This report is based upon work carried out by the author during the period 1994-1996. He would like to thank Charlotte Waelde, lecturer in the Legal Practice Unit, Department of Private Law, University of Edinburgh for her assistance with relevant Scottish law, Irene Loh, graduate student at the University of Hull, for invaluable research assistance, and the Law Faculty and Law Library of the University of Toronto for providing him with Visiting Scholar status in October 1995 - January 1996.

The author would like to thank the following for financial assistance during this period:

The Advisory Group on Multimedia Applications
The University of Hull Law School Research Committee
The Sir Philip Reckitt Educational Trust

The author would also like to thank the following institutions and organisations for allowing him a forum in which to discuss many of the issues raised here:

The Support Initiative for Multimedia Applications (SIMA).
The British and Irish Association of Law Librarians (BIALL).
The British and Irish Legal Education Technology Association (BILETA).
The Canadian Law and Society Association (CLSA)
The Centre for Teaching and Learning Support (CTLS), University of Hull.
The Centre de recherche en droit public (CRDP), The University of Montreal.
The Groupe de recherche informatique et droit (GRID), The University of Quebec at Montreal.
The Law Faculty, University of Edinburgh.
The Department of Computer Science, University of Edinburgh.
The Department of Computer Science, University of Glasgow.
The Department of Information Science, City University, London.
The Marketing and Commercial Liason Office & Staff Development Office, Lancaster University.
The UK Universities and Colleges Information Systems Association (UCISA)

Parts of this work have been published elsewhere, including:

The Law Librarian
"Legal Issues of the Internet" (1995) 26 *The Law Librarian* 524.

The Times Higher Education Supplement
"Code makers on the ether enigma", 10 November 1995 *Times Higher Education Supplement* Multimedia Supplement at iv.
"Theft by many other names", 12 January 1996 *Times Higher Education Supplement* Multimedia Supplement at vi.
"Welcome to the year of living less dangerously", 8 March 1996 *Times Higher Education Supplement* Multimedia Supplement at x.
"Never having to say you're sorry", 11 May 1996 *Times Higher Education Supplement* Multimedia Supplement at viii.

Contents

Introduction

If one spends some time examining the contents of some of the many and varied webservers that can be accessed via the Internet, it soon becomes clear that, even if one takes the largely uncritical and poorly informed media hype about the WWW with a sizeable pinch of salt, the increasing availability and sophistication of the new Internet application protocols has resulted in an unprecedented development in the field of publishing.

Until the development of the user friendly WWW protocol in the early 1990s, the ability to collate information in book, journal or pamphlet form, and then disseminate copies on a large-scale to a world-wide audience, was almost exclusively the province of increasingly monolithic firms of international publishers, and of government bodies and international organisations. In contrast, it is now the case that, by creating one copy on a Web server and allowing others to access it, an individual can publish on a similar international scale with a minimum of cost and effort. It is a change in the ability of the individual to disseminate information that, I think not unfairly, has been likened in some quarters to that which was occasioned by the Gutenberg press, and it is a change that has occurred in well under half a decade.[1]

It is in many ways the speed of that change that has created the problems with the law. Firstly, the law itself does not, and indeed cannot, react at such speeds, not least because the necessary knowledge base amongst lawmakers required to reach effective legal solutions is lacking. Indeed, previous attempts by legislators and the judiciary to deal with rapidly developing high technology issues have often exemplified the old proverb "Act in haste, repent at leisure".[2] Secondly, the rate at which individuals have been able to enter this brave new world of international publishing has at present outstripped the rate at which they can be educated in even the basics of the laws relating to publishing in their own countries. The large publishing firms in the traditional media have had decades and in some cases, even centuries to come to terms with both the national and international legal issues surrounding publishing, and how best to deal with them. Thus, even when they occasionally make mistakes, they are usually in a position to avoid, deflect or ameliorate both civil and criminal liability.

Many individuals have entered into electronic publishing on the WWW in utter ignorance of the potential legal implications of their actions, and a number have been rudely awakened to the fact that the law can and will be applied to activities on the WWW, contrary to the oft touted concept by ill-informed media pundits that the Internet is a place where one's actions and activities can have no legal consequence and where there is absolute freedom of speech, and freedom from censorship.[3] By way of illustration, during the early development of the WWW protocol, when relatively few people had access to the early web browsers, a number of webpages dedicated to comic strips, television programmes, films, movie personalities, etc. were set up by individuals who wished to demonstrate the functionality of the new protocol. However, these pages were almost always set up with an utter disregard for intellectual property rights. The novelty of the fact that pictures and text could be

---

1 In Kahin, B. "The Internet and the National Information Infrastructure" in *Public Access to the Internet* eds. Kahin, B. & Keller J. (1995, MIT Press), Figure 1 at p17 shows that the growth of the use of WWW applications on the NSFNET backbone did not reach an appreciable percentage until April 1993.

2 See for instance s5 of the Civil Evidence Act 1965 relating to computer evidence (this section was repealed by the Civil Evidence Act 1995), the sections of the Copyright Designs and Patents Act 1984 relating to computer programs, and the Computer Misuse Act 1990. Also Charlesworth, A. "Copyright in computer programs: Back to basics?" (1995) 145 *New Law Journal* 569 and Charlesworth, A. "Between Flesh and Sand: Rethinking the Computer Misuse Act 1990" (1995) 9 *International Yearbook of Law, Computers and Technology* 31.

3 The most famous phrase in support of this view are variations on the theme of "The Internet perceives censorship as damage and simply reroutes round it." This may well be true with regard to the Internet as a whole, but is of little consolation to an individual tangled in the "damage".

placed on-line in an easy and accessible manner appears to have completely overshadowed any thought as to whether or not the ability to do those things might in some very real way infringe upon the intellectual property rights of the actual owner of the material.

However, as the WWW began to attract a much wider audience, owners of copyrighted materials were alerted to the fact that their material was being used in this manner. Perhaps more importantly, they became aware that firstly, unlicensed distribution of their material via the WWW might eat into the market for traditional forms of distribution and secondly, there were new revenue generating possibilities on the WWW of which they themselves might want to take advantage.[4] It was at this point that the creators of home pages such as the "Unofficial Garfield Homepage" began to receive letters from lawyers representing the owners of intellectual property rights in the material they were placing on-line, threatening legal action unless the unlicensed use of their client's material ceased. This usually led to the rapid removal of the infringing material, a grudging apology, and a "chilling" effect on the activities of would be imitators. It would therefore seem obvious that, when one starts publishing on the WWW, having some knowledge of the potential legal issues that might arise would be useful.

With this in mind, it is worth turning back to the first point of this piece, that the law has not kept pace with the technology. As a nascent law of the WWW has begun to develop, the problems that have arisen in this and other areas of high technology have lead to a questioning, not just of the way in which existing laws are applied to high technology situations, but rather more importantly of the underlying rationale of those laws. Thus we have a situation where, for example, the question of how we apply copyright and other intellectual property rights to high technology, has evolved into more probing questions such as:

- should we attempt to use existing intellectual property rights such as copyright at all, as they are burdened with definitions and underlying biases that are at best irrelevant to the protection and development of modern technology, and at worst are a hindrance?[5]
- while the use of *sui generis* rights may bring their own problems, such as a lack of a current international framework, like the Berne Convention, through which to enforce them, will they not eventually offer the most effective method of protection ?
- perhaps, given the wholesale move towards digitisation, it is an appropriate time to consider not just adding *sui generis* rights piecemeal to the established body of intellectual property rights, but rather undertaking a radical overhaul of the entire intellectual property system, based as it is on the technologies and legal and social concepts of up to two centuries past.[6]

Thus, it can be seen that many of the areas of law that are currently relevant to high technology, the Internet, and the WWW, are heading into a state of flux. This article will, in examining certain areas of the law relating to the WWW as they stand at present, inevitably touch upon some of the current problem areas in successfully marrying the law to the technology, where there are few, if any, definitive legal answers to the questions posed, but a myriad of potential possibilities.

