E-MAIL @ WORK: ITS LEGAL IMPLICATION ON EMPLOYER'S LIABILITY [2001] 3 MLJ xxviii

Malayan Law Journal Articles

E-MAIL @ WORK: ITS LEGAL IMPLICATION ON EMPLOYER'S LIABILITY

Zaiton Hamin

Senior Lecturer, Faculty of Administration and Law, Universiti Teknologi MARA, Doctoral Researcher, Cyberlaw Research Unit, Centre of Criminal Justice Studies, University of Leeds

Introduction

The advent of the Internet, the Web and the proliferation of electronic mail communication (hereinafter 'the e-mail') have made them essential business tools and ubiquitous. E-mail has become a relatively cheap, quick and a convenient form of communication. The Electronic Mail and Messaging Systems report (1999) shows a high level of usage of more than 195 million corporate users worldwide that makes e-mail the most critical application on the Internet. Not since the introduction of television has there been such an exponential growth in the application of information technology. Datamonitor report in 1999 estimated that by 2000 the Internet population might reach 250 million and 300 million in 2005.[1]

Whilst providing innovation and generating efficiency, the proliferation and availability of e-mail in the workplace has presented considerable opportunities for misuse. For instance, a study in 1997 suggests that more than 30 percent of all e-mail messages sent by employees are non-work related.[2] Similarly, the IDC Research survey 1999 reported that 30–40 per cent of Internet access within corporate workplace was not business related.[3] However, the recent self-report Elron study 2000 of corporate Internet usage revealed a more alarming figure. Out of 576 respondents who have access to the Internet and e-mail at work, more than 85 per cent of them had used these facilities for personal matters.[4] Secure Computing survey 2000 confirmed these findings of non-work related use of the Internet and e-mail, when they reported that 50 per cent visit pornographic sites, 92 per cent buys goods online, 84 per cent searched for jobs online; 54 per cent visit chat rooms whilst at work.[5]

Despite the problem of the availability of independent data, such studies have significant implications for employers. They raise broader issues of the legal risks that could expose employers to a panoply of potential civil claims including contract, negligence, defamation, sexual or racial harassment or potential criminal actions for publication of obscene materials. Indeed, the potential for workplace mischief and a significant development in employment litigation from e-mail are certainly enormous. E-mail is said to have opened up a Pandora's box of legal issues.[6] Although corporate legal vulnerabilities are already in evidence in suits against major corporate employers (such as Microsoft and Intel) and against government agencies in the US and the UK, many employers and employee alike use e-mail without a clear understanding of their vulnerabilities. Even when employers are aware of these potential liability, they are not taking sufficient proactive measures to prevent inappropriate use of e-mail.

This article seeks to examine the legal issues and recent legal developments concerning the Internet and e-mail misuse and its impact on employer's liability in the UK and the USA. The first part commences by considering briefly the nature of the Internet and e-mail and by exploring the ideas underlying these new emerging technologies. The second part critically highlights and examines the problematic legal issues affecting employer's direct and vicarious liability that may arise from e-mail misuse. The last section concludes the article with the recommendation for non-legal measures to address the problem and to reduce, if not to eradicate, employers' liability for e-mail misuse.

The Internet, e-mail and the 'global village'

Historically, the Internet evolved in 1969 from an experimental computer network called the Advanced Research Project Agency Network (ARPANET) by the United States Department of Defence. ARPANET was devised as a decentralized system of computers that permitted computer communication across vast distances and was intended to withstand a nuclear attack.[7] The network was eventually extended to include academic institutions,[8] and then to commercial organizations and through them, to private individuals, particularly after the development of the Web or World Wide Web (WWW) in 1992.[9] In the technical sense, the Internet is a network of computers, which are able to inter-communicate data split into 'packets' via modem, through the Transmission Control Protocol/Internet Protocol standards. The Internet supports a wide variety of communications, including electronic mail, chat groups, newsgroups, and the World Wide Web. In this context, cyberspace, which has developed from a science fiction by Gibson (1994),[10] represents both the intangible communities and the interactive space made possible by the communications networks of the Internet. It has been commonly understood to be a place without the physical, political, economic and social boundaries or the physical dimension in which interactions occur.[11]

This characteristic has enabled the Internet to develop beyond its initial military and academic objectives, creating what is termed by Wall (1999) as the 'quantum leap in communication.'[12] Cyberspace is enabling a vast number of people across a wide jurisdictional range to communicate almost without restrictions. This has considerably reduced alienation and is making the world into a 'global village' as envisaged by McLuhan (1964) in which time and space simply disappears.[13] Thus, the Internet involves individuals in a simultaneous manner creating a new multi-sensory view of the world.

Significantly, as Wall (1997, 1999) has correctly observed, the Internet has also made an impact on the qualities imbued with high modernity,[14] in particular, the 'discontinuities' with the past and which, according to Giddens (1991)[15] has some bearing on time-and-space distanciation'. Commentators such as Giddens (1991), Bottom and Wiles (1996) and also Wall (1997) note that such a 'break' has disembedded or has resulted in the 'lifting out' of social relations from the local context of interaction and their restructuring across indefinite spans of time-space.[16] With the rapid development in the new information and communication technologies, this time-space distanciation or disappearance have translated into reality and have become more pronounced than ever before. It is now possible for individuals to work without the physical office, without their physical presence or face-to-face meetings. E-mail allows messages to be sent to more than one recipient at any one time and it allows easy distribution and dissemination of office files or information contained in reports, spreadsheets and presentations. Hence, e-mail has evolved further from being a mere communication tool to an information-sharing and routing facility.

Technically, e-mail is a method of transmitting information electronically from one computer to another, over a network. Such networks may involve a proprietary one such as the Local Area Networks (LANs) or the Wide Area Networks (WANs), in which the necessary hardware is owned or leased by, and under the control of the employer organization.[17] Alternatively, employees may use e-mail through public networks such as the Internet, or via the Intranet, a hybrid of the previous two networks.[18] The Intranet will not only allow users to access, download and transfer internal data from anywhere within the organization, it also allows users to go directly from their LAN or WAN to the Internet.[19] When employees are given the e-mail facility they may sometimes be provided with a password or they may choose their own. Generally, the use of passwords has led to the misconception that their e-mail communication is private. In fact, it is technologically possible to read employee e-mail from a different computer terminal and without the employee's consent, which is normally legal and regularly practised by employers in their monitoring exercise of their employees' activities at work.[20]

Consequently, cyberspace has not only engendered social and behavioural changes, but has also reconfigured many socially-understood terms, such as that of ownership and control that help mould our behaviour.[21] Barlow (1994) and Boyle (1996) suggest that the new primacy being placed on the information or the notion of intangible ideas has generated the new political economy of informational capital,[22] as well as the new society, which Castells (1994) termed as the 'networked society'.[23] Moreover, cyberspace has the tendency to blur the conventional borders between public and private law and also between criminal and wrongful conduct. Significantly, it also challenges many of the traditional legal principles upon which our conventional understanding of crime and tortious conduct are based. Important questions surface as to what kinds of employee activities can liability, be it direct or vicarious, be attached to employers and to what extent do the laws applicable to online behaviour differ from that we currently apply to conduct in the real world? Before examining these germane issues in detail, we may need to consider the basic tenets of employer's liability for employee conduct.

