



Misuse of Internet Access by Employees

John Lambert, Yatoni Cole-Wilson and Joanne Gretton
Barristers

IBA, SBL Barcelona, Committee P

28th September 1999

Lancaster Buildings
Northern Intellectual Property Chambers
77 Deansgate
Manchester
United Kingdom
M3 2BW
Tel +44 (0)161 661 4444
Fax +44 (0)161 661 4445
URL www.LBNIPC.com
Clerk's Email: Sandra@LBNIPC.com

Contents

1	Introduction	2
2	The Risks to Business of Allowing <i>Internet</i> Access	2
3	Potential Liabilities of Employers	3
	3.1 Possession and Dissemination of Pornographic Material	4
	3.2 Data Protection Legislation	6
	3.3 Discrimination	10
	3.4 Infringement of Intellectual Property	11
	3.5 Defamation	12
	3.6 Other Liabilities	13
4	Possible Legal Remedies	14
	4.1 The Implied Terms of the Employment Contract	14
	4.2 Convention Rights	15
	4.3 Transfer of Data Abroad	16
	4.4 Civil Procedure Rules	17
	4.5 Proceedings against Internet Service Providers	18
5	Need for an Information Handling Policy	19

1. Introduction

Since the value of transactions over the medium is expected to grow to €3 billion a year by 2002¹ in Europe alone, no business can afford to ignore the *Internet*. Yet every business that accesses that medium incurs some risk. As a recent Irish report observed:

"The *Internet* allows the same ease of expression to evil as it does to good. In fact it can be argued that with its relative anonymity and global dimensions, it facilitates the full expression of our darker side than any other communication medium so far."²

A coherent, corporate information handling policy enables businesses to participate in electronic commerce while containing those risks.

2. The Risks to Business of Allowing *Internet* Access

There are many ways in which a company can be harmed by employee access to the *Internet*. Hacking is perhaps the most obvious risk since 70% of all hackers come from the organization under attack,³ but loss can be sustained even without malice or fraud. For instance, goodwill may be eroded by customer service staff chatting on IRC⁴ to people on the other side of the world instead of answering enquiries and telephone bills run up by employees surfing in company time. In one extreme case that came before the employment tribunal the applicant had visited 150 websites in her employer's time in order to book a holiday.⁵ It has been estimated that the average time that an employee spends on surfing the net for his or her own purposes is 30 minutes a day costing British business £2.5 million per year.⁶ *Worldtalk Corporation ("Worldtalk")*,⁷ a company that supplies content security and policy management solutions, estimated in March 1999 that 31% of all emails endanger

¹ Per Robert Verrue, Director General Directorate-General XIII - European Commission "Electronic Commerce in Europe: The Present Situation" Seminar on Electronic Commerce, Kangaroo Group, European Parliament, Brussels, 20 January 1999.

² "Illegal and Harmful Use of the Internet" First Report of the Working Group of the Ministry of Justice, Stationery Office, Dublin, 1998.

³ "The Enemy Within" 2nd December 1998 PC Dealer Net (www.vnu.net)

⁴ "*Internet Relay Chat*" a real time messaging system

⁵ *Franxhi v Focus Management Consultants Ltd* (unreported) mentioned in James Lipson "*Surfers Beware*" Computer Contractor 30th July 1999 (available from www.vnunet.com).

⁶ Jan Howells "Net surfers wasting time and money at work" (reporting on a survey of 191 large international companies by InfoSec), News Wire 12th April 1999 (also at www.vnunet.com).

⁷ "Worldtalk releases first Internet email corporate usage report; concludes e-mail abuse at epidemic levels" 29th March 1999 (www.worldtalk.com/corporate%20Information/press%20releases/iecur.htm).

corporate information assets, employee productivity or messaging systems. Its breakdown of that statistic was as follows:

- 10% of all emails are unsolicited commercial communications (otherwise known as "spam")
- 9% disclose confidential information, are defamatory or otherwise unlawful
- 4% are bulk mail
- 4% contain profanities
- 2% carry jokes⁸ and
- 2% spread viruses.

Despite those risks relatively few companies in the United Kingdom restrict their employees use of the *Internet*.⁹ That may be explained by the fact that there may be some advantages for employers in allowing their employees to make some use of the net for their own purposes. Someone who learns how to navigate the web for fun does not have to be trained how to use it in his or her job so training costs can be saved. Because some extraneous use of *Internet* access is tolerated, employment tribunals have delivered apparently contradictory decisions on whether downloading pornography in company time constitutes gross misconduct justifying immediate dismissal. In one case, *Humphries v V H Barnett & Co.*¹⁰ the tribunal held that it did, but in another, *Dunn v IBM United Kingdom Ltd.*,¹¹ the tribunal held that it was unfair for an employer to dismiss its employee for this conduct in the absence of an express prohibition against downloading such material.