It should be noted at this point that this document does not claim to be a truly exhaustive survey of the legal issues that may need to be taken into account in this area, which would require a much weightier treatise than this.[7] In electronic publishing, as in traditional forms of publishing, there are a myriad pieces of legislation, as well as occasional common law provisions, which must be taken into account, including those concerning liability for content of publications, covering such topics as

---

4 See, for instance, the URL <http://www.unitedmedia.com/comics/dilbert/> (as of 03/03/96).

5 See Charlesworth, A. "Copyright in computer programs: Back to basics?" *op.cit.* at note 2.

6 See for example the proposals suggested by Roy N. Freed in his article "Comments on the Green Paper entitled 'Intellectual Property and the National Information Infrastructure' " *The Computer Law and Security Report* (1995) 11 at 234.

7 See further, the useful reference work by Henry, M. *Publishing and Multimedia Law* (1994, Butterworths) which has 351 pages examining the legal issues, and a further 447 pages of precedent documents.

defamation, obscenity, blasphemy, and provisions with regard to sex discrimination and advertising standards. The areas that are covered here have been chosen because there are either ongoing events, or recent developments in the law, which are of relevance to those working with the WWW.

However, the fact that certain areas of the law have been omitted from detailed discussion here should not be taken as meaning that they have no relevance to electronic publishers, for as the magazine Gay News discovered in the late 1970's, there is still life left in the English common law of blasphemy.[8] Equally, electronic publishers have to be sensitive to issues that are outside the scope of the laws of the United Kingdom. Anyone wishing to set up as a publisher on the WWW has to take into account the fact that unless the materials that they place on-line are access-limited to certain Internet domains,[9] or to fee paying readers,[10] they can in theory be read by more than 32 million users in over 130 countries.[11]

It should be apparent, given the recent experiences of publishers in the traditional media, that material that is perfectly legal in England may be neither legal nor acceptable elsewhere. In a salutary lesson for publishers in all media, traditional and electronic, the furore over Salman Rushdie's book *The Satanic Verses*, and the threats issued against both him and his publishers show that, even though English blasphemy law does not provide for Islamic sensibilities, publishing in both national, and international arenas, still holds many potential risks.

The legal issues surrounding WWW publishing are therefore likely to have even more of an international dimension than traditional publishing. It is unlikely that any institution running a website is going to be able to consider every legal rule in every possible jurisdiction, but given the fact that recent cases suggest that in on-line defamation, jurisdiction hopping - the ability to choose a national jurisdiction where one is most likely to succeed with a civil action - may well be an option open to the person defamed, a certain amount of thought will have to be given to limiting potential liability in other jurisdictions. That having been said, the final caveat to be mentioned at this point is that due to the constraints mentioned above, the majority of the issues to be discussed in this article will be examined only with reference to the law of England, Wales and where appropriate, Scotland.[12]

---

8 *R v Lemon, R v Gay News Ltd* [1979] 1 All ER 898, [1979] 2 WLR 281 (HL). It appears that Scots law contains no legal action for blasphemy.

9 It is possible to limit access to a webserver to specific domains such as .edu or .uk.

10 See for instance the URL <http://www.playboy.com/> (as of 03/03/96).

11 In reality, it is next to impossible to determine the number of individuals with Internet access with any precision.

12 Scots law contains some important differences in some of the areas discussed - notably the law of libel. See for instance Lloyd, I. "Managing legal risks - Liabilities in regard of content of on-line services" Conference paper for Communications and Law '95 29 September 1995. The author does not claim any great expertise in the area of Scots law and is grateful to Charlotte Waelde, lecturer in the Legal Practice Unit, University of Edinburgh for suggestions in this regard.

Intellectual Property

Electronic publishing, whether it takes the form of information distributed by CD-ROMs, a WWW server, or some other form of on-line provision, will inevitably raise a number of issues with regard to intellectual property rights. Of all the legal issues examined here, it almost certainly constitutes the single largest area of contention facing electronic publishers, and, of course, those who actually hold, and wish to protect, intellectual property rights in relevant material.

As multimedia publishers have discovered, the process of obtaining IPRs in materials for a package may be more time and resource consuming than any other part of the project. This highlights the paradox inherent in the relationship between the existing IPR regimes, and digital technology; that it can be a difficult and resource intensive task for an individual to ensure their compliance with the law, but an extremely simple matter, and one with little risk of penalty, for the law breaker to download and copy electronic versions of literary, artistic, musical and cinematic works.

This paradox has led to extensive discussion of the role and future of existing IPR regimes in relation to the proposed broadband digital networks, or "Information Superhighways" currently in fashion amongst governments.[13] So far, however, these discussions appear to have failed to provide any significant impetus for change against the inertia of existing national and international regimes.

Copyright and Associated Rights

Of all the IPRs, copyright is perhaps the most complex for the multimedia publisher to navigate.[14] From its creation in the 1600s where it was designed to provide a monopoly right for the early printers, it has been expanded to cover material as diverse as artistic works and computer programs. An unfortunate side effect of that diversity has been the need for copyright to contain a wide variety of types and lengths of protection.

In broad terms, there is a copyright infringement when an individual copies a work held in electronic format without the authority of the copyright holder. Such infringement is widespread in a number of Usenet newsgroups that carry pictures (notably those of supermodels or actresses),[15] where it has been estimated that between 95 and 100% of the pictures made available are infringing copies. Equally, electronic mail messages are subject to copyright protection as literary works, and as a result, copying them in whole or in part, without the permission of their author is a breach of copyright. In practice, however, there is often little more than lip service paid to this.[16]

---

13 See for instance in the US, the controversial report of the IITF Working Group on Intellectual Property Rights on "Intellectual Property and the National Information Infrastructure" which was chaired by Assistant Secretary of Commerce and Commissioner of Patents and Trademarks Bruce A. Lehman, and makes legislative recommendations to Congress to fine tune the law for the digital age - published September 1995 and archived in various formats at <http://www.uspto.gov/web/ipnii/> (as of 26/11/95).

14 For a general overview of intellectual property law, see Bainbridge, D. *Intellectual Property* 3rd ed. Pitman Publishing 1995. For a specific, but dated, overview of the CDPA 1988 see Dworkin, D. & Taylor, R.D. *Blackstone's Guide to the Copyright Designs and Patents Act 1988* Blackstone Press 1989.

15 See as an example the newsgroups alt.binaries.pictures.supermodels and alt.binaries.pictures.teen-idols (the latter is archived at <http://web.cs.ubc.ca/grn/newsgroups> as of 14/11/95).

16 Although increasingly, particularly on legal oriented e-mail lists and newsgroups, individuals are beginning to expressly assert their rights in their posts by way of statements, outlining what purposes their posts may be copied for, placed in their signature blocks.

Further, the recent development of Microsoft Network (MSN) and the resulting fear that Microsoft intends to dominate Internet services in the same way that it dominates the PC operating system and software markets, has led some individuals who post on Usenet newsgroups to expressly prohibit MSN from making and caching copies of their posts. For example:

"Microsoft Network is prohibited from reproducing this work in any form, in whole or in part, without the express written consent of the original author."

Section 107 of the Copyright, Designs and Patents Act (CDPA) 1988[17] states that where an individual sells, hires, exhibits, or distributes an infringing copy of a copyright work in the course of a business, or distributes "otherwise than in the course of a business to such an extent as to affect prejudicially the owner of the copyright" an offence will be committed. It is clear that this would catch individuals who attempt to sell infringing electronic media such as computer programs or pictures over the WWW, what is less clear is the situation regarding an individual who simply places infringing material on a webserver where it can be copied by others. Much turns upon the interpretation to be placed on the word 'distributes'; a broad concept would appear to cover virtually all situations where infringing material was placed on an open access webserver; a narrower interpretation would require that the individual placing the material on the open access web server perform some action other than to simply provide a facility for illicit copying.[18]

Table 1: What type of works may be protected ?