General principles of employers' liability

There are several possible courses of action in determining employers' liability, involving claims between employers and employees and vice versa; between third parties and employers and vice versa and between third party and employees and vice versa. From this multiplicity of claims it can be seen that the general basis for the liability of employers for the online conduct of employees may be drawn from the principle of either direct or indirect (vicarious) liability. The former type of liability implies that liability that attaches to the organization or a company when they themselves direct or authorize the employee to act in a certain way. In *Tesco Supermarkets Limited v Nattrass*,[24] Lord Reid held that this direct liability occurs when a person is 'not acting as a servant, representative, agent or delegate' of the company but as 'an embodiment of the company'.[25] This would not only cover acts of directors and senior management when they are acting 'as the company' but it may also extend to those acts of employees acting under delegated authority.

Vicarious liability, on the other hand, may be attached to employers for the acts of their employees in the course of their employment. With the usage of the new technologies by many employees nowadays, such liability that may be imposed on employers at common law [26] or by statutory provisions, both in civil and criminal law, have been one of the biggest concern of many employers. The imposition of vicarious liability on employers in the absence of any fault on their part might be premised on two principal policy

considerations. Firstly, the provision of a just and practical remedy to the victim. Secondly, the deterrence of potential

harm.[27] Nevertheless, the key question for such liability is whether the employee was acting 'in the course of his employment' at the time in question. In *Jones v Tower Boot Co Ltd*,[28] the Court of Appeal held that this phrase should be given its ordinary meaning and should not be construed restrictively. Latham CJ applied a broad interpretation of the concept in *Deatons Property Ltd v Flew*.[29] His Lordship held that an act is within the scope of his employment if the employee was retained to perform the act, or if its performance is reasonably incidental to the matters which the employee was retained to do.[30] This would suggest some importance of incidental connection, as opposed to a significant connection, between the employer's enterprise and the employee's wrongful act, which would be sufficient to establish vicarious liability. The mere fact that the wrongful act was committed during work hours or at the workplace would appear to be sufficient.

Nonetheless, an employee is within the scope of his employment if the act normally forms part of his employment and that the employer's prohibition from doing the act will not bar any liability (*Ilkiw v Samuels*).[31] However, in *Rose v Plenty*[32] the court was more willing to impose vicarious liability where the employee's act was advantageous to the employer. In *Century Insurance Co Ltd v Northern Ireland Road Transport Board* [33] the court went further and held that an authorized act of an employee albeit performed in an improper or wrongful manner will still constitute an act within the course of his employment. However, in *Tiger Nominees Property Limited v State Pollution Control Commission*,[34] Gleeson CJ held that it is immaterial that the employee is unauthorized to perform the act. Similarly, in *Bugge v Brown*,[35] Isaacs J held that the mere fact that an act is illegal does not bring it outside the scope of employment.

It is a matter of degree whether an employee is acting in the course of his employment or not. Hence, the same question for determining the scope of employment could well be asked in determining when an employee ceases to be so acting, i.e., what was the employee employed to do and was he still doing the authorized acts at the time in question?[36] The answers to these questions may be found if the employee's conduct is entirely independent and unrelated to the employer's business. Thus, in *Hilton v Thomas Burton (Rhodes) Limited* [37] the court held that the employees were not acting within the scope of their employment when they were 'filling in the rest of their time until their hours of work had come to an end.'[38] In the context of the Internet, an employer may be vicariously liable for e-mail sent by the employees to other employees, clients and customers whilst at work. However, they may not be so liable for conduct outside the work hours and those unrelated to work, such as e-mails to friends and family sent after work.[39]

Legal ramifications

In the proceeding analysis we will examine some of the significant areas involving employers' liability that have emerged in the UK and the USA, affecting tortious, contractual and criminal activities of employees.

Sexual harassment

Unacceptable conduct of a sexual nature that is unwanted or unwelcome whereby any reasonable recipient would be offended, humiliated or intimidated may occur in any workplace.[40] However, with the

prevalence of e-mail and the ease of forwarding e-mails to a far greater number of recipients, the availability of sexually explicit materials from the Internet and the ease of downloading such materials, harassment by e-mail is likely to escalate. Several employers including Eastman Kodak and Hallmark Cards Inc. have acknowledged that sexual harassment complaints are the most prevalently reported e-mail misuse in their companies.[41] The air of informality surrounding e-mail and its perceived impermanence would seem to generate some lack of inhibition and spontaneity on the part of its users. Additionally, sexual harassment via e-mail presents some problems for employers as its invincibility makes it harder to stop and

contain than the ones in the real world.[42] Of particular importance is the difficulty in determining the identity of the harasser given the anonymity available to users that is provided by the Internet through anonymous remailers.[43] Several interesting and problematic issues may be raised by sexual harassment cases. To what extent should employers act to stop such misconduct? Would changing the victim's e-mail address be adequate? If anonymous remailers were used would employers be required to subpoena anonymiser.com records in order to determine the true identity of the harasser?[44] There are no easy answers to these issues and it would be open for the courts to decide.

