND INTERDICTION STRATEGIES

---

### 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. 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 1<sup>st</sup> 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 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.

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.

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.

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.

---

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.

---



## THE LEGAL EXPOSURE CAUSED BY INAPPROPRIATE DIGITAL IMAGERY IN THE WORKPLACE - A PERSPECTIVE ON DEFENCES AND INTERDICTION STRATEGIES

---

### 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<sup>6</sup> 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.

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.

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.

On this point, the Employment Appeal Tribunal held<sup>7</sup> 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.

---

In *Morse v. Future Reality Limited* – 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.

---

---

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.

---

<sup>6</sup> *Morse v Future Reality Ltd* [1999]

<sup>7</sup> *Haringey Council v Al-Azzawi* [2002]



## THE LEGAL EXPOSURE CAUSED BY INAPPROPRIATE DIGITAL IMAGERY IN THE WORKPLACE - A PERSPECTIVE ON DEFENCES AND INTERDICTION STRATEGIES

### 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 Lords<sup>8</sup> (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.

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,<sup>9</sup> 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. In the event of a failed interdiction, appropriate and focussed insurance must be the last stage in mitigating this considerable exposure.

### Employees, Pornography and Obscene Material in General

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.<sup>10</sup> A similar offence 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*".<sup>11</sup>

After the decision in 2006 by the House of Lords<sup>12</sup> 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.

---

<sup>8</sup> *Majrowski v. Guy's and St. Thomas' NHS Trust* [2006] UKHL 34.

<sup>9</sup> *Spencer v Primetime Recruitment Limited* EAT 2 March 2006. A manager e-mailed his staff photographs of female genitalia.

<sup>10</sup> Sections 1(1)(b) Communications Act 2003. See especially the House of Lords decision in *DPP v. Collins* [2006] UKHL 40.

<sup>11</sup> Section 127(1)(a)s 1(1)(b) and 4. Malicious Communications Act 1988. See especially *Veronica Connolly v. DPP* [2007] EWHC (Hearing Date: 23<sup>rd</sup> January 2007) who sent photographs of aborted foetuses to pharmacies who stocked the 'morning after' contraceptive.

<sup>12</sup> *Majrowski v. Guy's and St. Thomas' NHS Trust* [2006] UKHL 34.



## THE LEGAL EXPOSURE CAUSED BY INAPPROPRIATE DIGITAL IMAGERY IN THE WORKPLACE - A PERSPECTIVE ON DEFENCES AND INTERDICTION STRATEGIES

---

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. The duty owed by the employer is in respect of the employee's physical and mental health, including ill-health caused by overwork<sup>13</sup>, psychiatric illness,<sup>14</sup> and stress and anxiety caused thereby.<sup>15</sup> 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.<sup>16</sup>

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<sup>17</sup> 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").

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.

### 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.

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.<sup>18</sup> It should be noted that the Criminal

---

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 and Insurance are the **ONLY** realistic answers.

---

---

<sup>13</sup> *Johnstone v. Bloomsbury Health Authority*

<sup>14</sup> *Frost v. Chief Constable of South Yorkshire Police*

<sup>15</sup> *Walker v. Northumberland County Council*. See also *Intel Incorporation (UK) Limited v. Tracy Ann Daw* [2007] EWCA Civ 70 (CA).

<sup>16</sup> *Petch v. Customs and Excise Commissioners*

<sup>17</sup> Sexual Offences Act 2003 (Amendment of Schedules 3 and 5) Order 2007 (Statutory Instrument 2007 No.296) coming into force on 19<sup>th</sup> February 2007. Made by the Secretary of State pursuant to Section 130 Sexual Offences act 2003. The Order does not apply in Scotland.

<sup>18</sup> 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.



## THE LEGAL EXPOSURE CAUSED BY INAPPROPRIATE DIGITAL IMAGERY IN THE WORKPLACE - A PERSPECTIVE ON DEFENCES AND INTERDICTION STRATEGIES

Liability attaches not only to the body corporate itself<sup>19</sup> 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.

There is considerable 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 it’s source since no amount of work-orientated training can restrain an individual from such a behavioural characteristic.

### Conclusions

Image Interdiction Technology is now an essential component in any organisation’s legal defence when being sued in respect of sexual harassment, bullying and actions founded on the lack of provision of a safe working environment. However, mere installation and execution will not do. In the hostile, complicated and interconnected HazardSphere a sophisticated network of response needs to be put into place. The technology must form part of a strategy designed to access the defences that are available in law to employers. But more than this, since no computer programming technology is infallible and since some areas of vicarious liability allow for no defence – then the prudent organisation must look to implementing a targeted and overarching insurance solution.

Officers and their managers are on the front line. Only a sophisticated, tiered and integrated defence strategy that encompasses:

- ? Image Interdiction
- ? E-Mail & Chat Control
- ? Resource Management
- ? Training & Awareness
- ? Enterprise Insurance Securities
  - o Liability
  - o Directors & Officers
  - o Legal Costs

will suffice.

<end of paper>

**Via eSafebusiness™; Guardware is one of very, very few companies able to deliver this truly integrated response**



**GUARDWARE**  
Ensure the Responsible  
Use of Information Technology

<sup>19</sup> 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.