Literary Works
Literary works for this purpose include not only novels, poetry and non-fiction books but also all sorts of other written works which are original. Their literary merit is unimportant.[19]. This means that letters, memoranda, directories, e-mail messages and WWW pages may be protected. It should also be remembered that computer programs and code are protected as literary works.

Dramatic Works
Dramatic works for this purpose include plays and instructions for dance or mime. There must be some spoken words or described actions to perform to distinguish a dramatic work from a literary work. However the fact that a play does not contain any dialogue does not prevent its qualification as a dramatic work

Artistic Works
Artistic works for this purpose include graphic works, photographs, sculptures, collages, maps, charts and plans. These are protected regardless of artistic merit. However, works of architecture and of artistic craftsmanship require artistic quality in the work to qualify for protection

Musical Works
Musical works for this purpose include musical scores including any annotations and directions. Lyrics, however, are not, as they are protected as literary works.

Sound Recordings
This category covers every type of sound recording on any type of medium from which sounds can be reproduced.

Films
'Films' in this context covers any medium from which a moving image may be reproduced. As the definition of film under the 1956 Act was similar video recordings appear to be covered from the time of their development.

17 Which applies to Scotland, s157 CDPA 1988.

18 The US case, *US v LaMacchia* No 94 10092 RGS (D.Mass December 28 1994) demonstrates why such distinctions may be important. See also the UK cases *CBS Records v Ames Records and Tapes* [1982] Ch 91; *CBS Songs v Amstrad Consumer Electronics plc* [1988] AC 1013.

19 Although their length may be important, as single words or short phrases may be denied copyright protection, particularly if they could be better protected by trademark or the tort of "passing off". See *Exxon Corporation v Exxon Insurance Consultants Ltd* [1982] Ch. 119.

Broadcasts
'Broadcasts' includes any transmission by wireless telegraphy which is capable of lawfully being received by members of the public. This clearly therefore includes satellite transmissions.

Cable Programmes
These are defined as transmissions carried as services via cable, including on-line services.

Published Edition
There is copyright in the typography and layout of a literary, dramatical and musical work.

Performers' Rights
While these rights are not technically copyrights, they provide protection to performers and persons who hold recording rights in a performance. These rights are included in the CDPA 1988.

Who owns the rights ?

In theory, the original owner of copyright in a given work is the person who created it. There are however, exceptions; in many cases, works created in the course of employment will be owned by the employer - universities are unusual in that by convention much of the literary copyright remains with academic authors. It should be stressed however, that this is a convention, and should University authorities be so minded, they could acquire copyright in literary works created by academics in the course of their employment, by virtue of their being an employer.[20] Ownership of copyright in a work can change hands after its initial creation, and like any property, can be sold or assigned and may be passed on in a will.

Table 2: Ownership of Rights in a Work created under the CDPA 1988 regime

Literary Work
The rights in a literary work are owned by the author, unless it is created in the course of his employment, or unless otherwise assigned.

Sound Recordings and Films
The rights in sound recordings and films are owned by the person by whom the arrangements necessary for the making for the recording or film are undertaken, unless otherwise assigned..

Broadcasts:
The rights in broadcasts are owned by the person making the broadcast, unless otherwise assigned..

Cable Programmes:
The rights in cable programmes are owned by the person providing the cable programme service in which the programme is included, unless otherwise assigned..

Published Editions
The rights in typography etc. of published editions of literary, dramatical and musical works are owned by the publisher, unless otherwise assigned..

This is subject to the proviso that works created prior to 1988 may be covered by different regimes, as UK copyright law has not been retrospective in nature. Thus, under the 1956 Act, copyright in a

[20] Indeed, as the HE funding obtained from the government continues to decrease, Universities are likely to look increasingly to alternative forms of revenue generation, and their attitude towards the ownership and exploitation of intellectual property rights may then become less informal.

photograph belonged to the person who owned the negative film, unless the photograph was taken under commission.

How long do the rights last ?

All works will eventually emerge from copyright protection. However, different types of works have different lengths (or terms) of copyright protection. Also, despite the role played by international agreements such as the Berne Convention, different countries apply different lengths of copyright protection to works. The CDPA 1988 made changes to the length of protection for various in the UK works but, as it did not apply retrospectively, it still remained necessary to be aware of the relevant provisions in the 1956 Act and the 1911 Act. Equally, there are various variations and exceptions, a particularly irksome one being Crown Copyright, which can be considerably longer than normal copyright term.[21] It is the issue of Crown Copyright, and the restrictive approach of HMSO Publications, which until recently prevented the placing on the WWW of any significant amounts of UK legislation.[22] This may be contrasted with the situation in the US,[23] Canada[24] and Australia,[25] where large amounts of legislation and other government material are already available on the WWW. The problem lies with the fact that HMSO Publications is, not unsurprisingly, unwilling to relinquish its lucrative role as monopoly rights holder and licensee of UK legislative and other governmental material.

Directive 93/98/EEC and the Duration of Copyright and Rights in Performances Regulations 1995

The provisions of Directive 93/98/EEC[26] on Term of Protection of Copyright were required to be implemented by the EC Member States by July 1995. This Directive, designed to harmonise Member State copyright laws, extended the basic term from author's life + 50 years to author's life + 70 years.[27] It has been implemented in the UK by way of the Duration of Copyright and Rights in Performances Regulations 1995 SI 1995 No. 3297.[28] It appeared that the provisions of the Directive would have retrospective effect, which would have meant that some material which had fallen out of copyright in the UK would be, as it were, recopyrighted, and it was unclear as to how this may effect those who have acted in reliance on the material being out of copyright.[29] S23, 24 and 25 of the Regulations address these issues.[30]

It has also been reported recently that following the implementation of that directive in the EC Member States, measures taken in accordance with the GATT related TRIPS agreement:

---

21 Up to 125 years from the end of the year in which the work was created. If the work is published commercially before the end of 75 years after its creation, the term is 50 years from the end of the year of publication.

22 A limited amount of legislative material may now be found on the HMSO Publications server at the URL <http://www.publications.hmso.gov.uk/hmso/document/Acts.htm>

23 See the URL <http://www.pls.com:8001/d2/kelli/httpd/htdocs/his/2.GBM> (as of 14/11/95).

24 See the URL <http://canada.justice.gc.ca/Loireg/index_en.html> (as of 14/11/95).

25 See the URL <http://austlii.law.uts.edu.au/austlii_sources.html> (as of 14/11/95).

26 OJ1993 L290, adopted in October 1993.

27 The Community having decided to adopt the highest level of term protection amongst the Member States, that of Germany.

28 SI 1995 No. 3297. This substitutes the Copyright, Designs and Patents Act 1988, s5, s12, s13, s14; amends s57(1)(b), (2)(b), 79(4), 80(6), 81(5), 85(2), 105(2), 117, 124, 154(3), 179, 191, 211(1), 212, .Sch 1, para 9. and adds s15A, s66A, s172A.