3. Potential Liabilities for Employers

It is in the interests of employers to regulate *Internet* access because they may incur criminal or civil liability for the wrongdoing of their employees under various statutes and at common law. The areas in which they are perhaps most at risk include:

- possession or dissemination of pornography

⁸ It is assumed that this category refers to insulting or other jokes in bad taste rather than harmless pleasantries.

⁹ *InfoSec* found that 84% of its sample of 191 large multinationals allowed their employees free rein (see Jan Howells "Net surfers wasting time and money at work").

¹⁰ (Unreported) mentioned in James Lipson "*Surfers Beware*" *Computer Contractor* 30th July 1999.

- breach of the data protection principles
- breach of contractual and statutory obligations to female, ethnic minority and other groups of employees
- infringement of copyright, trade marks and other intellectual property rights and breach of confidence
- defamation, and
- other wrongdoing or breach of contract.

3.1 Possession and Dissemination of Pornographic Material

There are three statutes under which prosecutions relating to pornographic material in digital form have been brought in England and Wales:¹²

- the Obscene Publications Act 1959 as amended by Obscene Publications Act 1964 and the Criminal Justice and Public Law Act 1994;
- the Protection of Children Act 1978 also amended by the Criminal Justice and Public Law Act 1994; and
- the Video Recordings Act 1984.

It is also an offence at common law to outrage public decency.¹³

It is an offence under section 2 (1) of the Obscene Publications Act 1959 to publish an obscene article, whether for gain or otherwise, or to possess an obscene article for publication for gain, whether for the person possessing it or for another. An "*article*" means

"any description of article containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures".¹⁴

An article is deemed to be obscene

"if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied."¹⁵

¹¹ *Ibid*

¹² Scotland and Northern Ireland have their own legislation to which separate reference should be made

¹³ *R v Gibson* [1990] 3 WLR 595

¹⁴ Section 1 (2)

¹⁵ Section 1 (1)

Publishing means distributing, circulating, selling, letting on hire, giving or lending or offering for sale or hire¹⁶ or, in the case of an article containing or embodying matter to be looked at or played, showing, playing or projecting it.¹⁷ The Criminal Justice and Public Law Act 1994 has extended the definition of "*publishing*" to include storing data electronically and transmitting that data.¹⁸ The Court of Appeal held in *R v Fellows*¹⁹ that these provisions were sufficient to uphold the conviction of a computer expert who had stored digital images of children in various indecent poses that he made available over the *Internet* to certain individuals to whom he had issued a password. The Court rejected the defendant's submission that the dissemination of material over the *Internet* had not been contemplated by Parliament when it enacted the legislation in 1959. It endorsed Lawton LJ's observation with regard to video cassette recordings its earlier decision in *Attorney General's Reference (No. 5 of 1980)*²⁰ that if the clear words of the statute are sufficiently wide to cover the kind of electronic device with which we are concerned in this case, the fact that the particular form of electronic device was not in the contemplation of Parliament in 1959 is immaterial.

Parliament has enacted special legislation to suppress child pornography. It is an offence under section 1 (1) of the Protection of Children Act 1978

- "(a) to take, or permit to be taken, any indecent photograph of a child²¹ ; or
- (b) to distribute or show such indecent photographs; or
- (c) to have in his possession such indecent photographs, with a view to their being distributed or shown by himself or others

and a person is to be regarded as distributing an indecent photograph if he parts with possession of it to, or exposes or offers it for acquisition by another person.²² References to an "*indecent photograph*" include an indecent film or a copy of an indecent photograph comprised in a film²³ and a *film* includes any form of video recording.²⁴ Section 84 (2) (b) of the Criminal Justice and Public Law Act 1994 has inserted the words "*or pseudo-photograph*"

¹⁶ Section 1 (3) (a)

¹⁷ Section 1 (3) (b)

¹⁸ Schedule 9

¹⁹ [1997] 2 All ER 548, (1997) 1 Cr. App R 244; [1997] Crim. LR 524

²⁰ 72 CAR 71, 74

²¹ A person under the age of 16 for the purposes of this Act.

²² Section 1 (2)

²³ Section 7 (2)

²⁴ Section 7 (5)

after paragraphs (a), (b) and (c) of section 1 (1) of the 1978 statute mentioned above.

Section 84 (4) (b) has expanded the definition of "*photograph*" to include

"data stored on a computer disc or by other electronic means which is capable of conversion into a photograph"

and section 84 (7) has defined "*pseudo-photograph*" as:

"an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph."