In the UK, employer's liability for sexual harassment arises either directly when the employer himself is directly responsible for the treatment, under sections 2 and 6 of the Sex Discrimination Act 1975, or vicariously as provided for in section 41 of the Act. This later section states that anything done in the course of his employment is treated as done by the employer as well as by him, whether or not it is done with the employers' knowledge or approval. Recent English cases have extended employers' liability for the acts of sexual (and racial) harassment at work both by employees and third parties.[45] However, in the USA the basis of employer's liability for e-mail sexual harassment is broader than the UK position in that employers' liability may well depend on the severity and pervasiveness of the act, the knowledge on the part of the employers and their responses to such misconduct.[46] Nevertheless, an employer in the UK may escape vicarious liability for such online misconduct by an employee if he can show that all reasonable steps have been taken to prevent the harassment in question from occurring.[47] Although in general, clear warnings to employees as

contained in an e-mail usage policy may not be conclusive, it would be of some assistance to an employer's defence.[48]

Two types of sexual harassment by e-mail can be identified. On the one hand, it may be committed directly when a repeated or persistent e-mail is sent to the victim requesting a date or sexual favours, or sending e-mail containing sexual innuendoes. On the other hand, harassment may be committed indirectly when a 'hostile work environment' is created, for example, by circulating sexually explicit images or e-mail jokes around the office or by installing sexually explicit screen savers or computer programs. Hence, a sexually suggestive e-mail in the workplace may constitute evidence of a sexual harassment or a hostile work environment. In *Harley v McCoach*,[49] an e-mail message sent to the plaintiff identifying her as 'Brown Sugar' was held to warrant a hostile workplace claim. In this present case, the court took into account whether or not the employer had taken any prompt and remedial actions (including withdrawal of e-mail privileges from the sender) upon receiving the complaint. However, in a contrasting case in *Schwenn v Anheuser-Busch Inc.*[50] the court held that three weeks of e-mail

harassment at work which contained messages such as, 'I want to eat you' and 'meet me in aisle 50 [at some specific time]' was not pervasive enough to justify a hostile work environment claim.

A sexually-offensive material circulating on the organization network may be used as evidence that the employer tolerates a 'climate conducive to a hostile environment.'[51] An example is a sexual harassment suit brought by a woman employee in 1995 against a Chevron Corporation subsidiary company for an e-mail that was circulated throughout the company about 'why beer is better than women', resulting in an out-of-court settlement of US$2.2 million.[52] Another illustration involved Microsoft, in which four female employees filed a suit against the company for sexual harassment over several sexually explicit e-mail messages sent between employees in the company's IT division culminating in an out-of-court settlement for US$2.2 million and costs.[53]

In the UK, an employer is deemed to have tolerated a hostile work environment even if the offending e-mail or Internet activity was not directed at the victim personally. It is adequate that such conduct created an atmosphere in which the victim felt uncomfortable and that the employer had not done anything to prevent such a situation. *Morse v Future Reality Ltd. London*,[54] a case involving Internet pornography in the workplace, may be instructive. In the present case, the employment tribunal suggested that an employer has a duty to respond immediately when attention has been drawn to inappropriate behaviour in the workplace. Here, a female employee worked in an office where a considerable amount of her male colleagues' time were spent looking at sexually explicit or obscene images downloaded from the Internet, one or two of which were specifically drawn to her attention as a joke. She resigned, citing that the obscene images, bad language and the general atmosphere of obscenity in the office constituted a hostile work environment. Although she accepted that these activities were not directed at her personally, they did cause her to feel uncomfortable. The tribunal held that these factors had a detrimental impact on Morse and thereby constituted sexual harassment and that the employer was liable for not taking any action to prevent such misconduct. The tribunal awarded £750 for injury and three months' loss of earnings.

Of equal importance is that liability for sexual harassment may arise even where the employee does not compose the e-mail message himself but merely forwards it on to others. In the *American case of Strauss v Microsoft* [55] two e-mails were forwarded to the plaintiff, a female employee, by a male member of the staff. One contained a news report on Finland's proposal for sex holiday and another relates to a parody of a play entitled 'A Girl's Guide to Condoms.' The court held that it is irrelevant that the e-mails were not composed specifically for the plaintiff and sent directly to her, the mere act of distribution of the offending e-mails was sufficient.

Racial harassment

In respect of racial harassment, the UK Race Relations Act 1976 contains corresponding provisions to sexual harassment, governing the employer's direct [56] or vicarious liability.[57] An employer may be vicariously liable for racial harassment committed via e-mail where the situation is sufficiently within the employer's control.[58] Again, similar to sexual harassment claims, it is a defence for the employer to show that he has taken reasonably practicable steps to prevent the harassment.[59]

Although there is no English authority on racial harassment via e-mail, several American decisions may

be instructive. In *Curtis v Dimaio*[60] the court rejected the claims that Citibank managers circulated racial and ethnic jokes over their e-mail system. It was held that hostile work environment claims are meant to protect against severe abuse and trauma and that they are not intended to promote or enforce civility, gentility or even decency in the workplace. Similarly, in *Daniels v WorldCom Corp* [61] the court held that four e-mails received by the plaintiff from a non-managerial employee that were alleged to be racial harassment did not amount to a hostile work environment. Failure to exhaust administrative remedies was held to be a ground for the dismissal of the suit. The court, however, observed that the prompt measures taken by the employer including disciplining the sender who has violated the company e-mail policy may be sufficient to prevent liability. However, in the contrasting case of *Owens v Morgan Stanley & Co Inc*,[62] two African-American employees successfully filed a US $60 million racial harassment suit against their employer, an investment banking firm, after receiving a racist joke via e-mail at work, resulting in a confidential out-of-court settlement in 1998.

Cyber-defamation

The increasing use of e-mail as evidence in corporate litigation (for example, in cases involving cyber-defamation) has been one of the main concerns of many employers.[63] Cyber-defamation involves a statement or publication (here, by e-mail) that has the effect of injuring the reputation of another person or holding such person up to hatred, ridicule or contempt.[64] Both libel and slander are the main components of defamation; the former relates to communication of such statement in a written permanent form (which would cover e-mail) whilst the latter refers to the statement that is made orally. In the UK, for a successful claim of cyber-defamation, the defamatory statement must not only exist, it must also identify the injured party and must be published (i.e., communicated), for instance, transmitted by e-mail, to a third party.[65] Proof of damage may be immaterial as this is automatically presumed.

Employers may be vicariously liable for the defamatory statements made online by their employees in the same manner as the defamation in the real world through letters and faxes. The employees must be acting within the scope of their employment at the time the statements were made (*Lloyd v Smith*).[66] This case also suggest that the fact that the employee's act was unauthorized and not for the benefit of the employer will not bar such liability. Furthermore, in *Limpus v London General Omnibus,*[67] the court held that an employer would still be held liable even if he has expressly prohibited the acts. The operation of this vicarious liability could therefore turn an employer into a primary publisher of the defamatory statement.