29 The UK Patent Office issued a consultation paper with regard to this issue. See (1995) 11 CLSR 107. for details.

30 See Appendix XX

> "....[a provision of GATT] will restore copyrights on a number of foreign books, paintings, films, photos and sketches that are currently in the U.S. public domain. The rule, scheduled to go into effect Jan. 1, 1996, will apply to works still protected by copyright in the country of origin. It could have a "big impact on multimedia rights," says the acting general counsel for the U.S. Copyright Office. France and Mexico have already said they intend to restore copyrights on all movies, and works by artists such as Picasso and Matisse could be covered if they were created within the past 75 years."[31]

Table 3: The period of protection extended to various types of works

Literary, Dramatic and Musical Works
The author's life and 70 years after his/her death. (amended by Directive 93/98/EEC & SI 1995 No. 3297)

Works of Joint Authorship
70 years from death of last author to die. (amended by Directive 93/98/EEC & SI 1995 No. 3297)

Artistic Works
The author's life and 70 years after his/her death. (amended by Directive 93/98/EEC & SI 1995 No. 3297)

Anonymous Works
70 years from first publication. (amended by Directive 93/98/EEC & SI 1995 No. 3297)

Films
70 years from the death of the last to survive of the principal director, the author of the screen play, the author of the dialogue and the composer of the music specially created for the film. (amended by Directive 93/98/EEC & SI 1995 No. 3297)

Sound Recordings
50 years from first publication, but 50 years from fixation, if unpublished during that time. (amended by Directive 93/98/EEC & SI 1995 No. 3297)

Broadcasts and cable programme services
50 years from when broadcast first made or programme included in a cable service.(unchanged - as per the CDPA 1988)

Computer Generated Works
50 years from first creation (unchanged - as per the CDPA 1988)

Published Editions
25 years from first publication of that edition. (unchanged - as per the CDPA 1988)

Publication or communication to the public of a previously unpublished literary, dramatic or musical or artistic work or film in which copyright has expired
25 years from first publication. (introduced by Directive 93/98/EEC & SI 1995 No. 3297)

The implications for electronic publishers.

A multimedia or WWW publication may include some or all of the following copyrightable components:

[31] *Wall Street Journal* 27 July 1995, section A1

- Literary elements - protected as literary works
- Dramatic elements - protected as dramatic works
- Musical elements - protected as musical works
- Artistic work (graphics, photographs, drawings and models) - protected as artistic works
- Moving images - protected in the same way as films
- Sound recordings - protected as sound recordings
- Typographical arrangements of published editions of literary, dramatic or musical work
- Computer program - protected as a literary work
- Choreographic routine - protected as a literary work

It will be obvious therefore, that in many circumstances, the prospective publisher of a multimedia work will have to engage in a carefully planned process of rights acquisition or licensing. Amongst the rights that may have to be obtained for each work are:

- the right to copy the work
- the right to issue copies of that work to the public and a limited right to let them copy it[32]
- the right to adapt the work
- the right to perform the work in public (dependent upon the medium to be used for publication)
- the right to broadcast that work (dependent upon the medium to be used for publication)

The process described above, however, may only scratch the surface of the identification and acquisition of rights process. For example, there is the issue of performers rights, a right associated with copyright.
Under the CDPA 1988, performers rights exist in musical works, dramatic performances, readings or recitations of literary works, and performances of variety acts. As a result, where a multimedia product includes recordings of such performances, various consents may be required from differing categories of performers. Obtaining such consents may be difficult particularly where one is dealing with older material. Problems include both identifying performers,[33] and identifying rightholders.[34] Further, while copyright in literary, dramatic, musical and artistic works produced in the course of employment transfers automatically to the employer, performance rights do not. Consent should therefore be obtained contractually.[35] In certain circumstances, the Copyright Tribunal under CDPA 1988 can give consent on behalf of untraceable or unreasonable rights holders, however, such consent can only apply to the United Kingdom.

Other areas to consider include:

- Copyrights in films and sound recordings
  These belong to the person or persons who undertook the arrangements which resulted in the film being made, and the principal director.[36] Multimedia producers should therefore ensure that it is clear in contracts of employment that such arrangements are undertaken on the understanding that they are on behalf of the producers.
- Outside hours work by employees

---

32 That is, a limited right to make RAM and hard disk copies, so that the electronic publication can be used by a computer, but not a general right to copy and distribute.

33 As performer's rights can include not just featured performers, but also backup musicians and singers, chorus girls and crowd extras.

34 Where a performer has died, the right of consent may well have been transmitted to their heirs.

35 Note that consent applies only to 'first fixing' although this problem can in turn be overcome by copyright.

36 SI 1995 No. 3297

Where employees undertake work outside their strict working hours, works created in that time may not be covered by the employers' right to the copyright. Contracts should thus ensure that this eventuality is catered for.

- Personality rights[37]
  The right of a person to prevent their name, likeness or biography to be used without their consent. therefore individuals mentioned in credits and packaging should give consent as should those featured in a multimedia product.
- Music
  The use of music in a multimedia publication may require the obtaining of synchronisation licences[38] and the payment of mechanical royalties.[39] Commissioned music by the multimedia producer can avoid both these problems, and may lead to potentially lucrative spin-offs.[40]

There are three important copyright issues relating directly to aspects of the WWW itself. It would seem that the actual layout of a webpage, as opposed to it's content, would be capable of protection as a published edition, in that there is copyright in the typography and layout of a work. Thus to copy the layout of a web page, something that the browser technology makes very easy, is potentially a infringing action. This may be ameliorated to some degree by the fact that a the moment the HTML standard is still a fairly limited technology, and thus there are only limited ways of designing a page.[41]

Another as yet unresolved question concerns the issue of a webserver which does not itself contain any infringing material, but which has links to sites that do. Does the owner of that website incur any liability with respect to the infringing material by virtue of providing links which users can follow to that material at other sites, especially where the links explicitly refer to the fact that the material is infringing?

Finally, there is the issue of caching. One of the solutions to the slow WWW link times, especially to transatlantic websites, has been the development of various levels of local storage of copies of resources held on remote websites. At the simplest level, this may simply be storage of copies of recently visited webpages on a user's PC, either in RAM or in a hard disk cache. At a somewhat higher level, some sites, such as HENSA in the UK, store large numbers of webpages in their caches, users can then set their browsers to check if pages are stored in those local caches, before attempting to access the remote website. However, a possible problem arises out of this clever workaround, in that the CDPA 1988 states that rights exclusive to the owner of a copyrighted work include its reproduction in any material form, and further that this includes storing the work in any medium by electronic means.[42] Whether or not this apparent infringement of intellectual property rights will affect the use of caching technology remains to be seen, although web sites with "revolving" commercial advertising[43] - may see caching as a threat to their future viability.[44]

---

37 Applies in the US and a number of other jurisdictions, but not the UK.

38 The consent of the copyright owner to use music and lyrics in synchronisation with or timed relation to moving images.

39 Payment above and beyond that for the synchronisation licence for each use of the music.

40 A example of this would be the music commissioned for the video game "Super Mario Brothers" which has since been used in a successful dance mix record.

41 Although it has been suggested in the computer software copyright debate that the fact that there are only a limited number of ways of creating a work does not necessarily prevent an individual gaining a copyright. See *Ibcos Computers Ltd v Barclays Mercantile Highland Finance Ltd* [1994] FSR 275; [1994] 1 *Masons Computer Law Reports* 2.

42 CDPA 1988 s16.

43 Where each time a web page is accessed a new advertising logo is seen.

44 Although apparently it is possible to add code to a webpage which in effect tells the caching software that the owner of that page does not wish it to be cached, see Wired 3.12 December 1995.

Trademarks

Many companies throughout the world have symbols and logos which they protect by way of trademarks, as indicated in the UK by the symbol ® for registered trademarks and ™ for unregistered trademarks. For example, Microsoft®, Windows®, and MS-DOS® are registered trademarks of the Microsoft Corporation. Companies register such symbols & logos in order to prevent other companies from using them or 'passing off' their product or service as a product or service of the original company.[45] As a result, many firms are unwilling to countenance other businesses and private individuals using trademarked logos on their WWW pages, unless their explicit permission is obtained, and the logo is stated to be a trademark of the holder.

A recent development in this respect is the controversy over the allocation of domain names. All sites on the WWW have host identifiers known as domain names and these usually contain the name of the organisation which runs the site i.e. www.hull.ac.uk or www.microsoft.com.[46] Domain names have in the past been allocated on a first come first served basis by a US based body called InterNIC.[47] The controversy lies in whether domain names are, or should be, subject to trademark law. For example, in the US, Adam Curry, a former MTV VJ engaged in litigation with MTV over whether he could use the domain name mtv.com.[48] Other problems have arisen when companies have registered domain names containing their competitors' names or brand names,[49] or when individuals have registered domain names containing the names or brands of major firms and then attempted to hold those firms to ransom.[50] However, the question now arises as to whether trademark law is being abused by companies that wish to have a certain domain name that is already owned by an other individual or business, and which does not appear to be being misused.