The Court of Appeal held in *Fellows*²⁵ that a digital image stored on the hard disc of a computer or other magnetic or optical media is a copy of a photograph for the purposes of the 1978 Act. Section 1 (1) was contravened by storing scanned images of indecent photographs of children and allowing others to download those images upon insertion of a password.

The Video Recordings Act 1984 does not suppress the dissemination of sexually explicit video recordings but requires them to be accompanied by a classification certificate.²⁶ As the Divisional Court remarked in *Meechie v Multi-Media Marketing (Caterbury) Ltd.*,²⁷ it is quite unnecessary that such images should be regarded as hard pornography or even, indeed, as offensive to fall within the ambit of this section. A video recording is defined so as to include "any disc or magnetic tap containing information by the use of which the whole or part of a video work may be produced." Thus the Court held in *Meechie* that a computer game that rewarded a successful content with an animation of a semi-naked female in a suggestive pose required a classification certificate and that the Medway justices had been wrong to dismiss a prosecution by local trading standards officers for distributing the game without such a certificate.

3.2 Data Protection Legislation

Although Parliament passed the Data Protection Act 1998²⁸ on the 16th July 1998 to implement the Data Protection Directive²⁹ (which should have been in force by the 24th

²⁵ [1997] 2 All ER 548, (1997) 1 Cr. App R 244; [1997] Crim. LR 524

²⁶ Section 9

²⁷ [1996] EGCS 135. The Times 26th April 1995

²⁸ 1998 C 29

October 1978) it is not yet law. The present legislation is the Data Protection Act 1984 which prohibits processing of personal data³⁰ without registering with the Data Protection Registrar either as a "data user" or as a "data user who also carries on a computer bureau."³¹ The Registrar can refuse to register a data user if she is satisfied that the user is likely to contravene certain principles on the proper handling of personal data (known as the *data protection principles*³²) or if the information available to her is insufficient to satisfy her that the applicant is unlikely to contravene those principles.³³ She can require a registered data user to take specified steps if satisfied that the user has contravened or is contravening one or more of those principles by serving an enforcement notice³⁴ or remove him from the register altogether in those circumstances.³⁵ *Data subjects* (that is to say individuals identified by such personal data) can bring proceedings in the civil courts for injunctions and compensation against data holders who deny them access to their data³⁶ or who cause them damage and distress by holding inaccurate data³⁷ or losing, destroying or allowing unauthorized access to such data.³⁸

There has not been very many cases under this Act either in the civil or criminal courts or in the tribunal that hears appeals from the Registrar's decisions³⁹ but one which illustrates the potential liability of employers is *British Gas Trading Ltd. v Data Protection Registrar*.⁴⁰ In that case, an employee of a public utility wrote a letter to a local authority public housing department in the following terms:

²⁹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

³⁰ Section 1 (3) defines "*personal data*" as "data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intention of the data user in respect of that individual."

³¹ Section 5 (1)

³² Section 7 (2) (b)

³³ Section 7 (2) (c)

³⁴ Section 10 (1)

³⁵ Section 11 (1)

³⁶ Section 21 (8)

³⁷ Section 22 (1)

³⁸ Section 23 (1)

³⁹ The Data Protection Tribunal established by section 3 (1) (b) of the Act.

⁴⁰ Unreported, Data Protection Tribunal, 24th March 1999 (available from the Data Protection Registrar's website at www.dataprotection.gov.uk/bgtl.htm).

"I am responsible for the tracing of our customers when they leave a property without providing us with a forwarding address ...I am aware that this is a sensitive area and that absolute discretion will be necessary in any arrangement. However, I am confident that a properly controlled exchange of information ...would be beneficial to both our departments. This scheme has been set up in other areas of Britain and has proven to be very successful to both parties."

This letter came to the notice of the Registrar who issued an enforcement notice against the utility. The Tribunal upheld the notice notwithstanding prompt action by one of the utility's directors to put a stop to the practice and undertakings to prevent its recurrence.

The Data Protection Act 1998 will apply eventually to certain manual records as well as computer files⁴¹ and will require virtually everyone who controls personal data to notify particulars of his processing with the Data Protection Commissioner (as the Registrar will then be known⁴²).⁴³ It will be an offence to process personal data without outside the scope of the notification.⁴⁴ New data protection principles will be in force:

Old Principles	New Principles
1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.	1. Personal data shall be processed fairly and lawfully. In particular, data shall not be processed unless at least one of a number of specified conditions is met in any case. In the case of sensitive data, at least one of a number of other specified conditions must also be met.
2. Personal data shall be held only for one or more specified and lawful purposes.	2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.	3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.	4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data shall be accurate and, where necessary, kept up to date.	5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.	6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

⁴¹ Section 1 (1)

⁴² Section 6 (1)

⁴³ Section 16 (1)

⁴⁴ Section 17 (1)