Publication is the key question in defamatory conduct on the Internet.[68] The mode of publication or posting of defamatory materials has been democratized by the Internet, not merely through e-mails but also through postings to bulletin boards; in newsgroups or discussion lists; through text placed on the web pages and also through downloadable files (such as on the ftp servers).[69] It is through these broad forums that many disgruntled employees or former employees have been able to vent their grievances against their employers and communicate it throughout cyberspace, which has become known as ‘cyber-libel' or ‘cyber-smearing'.[70] Moreover, it is also through such forums that an employer's vicarious liability for defamation by their employees might ensue, although undoubtedly the employee who makes the defamatory statement would be directly liable. If the libellous message is forwarded to another person, then the ‘forwarder' may also be liable for the re-publication of the statement. However, it may be more sensible to proceed with what is called a ‘deep-pocket litigation' by seeking action against the author's

employer rather than the author/employee, because the employer has undoubtedly more money and assets than the author himself.

The recent case of *Western Provident Association v Norwich Union* [71] is a salutary lesson for employers whose employees have access to the internal e-mail system and to the Internet.[72] It is also a classic illustration of employers' liability for defamatory e-mails that are being circulated by employees. The plaintiff, a private medical health insurer, sued the defendant, a competitor, for libel after discovering that the defendant was circulating damaging and untrue rumours on their internal e-mail system to create the impression that the plaintiff was in financial difficulties and was being investigated by the Department of Trade. The case was later settled out-of-court in which the defendant had to pay £450,000 in damages and costs and to apologize publicly for the libel. The present case would appear to suggest that the 'publication' for the purpose of cyber-libel occurred the minute someone other than the author of the material read it.[73] Furthermore, this case would also seem to suggest that technically, e-mail is a permanent discoverable document because 'delete' for e-mail does not necessarily mean so. The 'deleted' (i.e., clicking on the delete button with the mouse) messages may still be accessible in the computer's hard drive or in the backup tapes or disk and hence may leave a 'trail' of evidence or electronic footprints.[74] Such messages may still be subject to a discovery request, and consequently they can become the 'smoking gun' of litigation.[75] Given the existence of vicarious liability, there may be little that employers could do to protect themselves against cyber-libel liability.

Similarly, in *EGS v British Gas*,[76] disparaging remarks circulated via an internal e-mail in British Gas that the plaintiff, established by a former employee of the defendant, was being subject to serious complaints and that the public should not deal with them. The defendant would be deemed to be the author of the defamatory statement and could be vicariously liable. However, the case finally resulted in an out-of-court settlement costing British Gas £101,000.

A recent landmark American case on cyber-defamation not only raises jurisdictional issues but also raises the question of what constitutes a workplace and the justification of workplace monitoring by employers of employees' Internet usage. In *Blakey v Continental Airways*,[77] a female pilot sued the defendant, her employer, claiming that pinups and vulgarities that were rampant in the cockpit created a hostile work environment. Whilst the case was still pending in the federal court, some fellow pilots posted nasty messages on an online bulletin board hosted by CompuServe. This board was routinely accessed by the pilots and the cabin crews of the said company to check on their flight schedules, flight information and to engage in workplace gossip and chat. The pilots used the chat room to criticize the plaintiff, calling her an opportunist and inefficient for destroying a company engine and floatplane and viciously ridiculed her for her lawsuits. The plaintiff then filed another claim for defamation against the airlines and the pilots in New Jersey. The main issue in the present case is whether the court in New Jersey had jurisdiction over the pilots as most of them do not live or work in that state. The trial judge held that the court had no jurisdiction over the pilots and that the company was not liable for the pilots' defamatory online statements. On appeal, this decision was affirmed but was finally reversed by the New Jersey Supreme Court.[78]

In the present case, the Supreme Court judge, Justice O'Hern, held that if the bulletin board is integrally related to work, then it becomes an extension of the workplace. It is in such extensions that relationships among employees 'are cemented or sometimes sundered.'[79] Thus, if such a setting, whether physical or

virtual, is a site for severe or pervasive harassment, the employer who has knowledge of such conduct should take serious measures to stop it. O'Hern also held that if the pilots' statements were published 'with knowledge or purpose of causing harm' to the plaintiff in New Jersey, they had the requisite 'minimum contacts' to support New Jersey jurisdiction. Justice O'Hern took into account that inappropriate activity may occur when employees are given access to the Internet, which might necessitate online monitoring. However, despite the emphasis of the court that employers must respond positively upon any complaints of harassment, it stopped short of placing the burden on employers of systematic monitoring when it held that employers are not obliged to spy on their employees' use of the Internet.

However, in practice, defamatory statements may sometimes be made outside the scope of the employment although the employees may be using the employer's computing facilities. This would inevitably create a more problematic situation of direct liability of employers. Such a liability may attach to employers if they are deemed to be responsible for publishing the statement. By merely making the offending statement available to a broader audience, an employer could effectively be the secondary publisher and the service provider of the e-mail, particularly internal e-mail, which is typically owned and managed by an employer. This secondary liability is already developing in other jurisdictions outside the UK such as that of the USA and Australia.

As a service provider, an employer may be placed in an analogous situation to that of an Internet Service Provider (ISP) that provide facilities to home users. As such, the ongoing controversy on the liability of an ISP for its customer's conduct could inform the issue of employer's liability. Recently, the American court in *Lunney v Prodigy* [80] has held that an ISP could not be liable for the defamatory posting of its customer, on the grounds that like a telephone company, it is merely a conduit. It could not be considered a 'publisher' because it had not participated in preparing the message, or exercised any discretion or control over its communication, or in any way assumed responsibility. Even if the defendant were a publisher, it was entitled to qualified privilege in the same way as that of the telephone companies.

However, in sharp contrast to the American approach, liability for defamation in the UK is subject to the defence of innocent dissemination provided for by section 1(1) of the Defamation Act 1996. In order for an employer to rely on this defence, it must show that it was not the author, editor or commercial publisher of the statement. It must also show that it took 'reasonable care' in relation to the publication and that it did not know or that it had reasonable belief that what it did caused or contributed to the publication of the statement in question. The application of this defence to defamatory publication on the Internet was recently tested for the first time in the well-publicized case of *Godfrey v Demon Internet Ltd*,[81] which concerned alleged defamatory messages purportedly sent by the plaintiff to the defendant's bulletin board. The plaintiff denied ever sending them and requested that the statements be removed to which the defendant refused. The defendant claimed innocent dissemination. The trial court held that in view of the existence of the fax from the plaintiff and defendant's refusal to remove the offending material, the defendant is deemed to have knowledge of the defamatory statement. Accordingly, the defendant could not rely on the defence in section 1. The defendant settled the matter shortly before the appeal was heard and is reported to have paid £15,000 in damages and over £200,000 in costs.