Here, for example are extracts from a letter sent to a US member of the cyberia-l mailing list by US attorneys representing a firm which felt its trademark name was being misused.[51] Some material has been deleted or omitted.

> [material omitted]
>
> Our firm serves as counsel for [material deleted] which owns and publishes *Offshore* magazine. [material deleted] first registered its trademark "*Offshore*" with the United States Patent and Trademark Office under Registration [material deleted] on December

---

45 For an in-depth examination of UK trademark law see Annand, R. & Norman, H. *Blackstone's Guide to the Trade Marks Act 1994*, Blackstone Press, 1994. Note also the EC Regulation on the Community Trade Mark, Regulation 40/94/EEC, OJ 1994 L11/1, which was finally adopted in December 1993, and entered into force in March 1994. The purpose of the Regulation is to produce a trademark system which would permit trademarks to be valid in the whole of the EC by submitting an application to the Community Trade Mark Office, thus creating one unified legal procedure. This was seen by the Commission as the only means of ending the problems caused by differing national laws. However, as Member States were unwilling to abolish national marks, the Commission has been forced to accept a system in which, in the short term at least, Community trade marks will coexist with existing national trade marks. Community trademarks may only be obtained by registration.

46 Domain names provide a human friendly interface to the actual machine readable domain addresses which appear thus <204.254.209.2>. Thus if you wanted to access Hull University's WWW server you could type <http://www.hull.ac.uk/> or <http://150.237.176.8>.

47 Registering a domain name used to be free, but now costs $50 per year.

48 A court decision was given in *MTV Networks v. Curry*, 867 F. Supp. 202 (S.D.N.Y. 1994), but the effective result was an agreement between the parties that was not disclosed to the public - however, MTV now operates a WWW page at the domain name www.mtv.com.

49 e.g. the US telecommunications firm Sprint registered mci.com, the name of one of its rivals.

50 e.g. the dispute over the domain name mcdonalds.com, which was turned over to McDonalds by its owner in exchange for a donation to local schools.

51 E-mail message of Mon, 13 Nov 1995 18:29:49, sent by Duncan Frissell <frissell@panix.com> to recipients of list <cyberia-l@warthog.cc.wm.edu>

> 12, 1967. Over the past 28 years [material deleted] has expended substantial amounts of time and money to establish and promote the "*Offshore*" name throughout the world.
> It has come to our attention that you have registered the name "Offshore.com" as a domain name on the Internet. It is out opinion that the unauthorized use of the trade name "Offshore" violates [material deleted]'s rights to the protected use of its trademark under federal and state law. Your use of the domain name "Offshore.com" as an Internet on-line computer address is trademark infringement in violation of 15 U.S.C. P1114. It is further likely to cause confusion as to the source or sponsorship of such Internet address in violation of Section 43(a) of the Lanham Act and common law. Under general principles of trademark law, it is irrelevant whether Frissell Associate had the intent to infringe on [material deleted] mark. Liability for trademark infringement depends not on intent, but on the likelihood that the similar trademark will cause confusion. Obviously, the potential for confusion inherent in Frissell Associates' use of [material deleted]'s mark is substantial.
> Accordingly, unless we receive written representation from you by [material deleted] that Frissell Associates will cease and desist from all use of the name "*Offshore*," we have been instructed to commence legal action against Frissell Associates in order to assert and affirm [material deleted]'s right to its protected use of the "Offshore" trademark, and to terminate the confusion that results from your unauthorized use of "Offshore" in the Internet. Such lawsuit would include demands for injunctive relief, money damages for lost profits, costs, and attorneys' fees. While it is [material deleted]'s desire to attempt to avoid litigation to resolve this matter, [material deleted] cannot afford to allow confusion in the marketplace or among readers and advertisers of "*Offshore*."
>
> [material omitted]

The problem here lies not so much with the concept of whether trademark law can be used with regard to domain names, but rather whether it should. It is arguable that in stretching IPR concepts to deal with new technologies etc. we reach the point that they become so complex that we forget their original rationale, which may be very different from the interpretations that we now seek to place on them. Indeed, by attempting to fit yet another technology under an existing IPR, we risk making a mockery of the law - the fumblings of legislature, courts and academia with the issue of copyright and computer programs being one example, the issue of copyright in digital works potentially being another. It is possible to make them fit within those existing IPR categories, but only at the expense of coherency in, and enforceability of, the law.[52]

There are attractions to the use of trademark law, particularly to deal with the problem of individuals registering names solely to hold businesses to ransom, and in such cases, the concepts of fair use and "passing off" would seem to be workable and indeed desirable. However, in the letter cited above, Frizzell Associates were using <www.offshore.com> with regard to offshore financial centres. The complainants, by contrast, appear to be concerned with the drilling business. It is difficult therefore to see why the complainants should have a right of action under trademark law. The current holder of the domain name "offshore.com" is not 'passing off' his site as being the complainant's, he is not in the same business, and any confusion is likely to last only until an individual visits the WWW/FTP etc. site. An ASCII server address would also appear to lack the visual identifiers that one would usually associate with a trademark.

---

[52] Although not all commentators agree with this, there are a number of proponents who argue that trademark law is quite suitable for the Internet and WWW. See for instance Burk, D. "Trademarks on the Infobahn: A First Look at the Emerging Law of Cybermarks" at <http://www.urich.edu/~jolt/v1i1/burk.html> See also generally, "Billions registered, but no rules: the scope of trademark protection for Internet domain names" *Journal of Proprietary Rights* March 1995, and the bibliography on domain names held at <http://www.patents.com/schlacte.htm>.

To use a hypothetical example, if a company called "MacDonalds Shoes", run by an individual of that name, decided in early 1993 to put up a WWW site to advertise their shoe prices, and obtained the domain name <www.macdonalds.com> or <www.macdonalds.org> it is difficult to see why they should then be forced to give it up at a later date to the MacDonalds of hamburger fame. If, however, they called their site <www.macdonalds-burgers.com> or <www.macdonalds-goldenarches.com>, or when you accessed the site, the MacDonalds logo used was a copy of those on a MacDonalds shopfront, or it had the golden arches emblem, there would appear to be grounds for an action for trademark infringement.

Thus, the widely hyped circumstances where someone grabs the domain name of a big firm with the intent to hold them to ransom appear on the wane. What we now see instead are large companies exerting pressure on individuals and businesses, who have legitimately registered domain names, to give up those names, or risk legal action for trademark violation. The problem here lies in the fact that the threat of legal action in many cases would appear to be just that. The larger companies have been slow to pick up on the popularity of the WWW, and now that they have been apprised of that popularity, they wish to own domain names relevant to their business. However, in many cases it is arguable that they have no legitimate right to the domain names they want, as trademark law is not about using the courts to play catch-up in a commercial situation, where due to your own inactivity, you have been left behind. However, the threat of having to defend a legal action by a large firm, with all the attendant costs, will in many cases be sufficient to cause an individual or small business to surrender the domain name regardless of the letter of the law.

This would appear to be an abuse of both the spirit and the letter of trademark law, certainly it would not appear to be in keeping with the traditionally understood rationales for trademark law. In cases like that of the letter above, it is difficult to see any justification in trademark law for forcing the current owner of the domain name <offshore.com> to stop using it. <www.offshore.com> may be a desirable WWW domain name, but trademark law should not be about ensuring that those with the deepest pockets get the attractive names.

Patent

Patent did not appear to be a major influence in the area of the WWW, until the case of Unisys's patent on the mathematical algorithm which underlies the .gif picture compression format widely used to transfer and display pictures on the WWW. It is clear that the US Patent Office's decisions with regards to the granting of computer software patents (often for algorithms for which there would appear to be 'prior art'), and the use of 'submarine' patents,[53] may well have a significant effect in the way in which software in general, and WWW software, which has generally been available as freeware, in particular, develops.