<p>7. An individual shall be entitled-</p> <p>(a) at reasonable intervals and without undue delay or expense-</p> <p>(i) to be informed by any data user whether he holds personal data of which that individual is the subject; and</p> <p>(ii) to access to any such data held by a data user; and</p> <p>(b) where appropriate, to have such data corrected or erased.</p>	<p>7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.</p>
<p>8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.</p>	<p>8. Personal data shall not be transferred to a country or territory outside the European Economic Area (“the EEA”)⁴⁵ unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.</p>

Data subjects' rights under the 1984 Act were enforced mainly by the Registrar. Although the Commissioner continues to be entitled to bring proceedings in her own name in a matter of public importance, she has made it known that it will usually be up to data subjects to enforce their rights by private action.⁴⁶ Generally, the new Act will be at least as demanding as the old and any conduct that was actionable under the old law will continue to be such under the new.

Finally, the Telecommunications Data Protection Directive⁴⁷ will be implemented in the United Kingdom by The Telecommunications (Data Protection and Privacy) Regulations 1999⁴⁸ with effect from the 1st March 2000. Part of the directive is already implemented with amendments by The Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998.⁴⁹ The 1999 regulations deal mainly with telephony services but restrictions on the use of telecommunications services for direct marketing⁵⁰ and the security of telecommunications systems⁵¹ impact on electronic commerce. These

⁴⁵ The European Union plus Iceland, Liechtenstein and Norway

⁴⁶ Paragraphs 8.2 and 8.3 of the Consultation Paper on the EC Data Protection Directive published on the Registrar's website (www.dataprotection.gov.uk).

⁴⁷ Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. OJ L024, 30.01.1998 pa 1 to 8 (www.europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html)

⁴⁸ SI 1999 No 2093

⁴⁹ SI 1998 SI 3170

⁵⁰ Part V

⁵¹ Part VI

regulations also create rights of action that are enforceable by data subjects⁵² as well as by the Commissioner.⁵³

3.3 Harassment and Discrimination

While there has been nothing like the *Chevron case*, where a subsidiary of the Chevron Corporation agreed to pay substantial contribution to female staff who had been hurt by an email circulated round the company that compared women unfavourably to beer,⁵⁴ there is reason to suppose that a similar case would be decided the same way in the United Kingdom. Employers have been held liable for exposing their staff to racial abuse and sexual harassment. In *Burton and another v De Vere Hotels Ltd.*,⁵⁵ for example, two black waitresses recovered damages from their employer under section 4 (2) (c) of the Race Relations Act 1976 for being subjected to racist jokes at a reception addressed by an entertainer not known for commitment to racial harmony. Although the employer was in a delicate position in that it had no direct control over the conduct of the guests or the remarks of their speaker, the judge held that the hotel should have warned the staff to be on the look out for the speaker and to have withdrawn them when things became unpleasant. That decision was followed by *Chessington World of Adventures Ltd. v Reed*⁵⁶ where the employer failed to take adequate steps to prevent victimization of a transsexual maintenance mechanic by her colleagues after it had become aware of her harassment. The treatment to which she had been subjected included repeated theft of her tools and coffee mugs, refusal to work with her or to assist her with heavy lifting, verbal abuse, defacement of her clothing and other property with lipstick, leaving tampons, sanitary towels and a replica coffin inscribed with her name and the letters 'RIP' on her workbench and informing her that a 'book' had been taken out by her colleagues and that they had saved up to £100 to pay to anyone who succeeded in having her seriously injured or dismissed. In addition to its statutory duties, an employer may be liable for constructive dismissal if it fails to take steps to prevent embarrassment to its

⁵² Regulation 35

⁵³ Regulations 36 and 37

⁵⁴ For a discussion of the case, see the article by Mark S Dichter and Michael S Burkhardt "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age" read to the Fourth Annual Conference of The American Employment Law Council at Asheville, North Carolina, USA (2nd to 5th October 1996).

⁵⁵ [1996] IRLR 596

staff. An example of such a case is *Morse v Future Reality Ltd.*⁵⁷ where a female employee resigned after male colleagues had upset her by downloading pornographic materials from the *Internet*. In view of the finding in a report sponsored by *Novell UK*⁵⁸ that women are most likely to feel upset, angry, stressed frustrated or helpless after receiving an offensive email, employers should not be surprised by sexual harassment or constructive dismissal proceedings in a *Chevron* situation.