One could observe that liability for cyberdefamation is becoming more complex as it raises not only

jurisdictional issues but also a broader question concerning the applicability of the traditional defamation law to the Internet context. It also indicates the challenging task faced by the court in striking a correct yet delicate balance between promoting the Internet and providing relief to the plaintiff. The English case would seem to suggest that the general principles of defamation remain the same whatever the medium in which it was published, be it the newspapers or the Internet. This case also suggests that the liability of ISPs would depend on their actual knowledge or means of knowledge of the truth of the statements rather than on the fact that a defamatory posting appeared on their bulletin boards.[82] Moreover, fear of costly litigation might open up the floodgates for UK ISPs to censure their customers' postings. However, given the nature of the Internet, their customers/users (as well as their businesses) may simply go elsewhere where there is little danger of legal action or where they may send defamatory e-mails anonymously.

In the employment context, the conservative English approach would seem to suggest that employers would be under a positive duty to examine publication where defamatory materials are brought to their attention. Additionally, it would appear that employers would be walking on a tightrope. On the one hand, they must exercise some control to show 'reasonable care' but at the same time they should not attempt to do so much as to take them outside the ambit of the defence of innocent dissemination. Having said that, it is apparently prudent that British employers should inform their employees of the need to avoid making defamatory remarks in their e-mails. However, employers should not attempt to filter for defamatory material as this might create liability because they might be deemed to be the 'editor' of the statement. Additionally, employers should take the necessary measure to remove a defamatory e-mail if such matter is brought to their attention or if they reasonably suspects that the e-mail is defamatory.

In contrast, the American approach implies that employers might allow employees to say or post anything and might not curb much current e-mail misuse by employees, as the employers would be immune from liability. However, such an effect would be contrary to congressional intent in creating the Communications Decency Act 1996 that was aimed at protecting ISPs from liability from third party users' conduct. But consequently, American ISPs (and presumably American employers too) need not fear endless legal claims should they fail to monitor every mail and web page that passes through their servers.

Pornographic materials

Many organizations have singled out accessing pornographic websites, downloading pornographic materials and disseminating such materials as the main problem associated with the Internet usage and e-mail. Pornography is believed to be one of the fastest growing [83] and the biggest single problem of Internet misuse at work, even surpassing harassment.[84] For instance, in an Elron Software survey in 1998 of 110 companies with 50 to 15,000 workers found that sexually explicit web sites were accessed at 62 per cent of the companies.[85] However, an International Data Corp study found that 70 per cent of all Internet pornographic traffic in the American workplace occurs during the nine-to-five workdays.[86] Similarly, SexTracker found that about 70 per cent of traffic on popular pornographic sites such as Passion Palace and Planet Love take place during work hours.[87] SexTracker also estimated that one in five white-collar male workers are accessing pornography at work.[88] Yet again, one could not be certain as to the actual magnitude of this problem because software companies selling monitoring software generated these available statistics.

The legal risk associated with pornographic materials is that, since such materials are broadcast or electronically posted at work, many offended employees may claim that their employers are fostering a hostile work environment. Additionally, further damage could result from adverse publicity concerning the improper Internet and e-mail habits of employees. What is worse is that criminal liability may well be attached to employers if their employees were to engage in transmitting and forwarding e-mail with pornographic contents or downloading, distributing or posting such materials on the Internet. This is because the publication of obscene material or possession of such material for publication for gain is a criminal offence.[89] If the material involves an indecent photograph of children, mere possession would be criminal.[90] For liability under the Obscene Publications Act 1959, the article in the e-mail would have to be more than merely sexually explicit; it must show a tendency to deprave or corrupt.

Within the ambit of the 1959 Act, the ‘publication' includes transmission of obscene materials; as such it would include obscene material in the e-mail itself or in the attachments.[91] The intention of the publisher appears to be immaterial. In *R v Fellow*; *R v Arnold* [92] the Court of Appeal explained that a photograph within the meaning of the Protection of Children Act 1978 is a pornographic image downloaded to a bulletin board.[93] It was also held that merely providing the obscene images available for downloading would be sufficient distribution and therefore publication. This case would seem to suggest that storage of the material alone would amount to publication.[94] In a work environment, employers would be liable if it allows obscene materials to be published on the Internet (such as putting it on a web site) or if such material is in the possession of the employer (for instance, storing it on its network drives or Internet cache). However, as a publisher of the material, an employer would have a defence that it has not examined the article and that there was no reasonable suspicion that obscene material of any kind was being distributed using its systems.[95] It would be inadequate for an employer to simply ignore the materials held on its systems. The defence would only apply if he could show that he did not know there was material on his systems that was obscene and that such lack of knowledge was not due to his negligence.

Inappropriate e-mail misuse involving obscenity has resulted in a spate of dismissals for many employees in the UK and the US, which could be due to concern about hostile work environment claims. For example, in what is believed to be the biggest e-mail misuse sacking case in the UK, the mobile phone network operator, Orange, recently dismissed more than forty employees for the ‘distribution of inappropriate materials' via e-mail.[96] However, the most publicized sacking for Internet surfing came in February 2000 when twenty-three employees of the New York Times were sacked for exchanging pornographic materials at work via the e-mail.[97] With respect to Internet misuse, several White House employees were caught downloading pornographic materials and one of them later resigned over the incident.[98] Earlier on, in October 1999, Xerox Corp revealed that their zero-tolerance policy has resulted in the dismissal of at least forty employees for accessing web sites deemed inappropriate at work. Another notable case was the dismissal of twenty employees of Compaq Computer Corporation in 1997 for allegedly distributing pornographic images downloaded from the Internet on the employer's computers.[99]

Inadvertently creating a contract

Just like an ordinary letter, e-mail is capable of creating and varying a contract, either through an intentional or inadvertent act of employee. An employer may be bound by such an act if a third party

reasonably believes that such employee has the ostensible authority to negotiate or to enter into an agreement on behalf of the organization. Although without encryption authentication, the Internet makes it rather difficult to establish who sent an e-mail, it might be reasonable to assume that such authority exists as e-mails provided by an employer are usually identified as originating from the employer.

In the UK, apparent authority and vicarious liability were found to exist in a breach of contract case resulting from e-mail in *Hall v Cognos Ltd*.[100] In this present case the employment tribunal held that e-mail sent by a line manager in positive reply to his subordinate's request to submit a late claim against the company rules might bind the employer. On the issue of whether the e-mail constitutes a document 'in writing and signed by the parties', the tribunal held that once the e-mail was printed out it took on a written form and was signed by the parties as each message contained and printed the name of the sender. Additionally, on the issue of whether the line manager has ostensible authority to agree to a variation of the terms concerning payment of expenses, the tribunal held that the plaintiff was entitled to rely on his line manager's apparent authority to authorize payment for late claims. Hence, the employer was bound by the variation sanctioned by the line manager's e-mail.