[53] Where a patent holder does not assert his right until the object of the patent is in common use, at which point the holder then 'surfaces' and demands royalties for the use of the patented object. Another example of this was the purported patent that Compton Multimedia claimed over multimedia in general - a patent which was eventually struck down by the US Patent office.

Defamation

It is clear that the law of defamation will be applied to the various forms of Internet usage, including the creation and management of WWW sites, and will inevitably affect the way in which individuals and institutions use it. There are, however, a number of unresolved questions as to its application in this area. These include, who may be liable ? [54]
While definitive answers are difficult to come by, the answer to this in terms of e-mail may well include:

- the poster of the defamatory statement to a Bulletin Board AND the System Operator of the Bulletin Board;
- the poster of the defamatory statement to a moderated mailing list AND the moderator, where the moderator reads all the messages for content;

with regard to the WWW:

- the creator of a defamatory WWW page AND the owner of the WWW server on which it is based;
- potentially, under certain circumstances, the creator of a link to a defamatory WWW page where that link will have the effect of spreading the defamation, and it is clear that the creator of the link intended it to do so.

In the US it seems that the Courts have been inclined to hold the sysops of bulletin boards liable for material held on their boards, be it pornography, illegally copied software or other copyrighted material.[55] The debate in the US thus also touches on First Amendment issues and whether bulletin boards etc. should be granted the same type of privileged status as newspapers with regard to publication of allegations about public figures. In this country, the issues raised by electronic defamation inevitably have a less constitutional bent.

The Draft Libel Bill

A Draft Bill currently being sponsored by the Lord Chancellor's Department, aims to clarify some of the issues raised and may lead to the enactment of new legislation during 1996. The Lord Chancellor's Department has been encouraged to act by the fear that a large number of Internet related cases will come to court in the near future, and that existing defamation law is not suited to modern demands, and will be unable to cope. Reactions to the original consultation document were mixed, as it was felt that the provisions it envisaged would in fact discourage on line service providers such as access providers, proprietary hosts and operators of bulletin boards from monitoring the material that they carry, even where they do so at present.

Under the present legal regime it is not clear whether an Internet service provider could be held responsible for the nature of the material transmitted via its services, this uncertainty arises out of

---

54 For an excellent examination of this area, see Waelde, C. & Edwards L. "Defamation and the Internet: A Case Study of Anomalies and Difficulties in the Information Age" (1996) 10 (2) *International Review of Law Computers and Technology*.

55 A federal district court in Florida has held that a BBS operator is liable for infringing Playboy's copyright distribution and display rights by making available Playboy pictures in machine readable format. The interesting part is that the operator alleged that a subscriber had uploaded the files without the operator's knowledge, and the files had been removed as soon as the operator was aware of their presence. See *Playboy Enterprises, Inc. v. Frena*, No. 93- 489-Civ-J-20 (D.C. M. Fla. 12/9/93).

confusion over the status of service providers. If they are held to be publishers in the traditional sense, they can be held responsible for material distributed via their services. However, if they are held to be similar to operators of a basic telecommunications service or of postal services, such bodies are normally classed as "common carriers" and have a greater degree of protection against defamation actions under relevant legislation. As yet no service providers in the UK have been sued for defamation, so the issue remains undecided.

The draft Bill[56] creates a new statutory defence which will be available to distributors, printers and others who do not have primary responsibility for a defamatory publication, provided they exercised reasonable care in relation to that publication, and they neither knew nor had reason to believe that their acts contributed to the publication of defamatory material (s1). Thus, if a person is not an author, editor or publisher takes reasonable care in relation to the publication of material, and does not know nor have reason to believe that his actions may have caused or contributed to the publication of defamatory statements, he will have a defence against any resulting action for defamation.

Who is an Author, Editor or Publisher ?

S1(3)(c) and S1(3)(e) of the draft Bill exempts persons from being an author, editor, or publisher if they merely process, make copies of, distribute or sell any electronic medium in or on which a defamatory statement is recorded, operate the equipment, by which it is retrieved copied or distributed, or operate a communications system by which is transmitted or made available. The latter exemption however requires that there be no effective means of control by the operator over the person making that statement.

The apparent problem with these exemptions lies in s5 of the Bill which provides grounds on which to determine whether a person has taken reasonable care or has reason to believe that his actions may have caused or contributed to the publication of defamatory statements. The three grounds are:

- the extent of his responsibility for the content of the statement or the decision to publish it
- the nature or circumstances of the publication, and
- the previous conduct or character of the author editor or publisher.

The difficulty lies in deciding whether, under this section, if a service provider decides to regularly monitor, and where it feels it necessary, to censor, all or some of the messages on a bulletin board or home pages on a webserver, it runs the risk of losing the protection of this new defence of not being responsible for publication should a defamatory message slip through, because it will have moved from being a passive carrier of information, to performing some form of scrutiny or editorial function. For example a web site which hosts webpages created by students and staff, but which only monitors and censors the student pages, might also find itself liable for defamatory statements on the staff pages, as it would be possible to extrapolate from their actions with regard to the student pages that they were intending to exercise some form of editorial control. If the Bill passes into law in its current form, questions such as this will almost certainly arise in the judicial interpretation of the legislation, and it will be interesting to see if the courts are willing to accept an argument that the exercise of an editorial function in one sector of a site's business does not mean that it loses the right to the s1 defence for all its related activities.

Given the amount of information which may pass across a bulletin board, or be stored and adapted on a webserver, it seems clear that attempts to perform 100% effective scrutiny for defamatory statements are unlikely to succeed. Thus, it would seem likely in such a situation that the best

[56] Available from HMSO, price £3.75.

approach for service providers, if the Bill becomes law would be to abdicate any responsibility for content, as to perform a monitoring function would potentially lay them open to a successful lawsuit, which they might otherwise not face. On the other hand, it would appear from a reading of s1(5) of the Bill and its Explanatory Memorandum that a service provider who was aware that an author, editor or publisher had previously published defamatory material might be running some risk of liability if it did not then check any further output from that author, editor or publisher for further potentially defamatory material. This may pose something of a dilemma for both ISPs, and institutional websites.

Perhaps unsurprisingly, this issue has been litigated in the US, and service providers who performed a monitoring or censorship function have, as a result of that activity, been found liable for defamation.[57] By contrast those who have not performed such a function have in effect been held to be passive carriers and not liable for content.[58] However in the US, it is the absence of any form of an "all reasonable care" test that allows a service provider the option not to monitor traffic, and thus effectively to be classed as a common carrier.[59]
However, until the draft defamation bill reaches the statute book in this country, what are the matters which need to be considered in regard to an action for libel?:

Essentials of Libel

- In England and Wales,[60] "Libel consists of a defamatory statement or representation in permanent form ... Any thing temporary and audible only is slander. Statements in books, articles, newspapers and letters are libels."[61] It might be possible to argue therefore that electronic communications/publishing are not permanent and thus cannot be libellous. However, as electronic communications/publishing are often downloaded as hardcopy for dissemination and reading, I suspect that this line of argument would be unlikely to succeed, despite the problems that the courts have often had in applying the law to modern technology.
- Is the allegation complained of defamatory as opposed to vituperative/abusive ? Those involved in flame wars on the Internet are frequently abusive about their opposite numbers - however, venting one's feelings, even if they injure the other person's self esteem, is not sufficient for libel - defamation is only made out where the plaintiff is held in lower esteem by others as a result.
- Does the defamatory statement refer to the plaintiff ? That is, would the ordinary man in the process of scanning his newspaper, e-mail, bulletin board or WWW page be led to believe that the plaintiff was being referred to.

---

57 *Stratton Oakmonth, Inc. and Daniel Porush v Prodigy Services Co. & Others,* New York Supreme Court 24 May 1995

58 *Cubby Inc. v Compuserve* (776 F. Supp. 135, 140.)