3.4 Infringement of Intellectual Property Rights

Just about every type of copyright work except perhaps *models* for buildings within the meaning of section 4 (1) (c) of the Copyright, Designs and Patents Act 1988 and *published editions* within the meaning of section 8 (1) may be digitized, stored on magnetic or optical media and disseminated over the *Internet*. Any such digitization, storage on an employer's computer or dissemination by one or more of its employees without the licence of the copyright owner other than the acts permitted by Chapter III is a primary infringement of the copyright subsisting in the work.⁵⁹ Although downloading from a website, printing a reasonable number of copies for personal use and storage on a computer are usually licensed in the absence of a specific prohibition, dissemination of copies over the *Internet* is not. Software is usually supplied over the *Internet* under click-wrap licences. Copyright in a computer program downloaded from a website outside the scope of an express licence is also infringed by loading and running it on a computer.⁶⁰ Ignorance on the part of the employer of a primary infringement by an employee is immaterial to liability. Copyright is secondarily infringed by importing,⁶¹ possessing in the course of business,⁶² selling, letting for hire, offering or exposing for sale or hire,⁶³ exhibiting or distributing in the course of business or otherwise to such an extent as to affect prejudicially the owner of the copyright any copy of a copyright work that the employer knows or has reason to believe to be an infringing copy.

⁵⁶ [1997] IRLR 556

⁵⁷ (Unreported) discussed in James Lipson "Surfers Beware" Computer Contractor 30th July 1999.

⁵⁸ "Shaming, Blaming and Flaming: Corporate Miscommunication in the Digital Age" Firefly Communications, London.

⁵⁹ Section 16 (1)

⁶⁰ Section 17 (2)

⁶¹ Section 22

⁶² Section 23 (a)

The remedies for copyright infringement are draconian. In addition to injunctions, orders for delivery up and forfeiture of infringing copies and the equipment for making such copies, accounts and damages the courts have power to order additional damages if by reason of the flagrancy of the infringement and the benefit accruing to the defendant the justice of the case so requires.⁶⁴ Making, importing, possessing in the course of business,⁶⁵ selling, letting for hire, offering or exposing for sale or hire,⁶⁶ exhibiting or distributing in the course of business or otherwise to such an extent as to affect prejudicially the owner of the copyright any copy of a copyright work that the employer knows or has reason to believe to be an infringing copy is also an offence under section 107 (1) of the 1988 Act. Other intellectual property infringements for which an employer may incur liability from the acts of its employees include infringement of the rights of an actor, ballet dancer, musician, singer or other performer in his or her performance by unlicensed copying, storage and dissemination of films, plays, concerts, ballets or other performances, infringement of database rights by unlicensed abstraction and dissemination of the contents of a database and infringement of trade marks by counterfeiting a software package, database or other digital work. It should not be forgotten that employers may sustain an infringement of their own, as well as infringe others', intellectual property. Many of the 9% of emails that WorldTalk included in the "unlawful" category disclosed confidential or proprietary information to strangers or disseminated software or other copyright works without proper authority.⁶⁷

3.5 Defamation

Corporate vulnerability for employees' emails was first brought home to employers when *Norwich Union* was forced to pay substantial damages to *Western Provident* in compensation for certain unguarded remarks about Western which a Norwich manager circulated to a number of colleagues. There is, as Morland J remarked in *Godfrey v Demon Internet Ltd.*⁶⁸ "a substantial divergence of approach between English and American defamation law" as a

⁶³ Section 23 (b)

⁶⁴ Section 97 (2)

⁶⁵ Section 23 (a)

⁶⁶ Section 23 (b)

⁶⁷ "Worldtalk releases first Internet email corporate usage report; concludes e-mail abuse at epidemic levels" 29th March 1999 (www.worldtalk.com/corporate%20Information/press%20releases/iecur.htm).

result of the impact of the First Amendment to the United States Constitution. In England, for example, the publisher of a libel has to prove that he was innocent whereas in America it is for the claimant to prove that he was not.⁶⁹ It is possible that English law may converge with American law as a result of the incorporation of the European Convention of Human Rights into English law. Article 10 (1), like the first amendment, guarantees freedom of expression including freedom to receive and impart information and ideas without interference by public authority and regardless of frontiers. On the other hand, that freedom is subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society for the protection of the reputation or rights of others and for preventing the disclosure of information received in confidence.