Negligent misstatement

Similar issues that apply to contract may also apply to negligent misstatement or advice given via e-mail. The traditional principles that were established in *Hedley Bryne & Co Ltd v Heller & Partners Ltd* [101] might be relevant in determining liability in the Internet context. Therefore, if an e-mail gives an impression, without limitation or disclaimer, that advice or information is considered advice, a plaintiff may be able to rely on such statement to establish a duty of care. It may be sufficient for the plaintiff to show that the defendant could have inferred that the advice was to be relied upon.[102] Therefore, employers should ensure that employees are clear as to what they can do or otherwise, with regard to office e-mail. In addition, employers should consider whether or not appropriate disclaimers should be attached to e-mail messages.

Conclusion

In general, the benefits of using e-mail and the Internet in the workplace outweighs the possibilities for its misuse. However, one cannot underestimate the legal risks to employers when employees are allowed access to the Internet and e-mail. The exposure to such legal liability might be exacerbated by the very nature of e-mail itself, which tends to be more informal and spontaneous, engendering employees to write things they would never say on the telephone or in an ordinary letter. When coupled with the lack of awareness of users/employees as well as employers of the risks involved, they might make a good recipe for increased e-mail misuse and legal vulnerabilities.

However, a survey by QA Research in 1998 on e-mail misuse and its threat to corporate liability among a cross-section of 200 UK business organizations suggests that employers are becoming more concerned of their potential liability through e-mail communication.[103] The fact that many employers (70%) were concerned about inadvertent disclosure of confidential information by employees through e-mail indicates the awareness of the significance of data and information as corporate assets. 66 per cent considered that they were exposed to hacking. 63 per cent of employers are concerned about negligent virus transmission, 60 per cent about negligent advice or misstatement and misuse of personal data by employees. Whilst 52 per cent thought that they were exposed to cyber defamation, 51 per cent felt that

they were liable for sexual or racial harassment claims and 49 per cent thought that they could be bound by contracts inadvertently entered into by their employees. Nonetheless, the survey notes that in many instances little has been done to alleviate these threats and consequently a massive knowledge gap is generated.[104]

In order to address the issue and to correct such imbalance, a tripartite approach should be adopted. This may involve non-legal measures in which a clear code of conduct contained in e-mail and Internet acceptable use policies should be implemented and communicated to the employees.[105] Furthermore, the employees should be educated as to what these appropriate and acceptable uses are.[106] However, such an e-mail policy may not totally limit the potential liability of employers,[107] in particular those that operate their own internal e-mail system because they are deemed to be aware of inappropriate online activities. More efforts would be required on the part of these employers. The fact that it might be almost impossible to know about such wrongful online behaviour due to the bulk of Internet and e-mail traffic on their systems and networks may not bar the plaintiff's claims.[108] For a successful defence against any claims, employers might want to consider using some technological measures to monitor employees' e-mail content and Internet activities.[109] Although employers in the UK would have to adhere to the relevant laws and regulation [110] (Federal and State laws in the USA) in these monitoring exercises such a market or technological solutions might work in the employers' favour in employer liability claims. Such practices, however, raise wider legal issues concerning employee's electronic privacy and the need for legislative control over workplace surveillance.[111]

What is significant is that these combined proactive strategies might not only weed out improper e-mail and Internet activities in the workplace but also minimize employer's exposure to legal liability. More importantly, however, e-mail misuse and the exposure to legal liability arising from such misuse, highlight some of the challenges that many employers are facing, and will continue to face, in dealing with employee online behaviour and in defending themselves against such conduct. Of equal significance is the difficult task ahead of the courts. It is not only problematic to determine the standards they would apply in deciding employer's liability in the context of the Internet and e-mail, but also to balance the interests of promoting the new emerging technologies and in providing remedies to the plaintiffs. Not only that, the world over, the judiciary and the legislative bodies are still grappling with the questions of how the laws of the old unwired world should be applied to the wild reaches of the electronic frontier.

[1] See '300 Million Online by 2005 Asia, South America Leading the way,' available at http://www.cyberatlas.internet.com/big_picture/demographics/data.html, 31 March 1999.

[2] K Girard, 'Hold that thought, IS tells e-mailers', *Computer World*, 21 April 1997.

[3] See D Draycott, 'The Double-Edged Sword of the Net: Turning E-Porn into Productivity' *Computer Fraud & Security* (2000) 6: 11–12.

[4] See http://www.elronsw.com. See also B Leonard,' E-mail @ Work: Ripe for Employee Abuse,' HR Magazine (1999) 44(6): 28.

[5] See Draycott, supra n 3, at p 11.

[6] LL McMurchie, 'E-mail Opens 'Pandora's Box of Vulnerabilities,' *Computing Canada*, 15 January 1999, 25(2): 14-16.

[7] See http://www.bbn.com/aboutbbn/history.htm. See also H Rheingold, 'Why Censoring Cyberspace is Dangerous and Futile' at http://www.com/user/hlr/tomorrow/tomorrowcensor.html

[8] In the United Kingdom the Joint Academic Network (JANET) was established in 1984. See http://www.ja.net

[9] See http://www.cern.ch/

[10] See W Gibson, *Neuromancer*. Harper Collins, London, 1994.

[11] DS Wall, 'Policing The Virtual Community: The Internet, Cyberspace and Cybercrime' in P Francis, P Davies and V Jupp (Eds) *Policing Futures*, Macmillan, London, 1997. See Byasee, 'Jurisdiction in Cyberspace: Applying Real World Precedent To The Virtual Community,' 30 *Wake Forest Review* (1995): 197. See also L Lessig, 'The Zones of Cyberspace,' *Stanford Law Review* (1996): 1403.

[12] DS Wall (1997), *ibid*. at p 106.

[13] M McLuhan, *Understanding Media: The Extensions of Man Routledge*, London, 1964.

[14] DS Wall (1997), supra n 12.