59 There are however moves afoot in the US to make service providers liable for carrying indecent material. An amendment to the recent telecommunications bill passed by the US Senate in June 1995 (the Exon amendment) would appear to threaten the common carrier status of service providers, although critics have noted that the language in which the amendment is couched means that it is likely to be successfully challenged on First Amendment grounds.

60 The law of Scotland differs. A brief synopsis of the salient points is given below. For further information, the reader is referred to Norrie, K. *Defamation and Related Actions in Scots Law* Butterworths 1995. In Scotland, there is not the same distinction between libel and slander. Rather, an action for defamation arises as a result of an attack on a person's character, honour and reputation, arising from a falsehood, the falsity of which is rebuttably presumed. If however, a statement cannot be proved to be defamatory by the pursuer, then an action for verbal injury may be available. This requires the pursuer to prove falsity, intent to injure, and actual injury. One of the more significant differences between English and Scots law in this area is that the defamatory statement need only be communicated to the pursuer for an action to lie (Mackay v McCankie (1883) 10 R 537) and justify an award of at least nominal damages. The purpose is to provide solace for the affront or injury felt. Thus a private e-mail communicating a defamatory statement from one individual to another may be actionable.

61 Dias & Markesinis *Tort Law* (1985: Oxford)

- Has the defamatory statement been made known to others - has it been published ? Communication to the party named in the defamatory statement is not publication, as libel is concerned with how third parties view the plaintiff. It has been said that "the question of publication of a libel contained in a letter will depend on the state of the defendant's knowledge, either proved or inferred, of the conditions likely to prevail in the place to which the libel is destined".[62] In the case of an electronic mailing list the individual posting the communication will be well aware of the fact that it will be widely disseminated by the listserver, and still further by automated forwarding devices and the actions of others. In the case of a BBS, the individual posting the communication will similarly be aware that it will be available to anyone who dials up that BBS. It would seem that WWW pages might well have the widest potential dissemination rate of all. Thus the original poster cannot claim involuntary republication, for he is aware that this will occur.
- An important point to note is that "every repetition is a fresh publication giving rise to a fresh cause of action against each successive publisher. Thus not only the author of an article, but the editor, printer and publisher are also liable. Moreover, even mechanical distributors such as bookstalls, could be liable"[63] This is subject to the defence of unintentional defamation. Thus it could be argued that a BBS sysop could potentially be held liable for postings on his board, and that a moderator of a moderated e-mail list (where the messages are read by the moderator before posting to those on the list) almost certainly would be. Similarly the owner of a WWW server would appear to be caught by this, and even possibly an individual providing a link to the WWW page in question.

National and International Caselaw

It seems likely that the English courts would be inclined to accept that it is possible to libel individuals on BBS, mailing lists or WWW pages by posting untruthful and damaging statements about them in such fora. Thus an English citizen posting untruthful and damaging statements about another English citizen, on a list, BBS or WWW page where such a message would be read by others in the UK, and where this would be damaging to the plaintiff's good name or reputation, would almost certainly be liable to an action for libel. The issue of an English citizen libelling a US citizen is perhaps less clear as this might be considered by the courts to be out of their jurisdiction. However in the recent UK case *Godfrey v. Hallam-Baker*[64] where the claim was for damages for libel or alternatively slander regarding seven Usenet messages posted in 1993, the defendant apparently worked at CERN.[65] This case appears to have been settled out of court in June 1995 when Laurence Godfrey accepted undisclosed damages from Philip Hallam-Baker.[66] The first libel case arising from a WWW page appears to have occurred in early 1996 when the Guardian reported that the Poetry Society was to be sued for defamation, after it published an article on its Web pages

---

62 *Theaker v Richardson* (1962).

63 Dias & Markesinis *op.cit* n.52

64 Unreported.

65 *The Independent*, 22 August 1994 at 22

66 *Financial Times*, 19 July 1995. Waelde & Edwards note the following examples of libel actions taken or in progress:

"Asda is reported to have paid a police constable 'substantial' damages when he discovered a message on the company's e-mail system alleging that he had fraudulently obtained a refund for a joint of meat about which he had complained (*Daily Telegraph*, 20 April 1995). Western Provident Association, a private medical insurer, sued Norwich Union in respect of allegedly defamatory comments made about WPA on their internal email system by unauthorised members of staff (Venables ed. *Internet Newsletter*, Nov/Dec 1995). The *Times*, 7 December 1995, reported that computer games designer David Braben was suing former colleague Ian Bell over statements made in an interview published on the Internet, that Braben had made a fraudulent copyright claim over computer games. The result of these last two actions is not yet known."

accusing a publishing company of "preying on poets who cannot otherwise get their poems published".[67]

As all the settled litigation which has so far taken place appears to have concerned libellous statements via e-mail, it is to this that we have to turn to obtain a view of the way in which courts have reacted to defamation in the electronic forum.

The Australian case of *Rindos v Hardwick*[68] seems to make it quite clear that the Courts in that country are willing to accept that an individual can be libelled via the medium of a bulletin board or mailing list. The case concerned, in part, an entry placed on the DIALx science anthropology computer bulletin board by the defendant. The plaintiff was an academic at the University of Western Australia who was sacked on the ground of insufficient productivity. This action drew protests from academics at a number of international archaeological institutions, including one to the bulletin board from US anthropologist Hugh Jarvis. This in turn was replied to by Gilbert Hardwick from a computer in Derby, Western Australia. This entry imputed that the plaintiff had engaged in sexual misconduct with a local boy, and that his academic reputation was not based on appropriate academic research but "on his ability to berate and bully all and sundry" from which the inference could be drawn that these had some bearing on the plaintiff's sacking
The bulletin board in question was mainly used by academics and students, and according to the Court was accessible by upwards of 23 000 people world-wide. It noted that items placed on the board could also be printed out, and distributed in hard copy. The defendant made no effort to justify his comments, and did not defend his action in court. In his judgment Ipp J found that the remarks were clearly defamatory and had been widely published, and that the plaintiff had thus suffered serious harm to his reputation as a result of them, and awarded him $40 000 dollars in damages. Dr Rindos' lawyer, Robert Castiglione said " Computer users who use these world-wide bulletin-boards should be aware that they could be exposing themselves to defamation actions ... It's an informal system where people say quite personal things, but making allegations of paedophilia and bullying is going too far.[69]
The case involved two Australian based scientists - as yet it is unclear as to what would happen if the issue had involved an Australian scientist and a Canadian scientist. At this stage, the issue of jurisdiction comes into play, and this has several levels. We accept that it is clear that an Australian resident libelling an Australian resident on an internationally read bulletin board/mailing list will be liable in the Australian courts, however would the Australian courts accept jurisdiction over:

- a libellous statement made by a national of another country against an Australian national on a bulletin board which would be read internationally, including by other Australians ?

- a libellous statement made by an Australian national against a national of another country on a bulletin board which would be read internationally, including by other Australians, and nationals of the libelled party's country ?

- a libellous statement made by a national of another country such as the US, against another US citizen, which by virtue of the Bulletin board was widely read throughout Australia ?

---

67 *Guardian*, February 15 1996, noted in Waelde, C. & Edwards L. "Defamation and the Internet: A Case Study of Anomalies and Difficulties in the Information Age" *op.cit.*

68 31 March 1994, Unreported. See 'Computer libel wins academic $40 000' M.Lang, *The West Australian*, 2 April 1994

69 *Ibid*.

In short, because the standard for defamation would appear easier to meet in Australia than in the US and the defences available are fewer, would it be possible for a plaintiff pick his forum and his law because of the international nature of the Internet - to "jurisdiction shop"?[70]

The nature of the electronic dissemination itself might be a factor - i.e. an individual sends a libellous communication to a listserver in Canada, intending for all the subscribers of the list (including some in Australia) to receive the column, as opposed to his posting his libellous communication on a BBS in Canada, and someone in Australia dialling up and reading it. In the first case the individual is deliberately placing the material into a foreign jurisdiction, in the second that intent would appear to be lacking. The very nature of the WWW however, would appear to place all such defamatory material placed on WWW servers into the first category.