3.6 Other Liabilities

There are many other ways in which an employer could incur liability to third parties as a result of the acts or defaults of its employees. Breach of a contract to acquire or supply information or services on-line is one obvious possibility and negligence in supplying those services is another. At some stage *Internet* transactions are likely to be taxed and suppliers may find themselves liable not only to their own fiscal authorities but also those of other countries on the basis that they carry on business there. Even in the United States, which has campaigned for a moratorium of electronic taxation, such liability would not be an enormous leap beyond the decision of the Supreme Court in *International Shoe Co. v Washington*.⁷⁰ Another possible hazard is legislation to protect national languages and culture. According to an excellent, recent article in the *Computer Law Association Bulletin*,⁷¹ an American University, which advertised on its English language website courses in France in association with its French campus and two local companies, was prosecuted under laws that required advertisements to appear in French. The proceedings failed only on procedural grounds and the prosecutors have appealed. The authors noted that a similar prosecution had been threatened in Montreal against a local retailer who had advertised only in English in

⁶⁸ Unreported, Queen's Bench Division, 26th March 1999

⁶⁹ Per Morland J

⁷⁰ 326 U.S. 310 (1945)

⁷¹ Claudia Ray and Dale Cendali "The Internet and Jurisdiction: The International Experience" (1999) 14 CLA Bulletin page 43.

contravention of provincial language laws. Liability under national and supra-national anti-trust and anti-monopoly laws is yet another possibility as electronic commerce matures. The scope for liability is probably limitless.

4. Possible Legal Remedies

4.1 The Implied Terms of the Employment Contract

The implied terms of an employee's contract of employment provide some ground rules for regulating employee's access to the *Internet*. An employee owes his or her employer implied duties of loyalty, service and obedience⁷² just as an employer owes his or her employee an implied duty of reasonableness.⁷³ Strictly the implied obligations of an employee would preclude any access to the *Internet* for purposes other than the employer's business since an employer is entitled to expect the employee to give of his best in company time. On the other hand, zealous enforcement of such obligation would conflict with the employer's obligation of reasonableness. It would be manifestly reasonable, for example, to object to an employee's consulting a railway timetable website or emailing his wife to say that he will not be home for dinner if he is obliged to work late. Employees need to break from time to time and a few minutes harmless surfing to check a cricket score is no more objectionable than a quick call to a bookmaker or even staring out of the window.

The implied duty of loyalty would, however, preclude an employee accessing the *Internet* or making any use of such access that is detrimental to the employer. As Laddie J explained in *Ocular Sciences Ltd. v Aspect Vision Care Ltd.*⁷⁴ in the context of deciding whether there was any proprietary information that an employee could lawfully publish in the course of his employment without his employer's consent:

"When an employee works for his employer he is bound by an implied obligation of good faith. Generally, he is expected to work for his employer not for his employer's competitors. He is expected not to put his skills at the service of one person while his salary is paid by another. This has nothing to do with the confidentiality of his skills and expertise. Similarly when he learns new things during his employment that, which become part of his skills and expertise, the employer can insist that, while he is employed, he uses those things only for the purpose of his employment. Whether or

⁷² Chapter 3B of Harvey on Industrial Relations and Employment Law

⁷³ Chapter 3A (5) *Ibid*

⁷⁴ [1997] RPC 289, 370

not those things are confidential, in the *Coco v Clark* sense, is largely irrelevant to the restraint on his ability to use it to his employer's detriment while he is still employed by him. The significance of this is that there is risk of slipping into thinking that what an employee can be restrained from doing while in employment is likely to be secret when, in truth, that restraint has little to do with secrecy but a lot to do with the employee's obligation to act in the interests of his employer."

It follows that any access to, downloading or dissemination of material that would be detrimental to the employer's interests in that it would expose the employer to criminal liability or civil liability to another employee or a third party, injure the employer's competitive position or benefit a competitor, or otherwise dissipate its resources or impair its efficiency would breach the implied duty of loyalty.

The difficulty of applying this general rule is that the consequences of an act are not always obvious. For instance, it is unlikely to have occurred to the British Gas employee who offered to exchange information on defaulting customers with local authority landlords that his initiative could injure his employer. For this reason, a comprehensive and coherent information handling policy accompanied by comprehensive training and ready access to technical and legal advice must be available to employees.

4.2 Convention Rights

Any information handling policy would be a dead letter unless it is enforced and enforcement requires employees' communications to be monitored. Monitoring is intrusive and unless it is done reasonably and with the employee's consent it may invade his right to privacy under article 8 of the European Convention of Human Rights. This guarantees everyone the right to respect for his private and family life, his home and his correspondence. The European Court of Human Rights held in *Halford v United Kingdom*⁷⁵ that the Merseyside Police infringed that article by monitoring telephone calls made by one of its senior women officers in order to gather evidence to defend a sex discrimination case that she had brought against it on the grounds that she had been denied promotion. In the light of *Halford*, OFTEL⁷⁶ has issued guidelines⁷⁷ requiring companies that monitor telephone calls made by their

⁷⁵ ECHR 25th June 1997 (available from the Court's website at www.dhcour.coe.fr/eng/JUDGMENTS/HALFORD.htm)

⁷⁶ The British Telecommunications regulator.

⁷⁷ 47/99 19th August 1999

employees to ensure that employees are able to make calls that are not recorded and to warn them that any other calls may be intercepted and recorded. Neither the Court's decision nor the OFTEL guidelines apply expressly to emails but there is no obvious reason for treating *Internet* access differently from the telephone.