[15] A Giddens, *The Consequences of Modernity*, Polity Press, London, 1990

[16] A Giddens, *ibid*. See also A Bottom and P Wiles, 'Understanding Crime Prevention in Late Modern Societies,' in T Bennett (ed.), *'Preventing Crime and Disorder: Targeting Strategies* and *Responsibilities*', University of Cambridge, Cambridge 1996. DS Wall (1997) *supra*, n.12

[17] See J Araneo, 'Pandora's (E-mail) Box: E-mail Monitoring in the Workplace,' *Hofstra Labour Law Journal* (1996) 14: 339-364. See also P Brown, 'Developing Corporate Internet, Intranet and E-mail Policies,' *PLI/P* at (1998) 520: 347.

[18] DH Seifman and CW Trepanier, 'Evolution of the Paperless Office: Legal Issues Arising Out of Technology in the Workplace,' *Employee Relations LJ* (1995) 21(3): 5-36.

[19] P Brown, *supra*, at n 10, at p 350-351.

[20] H Adams, S M Scheuing & SA Feeley, 'E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly,' *Defence Counsel Journal* (2000) 67(1): 32-46.

[21] DS Wall, *supra*n 11.

[22] JP Barlow, 'The Economy of Ideas: A Framework for Rethinking Patents and Copyrights in the Digital Age, *Wired*, 1994 2(3): 84. See also J Boyle, *'Shamans, Software and Spleens: Law and the Construction of the Information Society*', Cambridge, Mass.: Harvard University Press, 1996.

[23] M Castells, 'The Rise of the Network Society', Cambridge, Mass.: Blackwell, 1966. He argues that in contrast to the earlier industrial societies, the network society has begun to organize itself around 'the technology of knowledge generation, information processing and symbol communication.'

[24] [1972] AC. 153.

[25] See ibid. at p 170.

[26] See for example *Broom v Morgan* [1953] 1 QB 597.

[27] L Harnden, 'A Risky Business: Liability of Employers for the Wrongful Acts of Their Employees' (2000) available at http://www.emond-harnden.com.

[28] See [1997] IRLR 168.

[29] (1949) 79 CLR. 370.

[30] See ibid. at p 378.

[31] [1963] 1 WLR 991.

[32] [1976] 1 All ER 97.

[33] [1942] 1 All ER 491.

[34] (1992) 25 NSWLR. 715

[35] (1919) 26 CLR. 110 at 117.

[36] RB Mawrey and KJ Salmon, *Computers and the Law*, Oxford, BSP Professional Books, 1988, at p 125.

[37] [1961] 1 All ER 74.

[38] See ibid, per Diplock J at 77.

[39] T Gole and T Hughes, 'Employer Liability for Employee Use of the Internet,' *Computer & Telecommunication Law Review* (1999) 5(2): 35-42, at p 36.

[40] In the UK there is no statutory definition of harassment. Industrial tribunals and appeal courts have occasionally resorted to the persuasive authority of the *European Commission's Recommendations and Code of Practice of the Dignity of Women and Men at Work 1991*. Here, sexual harassment is defined as 'physical, verbal or non-verbal conduct of a sexual nature or other conduct based on sex affecting the dignity of women and men at work' and such conduct is unacceptable if 'unwanted, unreasonable and offensive to the recipient'. Also, such conduct 'creates an intimidating, hostile or humiliating working environment for the victim.'

[41] M Betts and J Maglitta, 'IS Policy Target E-mail Harassment,' *Computer World*, 13 February 1995, at p 12.

[42] E-mail harassment has received much attention in the USA. For example, see DK McGraw, 'Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail,' *21 Rutgers Computer & Tech. LJ* (1995) 491. See also Barton, 'Taking a Byte out of Crime: E-mail Harassment and the Inefficiency of Existing Law,' Wash L Rev (1995) 465. See ES Ross, 'E-mail Stalking: Is Adequate Legal Protection Available?' 13 J *Marshall J Computer & Info L* (1995) 405.

[43] Available at http://www.anonymiser.com

[44] See GG Mathiason 'Selected Employment Law Implication' in *Practical E-Law Recommendations for Networked Employers* (1999) available at http://www. prof.findlaw.com/networked/networked_2.html

[45] See *Jones v Tower Boot* [1997] IRLR. 168. See also *Burton and Rhule v De Vere Hotels* [1996] IRLR. 596.

[46] MS Dichter and MS Burkhardt, 'Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communication in the Internet Age,' (1999) available at http://www.mlb.com/art61499.htm and at http://www.mlb.com/speech1.htm

[47] Section 41(3) of the Sex Discrimination Act 1975. *Balgobin & Francis v London Borough of Tower Hamlets* [1987] IRLR 401. See also J Whelan, ' *E-mail @ Work'.* Harlow: Pearson Education Limited, 2000, at p 104.

[48] M Hart, 'Corporate Liability for Employee Use of the Internet and E-mail: Steps to Take to Reduce the Risks,' *Computer Law and Security Report* (1998) 14(4): 223-231, at p 225.

[49] 928 F Supp 533 (ED Pa 1996)

[50] 1998 WL 166845 (N.D.N.Y.)

[51] See M S Dichter and M S Burkhardt (1999) *supra* n 46.

[52] See ibid.

[53] A Soden, 'Protect Your *Corporation From E-mail Litigation,' Corporate Legal Times* (May 1995) at p 19.

[54] (North) Employment Tribunal (22/10/96, Case No 5471/95).

[55] No 19 Civ 5928, 1995 WL 326492, at p 5 (SDNY 1995).

[56] Sections 1 and 4 of the Race Relations Act 1976.

[57] Section 32 of the Race Relations Act 1976.

[58] See *Jones v Tower Boot Co Ltd* [1997] IRLR 168, supra at n 45. See also *Burton & Rhule v De Vere Hotels* [1996] IRLR 596.

[59] Section 32(3) of the Race Relations Act 1976.

[60] 1999 WL 224603 (EDNY).

[61] 1998 WL 91261 (ND Tex)

[62] 1997 WL 793004 (SDNY)

[63] P Mendels, 'E-mail abuse leads to firings at investment firm,' *The New York Times*, 14 May 1999 available at http://www.nyt.cyberlawjournal

[64] See *Sim v Stretch* [1936] 2 All ER 1237.

[65] J Whelan, (2000), *supra* at n 47.

[66] See *Lloyd v Grace Smith* [1912] AC 716.

[67] (1862) 1 H&C 526.

[68] *Rindos v Hardwick* (unreported, Supreme Court of Western Australia, 31 March 1994) suggests that the fact that anyone connected to the Internet could have read the posting on the Usenet newsgroup 'sci.anthropology' may be sufficient publication. See http://www.law.auckland.sc.nz/cases/Rindos.html

[69] Abbreviation for File Transfer Protocol, referring to both the programs that transfer files from one computer to another across the Internet, as well as the technical standards it uses.