4.3 Transfer of Data Abroad

All countries of the OECD, including the United States, have subscribed to Recommendations of the Council of the OECD concerning guidelines for the protection of privacy and transborder flows of personal data⁷⁸ for nearly 20 years. The most substantial difference in approach is that member states of the European Economic Area have enshrined those guidelines in legislation while the United States prefers to leave them to the good sense and self-interest of data users. The difficulty is that countries that have enacted data protection legislation authorize their supervisory authorities to prohibit the transfer of data to countries without similar legislation. Occasionally that has affected business such as when the Swedish data protection authority objected to the transfer by the local subsidiary of *Siemens AG* of records of its Swedish employees to Germany before the Federal Republic enacted similar legislation. Although there have been relatively few complaints either of interference with trans-border data flows or of misuse of personal data in countries with no legal protection of personal data over the last two decades the European position has been interpreted by some in the United States as protectionism. The tension between the United States and Europe is likely to be the adoption and enforcement of what the United States Secretary of Commerce calls "*The International Safe Harbor Principles*."⁷⁹ These principles cover most of the data protection principles:

- "1. **NOTICE:** An organization must inform individuals about what types of personal information it collects about them, how it collects that information, the purposes for which it collects such information, the types of organizations to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language that is readily understood and made available when individuals are first asked to provide personal information to the organization.
2. **CHOICE:** An organization must give individuals the opportunity to choose (opt out choice) whether and how personal information they provide is used (where such use is

⁷⁸ Published in the white paper "*Data Protection The Government's Proposals for Legislation*" April 1982 (Cmnd 8539)

⁷⁹ US Department of Commerce, David Aaron's circular to industry representatives dated the 4th November 1998 (available from www.epic.org/privacy/intl/doc-safeharbor-1198.html).

unrelated to the use(s) for which they originally disclosed it). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option. For certain kinds of sensitive information, such as medical information, they must be given affirmative or explicit (opt in) choice.

3. **ONWARD TRANSFER:** Individuals must be given the opportunity to choose whether and the manner in which a third party uses the personal information they provide (when such use is unrelated to the use(s) for which the individual originally disclosed it). When transferring personal information to third parties, an organization must require that third parties provide at least the same level of privacy protection as originally chosen by the individual. For certain kinds of sensitive information, such as medical information, individuals must be given opt in choice.

4. **SECURITY:** Organizations creating, maintaining, using or disseminating records of personal information must take reasonable measures to assure its reliability for its intended use and must take reasonable precautions to protect it from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

5. **DATA INTEGRITY:** An organization must keep personal data relevant for the purposes for which it has been gathered only, consistent with the principles of notice and choice. To the extent necessary for those purposes, the data should be accurate, complete, and current.

6. **ACCESS:** Individuals must have reasonable access to information about them derived from non public records that an organization holds and be able to correct or amend that information where it is inaccurate. Reasonableness of access depends on the nature and sensitivity of the information collected and its intended uses. For instance, access must be provided to an individual where the information in question is sensitive or used for substantive decision-making purposes that affect that individual.

7. **ENFORCEMENT:** Effective privacy protection must include mechanisms for assuring compliance with the principles, recourse for individuals, and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which individuals' complaints and disputes can be resolved; (b) systems for verifying that the attestations and assertions businesses make about their privacy practices are true and privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of and consequences for organizations announcing adoption of these principles and failing to comply with the principles. Sanctions must be sufficient to ensure compliance by organizations and must provide individuals the means for enforcement."

The sticking point at present appears to be investigation and enforcement. The solution may lie in some form of auditing acceptable to a European supervisory authority with insurance cover or compensation fund in Europe to which aggrieved data subjects may have recourse.

4.4 Civil Procedure Rules

On the 26th April 1999 a new code of civil procedure consisting of a new Civil Procedure Act, new rules of court, practice directions and protocols came into force in England and Wales with the overriding objective of dealing with cases justly.⁸⁰ Dealing with a case justly includes "saving expense" and "ensuring that it is dealt with expeditiously and fairly." All the powers to grant interim relief formerly exercised by the High Court are retained. Indeed section 7 of the Act provides a statutory basis for injunctions (formerly known as *Anton Piller orders* but

now called "search orders") requiring respondents to permit the applicant's solicitors to enter and search their premises to secure evidence that might otherwise be destroyed, removed or tampered with. This remedy is often used in cases where a former employee is suspected of removing documents or data from his employer's premises with the intention of using it in a competing business. Theoretically, the new rules should shorten waiting times and thereby reduce the need for interim injunctions but it is too early to say whether that will be the case in practice. Certainly there is the anomaly that an action can come on for trial in Manchester 5 months sooner than an application for summary judgment can be heard.