[70] See J Sullivan, 'Sticks and Stones on the Net,' (1998) available at http://www.wired.com/news/news/business/story/16059.html

[71] (Unreported, 1998).

[72] See 'Research on Coping with E-mail and Internet Risks,' *SCL Electronic Magazine*, Aug./Sept. 9 (4) available at http://www.scl.org

[73] J Warchus, 'E-Defamation: The Atlantic Divide Grows Wider,' *Computer Law & Security Report* (2000) 16(4): 261-262.

[74] C O'Blenes, 'Tangling With Technology,' *Management Review* (1999) 88(4): 52-54. See also DH Seifman and C.W. Trepanier (1995) supra at n 18.

[75] CO' Blenes, ibid., at p 52. See also DH Seifman and CW Trepanier, ibid., at p 19. See M Stepanek, 'When the Devil is in the E-mail: Casual Messages Can Come Back to Haunt You in Court,' *Business Week* (8 June 1998): 72.

[76] (Unreported, 1999).

[77] D Eviatar, 'Cyber-harassment: Sticks and Stones Hurt Online' *Corporate Counsel*, August 10 (2000) available at http://www.infowar.com and http://www.tm0.com/sbct.cgi?s=60409626&I=231179&d=362257

[78] Ibid.

[79] See MP Gallagher, 'Worker Slurred by Peers Online May Sue Employer,' (2000) available at http://www.law.com.

[80] WL 999836 (NYAD 2 Dept.). The court confirmed earlier decisions in *Zeran v America* Online 129 F 3d 327 (4th Cir 1997) and *Blumenthal v Drudge* 992 F Supp 44 (DDC 1998). See also *Cubby Inc. v CompuServe Inc.* 776 F Supp 135 (1991). Cf. *Stratton Oakmont Inc. v Prodigy Services Co* 1995 WL 323710 (NY Sup Ct 24 May 1995).

[81] [1999] 4 EMLR 542.

[82] See T Keinan, 'A Web of Lies,' *Computer Law & Security Report* (2000) 16(4): 263-265, at p 264.

[83] See for example, L Berg, 'Employers must guard against electronic workplace abuses,' (2000) available at http://www.bizjournals.com/southflorida/stories/2000/05/08/focus3.html.

[84] See for example D. Plotnikoff, 'Liability-wary employers look over shoulders of web users,' (2000) available at http://www.seattletimes.com/technology

[85] Ibid.

[86] See M Frazier, 'Web users under watchful eye,' (2000) available at http://www.bizjournals.com/cincinnati/stories/2000/04/24/story2.html.

[87] See M Conlin, 'Worker, Surf at Your Own Risk,' (2000) available at http://www.businessweek.online.com_files/b3685257.html.

[88] Ibid.

[89] See Obscene Publications Act 1959, s 2.

[90] See Protection of Children Act 1978, s 7.

[91] Obscene Publications Act 1959, s. 1(3). As amended by the Criminal Justice and Public Order Act 1994, s 168 and Sch 9.

[92] Unreported, Court of Appeal, 27 September 1996.

[93] The term 'photograph' has been defined in the Criminal Justice and Public Order Act 1994 as including 'data stored on a computer disk or by other electronic means which is capable of conversion into a photograph.' This would cover digital graphic images.

[94] See also *R v Pecciarich* (1995) 22 OR (3d) 748 at 765.

[95] Obscene Publications Act 1959, s 2(5).

[96] See J Wakefield, 'Orange sacks forty over Internet porn,' (2000) available at http://www.zdnet.Couk/news/2000/34/ns-17649.html.

[97] See J Wakefield, '23 sacked for e-mail abuse,' (2000) available at http://www.zdnet.couk/news/1999/48/ns-11945.html.

[98] See http://www.zdnet.couk/news/2000/31/ns-17244.html.

[99] See 'Employee Internet Use: Big Brother Gets Involved,' *New York LJ*, 17 March 1997.

[100] Hull Employment Tribunal (17.2.98 Case No 1803325/97).

[101] [1963] 2 All ER 575. See also *Caparo Industries plc v Dickman* [1990] 1 All ER 568.

[102] See C Gringras, *The Laws of the Internet*, Butterworths, London, 1997, at p 83.

[103] See 'Cyberliability Gap Opens Wider in UK' available at http://www.newsbyte.com.

[104] See ibid.

[105] A Bequai, 'Romancing the Internet and Management's Quagmire,' *Computers & Security* (2000) 19: 591-595. See M Hart (1998) supra n. 48. See also MD. Scott, 'Liability in Cyberspace –111: Creating a Corporate Internet Acceptable Use *Policy,' Computer Law & Security Report* (1997) 13(6): 451- 453.

[106] C O'Blenes (1999), supra n. 74.

[107] N Miller, 'E-mail Abuse and Corporate Policies,' *Network Security* (April 1999): 13-17.

[108] See JS Nowak, 'Employer Liability for Employee Online Criminal Acts,' Federal Comm. LJ (1999) 51: 467-490 available at http:// www.law.indiana.edu/fclj/pubs/v51/no2/nowakmac.pdf.

[109] See JJ White, 'E-mail @Work.Com: Employer Monitoring of Employee E-mail,' Alabama LR 48(3): 1079 available at http://www.boots.law.ua.edu/lawreview/whitfull.html. See J Araneo supra n. 18. See also R. Dixon, 'With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age, 'J of Technology Law & Policy (1998) 4(1) available at http://www.journal.law.ufl.edu/~techlaw/4/Dixon.html. See LON Gantt, 'An Affront to Human Dignity: Electronic Mail Monitoring in the Private workplace', Harvard JL & Tech. (1995) 8(2): 345.

[110] A Hamilton, 'E-mail: Restrictions on Employers' Snooping,' Computers & Law (1997): 5-7.

[111] M Ford provides an excellent review of workplace surveillance in Surveillance and Privacy at Work, Inst. of Employment Rights, London, 1999. See also LT. Lee, 'Watch Your E-mail! Employee Monitoring and Privacy Law in the Age of the 'Electronic Sweatshop,' J Marshall L Rev (1994) 28: 139. See: The Human Rights Act 1998 will have an impact on employers' ability to monitor employee's e-mail. See Art. 8(1) of the European Convention of Human Rights. See also The Regulation of Investigatory Powers Act 2000, The Data Protection Act 1998 and its Code of Conduct, which now govern monitoring and interception of employees' e-mail in the UK.

End of Document