4.5 Proceedings against Internet Service Providers

The new rules will not of themselves avail persons in England who are aggrieved by wrongdoing abroad. Since *Internet* service providers ("ISP") have the power to control at least some *Internet* traffic by blocking access, refusing to host websites or otherwise and because they are likely to have contracted with at least one of the parties and are within the jurisdiction of the claimant's courts, aggrieved individuals and prosecutors in Europe have begun to look to them for redress. This is yet another difference in approach between Europe and the United States, where ISPs enjoy statutory immunity from suit for harm done by traffic flowing through their channels or stored on their systems even where they are aware of wrongdoing and do nothing to correct it. An extreme case is *Zeran v America On Line*⁸¹ where an action for defamation against the ISP was dismissed summarily even though the claimant had suffered abuse unnecessarily for several days before the defendant removed an offending notice. The contrast with the American position is shown by two cases, one German and the other French. In *People v Somm*⁸² the manager of the German subsidiary of CompuServe was convicted under local anti-pornography and anti-racism laws and sentenced to a term of imprisonment for not preventing German subscribers from accessing obscene material from American newsgroups. In *Estelle v Valentin*⁸³ the Tribunal de Grande Instance of Paris has enjoined an ISP from hosting a website that displayed photographs of a well-known fashion model without her consent. The United Kingdom legislature has taken a

⁸⁰ CPR 1.1 (1)

⁸¹ 129 F3d 327 (1997)

⁸² Amtsgericht, Munich 28th May 1999

middle position at least with defamation in that the Defamation Act 1996 provides some immunity from suit for an innocent publisher, provided it acts promptly on notification of the libel.⁸⁴ A welcome decision from Ontario in controlling spam, which suggests that an ISP owes some legal obligations to users of the network other than its own customers, is the recent refusal by Wilson J in *1267623 Ontario Inc v Nexx Ontario Inc*⁸⁵ of an interlocutory injunction to force an ISP to reconnect a subscriber who had been disconnected because it insisted on transmitting 200,000 unsolicited emails a day. Although there was no express prohibition against spam in their Internet service contract, the learned judge dismissed the application on the basis that it was an implied term. A similar case in England and Wales argued on similar points would probably be decided the same way. Articles 12 to 15 of the latest draft proposal for a European Parliament and Council directive on certain aspects of electronic commerce in the Internal Market⁸⁶ would afford some immunity to ISPs.

5. Need for an Information Handling Policy

The desirability of a policy that regulates employees' access to the *Internet* should already be obvious. In addition to the considerations already addressed, article 16 (1) of the draft electronic commerce directive requires member states to encourage codes of conduct at Community level by trade, professional and consumer associations or organizations designed to contribute to the proper implementation of the directive. Further, section 23 of the Data Protection Act 1998 provides for companies to appoint data protection supervisors with the incentive that they will carry out some of the regulatory functions that would otherwise be carried out by the Commissioner. An information handling policy should therefore dovetail with the employer's policies for processing personal data, protecting its trade secrets and safeguarding its intellectual property. The development and implementation of the policy is too important to be left to the information technology, personnel or any other single department. A decision to develop a policy should be taken at the highest level and coordinated by a director or at the very least a senior manager with some weight in the

⁸³ 9th June 1998

⁸⁴ *Godfrey v Demon Internet Ltd.* Unreported, QBD, Morland J 26th March 1999

⁸⁵ [1999] OJ No 2246

⁸⁶ COM (1999) 427 final, 1st September 1999

company. He or she should consult all departments of the company and probably its auditors, solicitors and other professional advisors. If a trade union or staff association is recognized its representatives should be consulted. If the company has overseas subsidiaries, its managers, professional advisors and staff should also be consulted. Any document should be drafted as simply and as clearly as possible using non-technical and non-legal language wherever possible. Difficult points should be clarified by simple tests and examples.

The precise contents of the policy will vary from organization to organization but it is likely to include:

- Instructions on how to identify and handle sensitive technical or commercial information;
- the persons who can authorize disclosure of such information and in what circumstances;
- authentication procedures where data are to be transmitted across the *Internet*;
- a list of websites that may never be visited and materials that may never be downloaded or disseminated;
- model forms of emails with disclaimers, confidentiality notices and other warnings;
- a warning that *Internet* access from the employers' equipment will be monitored but offering access for private use such as a cyber café in the staff canteen;
- a fair but rapid procedure for resolving grievances and appeals against disciplinary decisions.

Employees should be trained regularly and frequently in the application of the policy and any changes should be notified promptly preferably by electronic means. The policy should be kept constantly under review and the persons who were consulted in its development should continue to be consulted in its review.