There is of course a further twist to this with regard to the WWW. Take the example of an individual who, while not placing defamatory materials on his WWW home page or server, provides links to such material with the aim of directing others to them. Is the individual concerned, and perhaps his employer, thereby 'publishing' the material as regards any possible libel action?

The recent US lawsuit involving a journalist running his own on-line newsletter demonstrates possible problems for electronic publishing. The journalist, Brock Meeks, a resident of the Washington, D.C. area and an employee of a communications trade journal, created the on-line news service, Cyberwire Dispatch, to comment on developments in the IT field.

In one of his articles, he expressed his personal disapproval of the business activities of a particular company, Suarez Corporation Industries (SCI) concerning their activities in the direct mailing business.[71] SCI objected to the article and filed a defamation lawsuit claiming Meeks made defamatory remarks and sought to disparage its products. The owner claimed that the Dispatch article lost him business and he thus sought compensatory and punitive damages and demanded an injunction to block Brock from writing further about SCI or its owner.[72] In the event, the issue was settled out of court, with Meeks paying SCI's court filing fee, some $64, and promising to contact SCI before publishing any further articles about it.

The case would, however, appear to demonstrate an interesting problem with the law of defamation. The cost of setting up a bulletin board, or Web server is not particularly expensive, however the cost of defending a legal action is likely to be very high. Concern has thus been expressed that as the number of libel suits internationally appears to be on the increase, the law of libel may well be used increasingly to stifle what many Internet users have long considered to be their right to absolute free speech on the networks, and that this will in turn have a "chilling" effect upon the willingness of individuals to carry out certain forms of electronic publishing, and may also make academic institutions less willing to allow staff and students a free hand in this area.

It is clear from the above that this area throws up a number of questions which the courts in the UK do not yet appear to have addressed.

- Can BBS sysops and WWW server owners be held liable when untruthful and damaging statements about individuals are made on systems under their control, even without their knowledge - where does the buck stop?
- If they can be held liable, are they then obliged to monitor every communication or web page - something that is probably next to impossible to do?
- Further, should they then go on to censor those communications or web pages which they suspect to contain untruthful and damaging statements about individuals?

---

70 Or "jurisdiction hop" as it is also known.

71 Notably that state and federal enforcement agencies had brought actions against SCI as result of their direct mailing practices.

72 It should be noted that the suit against Meeks was filed in Ohio.

- In allowing untruthful and damaging statements about individuals to be made on systems under their control, are they leaving themselves open to multi-jurisdictional liability?

These are topical issues in the US at present and should be considered seriously in the UK as well. It appears that most UK institutions approach this problem via their rules for use of their computer systems, although others have specific rules about the setting up of individual as opposed to institutional WWW home pages. These type of rules and regulations may provide a defence should a user of the institutions machines, use them to disseminate defamatory material, subject to the actual response of the institution upon the defamation being brought to the attention of the relevant authorities.

Criminal Liability

What should or should not be published, what is or is not obscene, and what the general public have or do not have the right to know, are naturally divisive issues. Thus, it is no surprise that the development of the WWW has led to sweeping statements by ill-informed media pundits about the absolute freedom of speech, and freedom from censorship, in cyberspace. It is true that the Internet in general, and the WWW in particular, has made it easy for individuals to publish material in a manner hitherto unprecedented. It is also true that the criminal law and those who enforce it have taken some time to come to terms with the implications of that change. However, from the increasing number of Internet related criminal prosecutions, in the UK and abroad, it would seem that the initial inertia has ended The actual degree and nature of computer crime, particularly as it affects the WWW, is extremely difficult to gauge. It would appear from surveys in the area of computer crime/misuse[73] that while computer crime is clearly on the increase, the majority of it is committed by individuals against their employers in a business environment.

As far as the WWW is concerned, the issue of crime and criminal liability has so far played a fairly low key role. What might be described as webcrime can be fairly readily divided into three aspects. The first of these, with regard to webserver and webpage owners, is the provision of illegal material for display or downloading via a webpage or link from a web page. The second, with regard to those browsing the Web, is the display or downloading of illegal material via a webpage or link from a web page. Finally, there is the issue of hacking: i.e. illegal access to a webserver, the unauthorised altering or deleting of parts of a webserver, or the illegal interception of communications resulting from the use of a feature of a webpage e.g. the interception of credit card numbers collected by the use of the forms function.

Pornography

The most obvious (at least it seems to journalists) crime that might be carried out via the Web is the distribution/downloading of computer pornography. This may be covered by a number of provisions covered including the Telecommunications Act 1984[74] the Obscene Publications Act 1959,[75] and with regard to child pornography, new legislation in the form of s84-87 of the Criminal Justice and Public Order Act 1994.[76] The relevant provisions of this Act, which amend other legislation, including the Protection of Children Act 1978, are aimed specifically at computer generated and distributed pornography. That having been said, even when one takes the media hype into account[77] in the period 1991-1993 of the 976 obscenity cases handled by the Crown prosecution Service, only 11 involved computer pornography and only 7 of those went to court.[78]

That having been said, the WWW was only in its infancy in 1993, and it appears that its development, combined with the increasing availability of Internet services outside the academic sphere, has led to an increase in both webservers containing pornography and those with web browsers who wish to access it. Examination of sites containing pornographic material, appears to show that they fall into two main categories;

- those run by individuals which contain small personal collections of pornography, accessible at no charge,

---

73 For example *Opportunity Makes a Thief: An Analysis of Computer Abuse*, the fifth triannual report of the Audit Commission on the extent of computer abuse and fraud in the UK (1994, HMSO Publications).

74 See Appendix XX

75 Not applicable in Scotland.

76 See s172 (8) for those parts of the Act applicable to Scotland.

77 And there seems to be no end to the number of articles like the one run by *The Guardian*, 24 August 1994 somewhat unoriginally entitled 'Computer going down' which noted that a University of Wales computer was put out of action for two days due to an overload caused by a student downloading pornography from the US.

78 'Industry focuses on cleaning up its act' *The Guardian* 27 September 1994 at 8.

- commercial websites which contain large amounts of pornography but which charge for access to all but a very small amount of it.[79]

Of these two categories, it is the latter that appears to be the major area of growth. Those in the former category are usually individuals who are at universities, or who have Internet access via their employer, or via an Internet service provider (ISP). In general, most WWW sites, particularly those based at academic institutions, are keen to avoid any problems with hard or soft core pornography, and a great deal of control can be exercised by peer pressure from other institutions without the aid of the law, even where the law of the country involved does not forbid such material. For instance, WWW servers at the University of Delft (hard & soft core) and the Conservatoire National des Arts et Metiers (CNAM) (soft core), which carried pornographic pictures that had been downloaded by automatic newsfeed from Usenet groups,[80] have both been forced to remove the offending material due to pressure from their governing bodies.[81] The situation in the US has tended to be more problematic in this regard due to the First Amendment issues involved.[82]

Computer Misuse

Pornography, whilst the most hyped by the media, is not the only form of information publication which may result in criminal liability. It has been suggested that publishing material that might be used in order to breach computer security, or to facilitate unauthorised entry into computer systems, will be caught by those provisions of the Computer Misuse Act 1990 that deal with the issue of conspiracy to commit an offence under the Act. This is supported by the recent conviction of Christopher Pile (a.k.a. "The Black Baron") who admitted 11 charges under the Computer Misuse Act 1990 with regard to writing and distributing computer viruses, and one charge of inciting others to spread computer viruses.[83] It is unclear how far this could be extended to other potentially undesirable types of information, such as bomb making manuals. Equally, there is as yet no indication as to the likely liability of an institution that carries hacker-related newsgroups such as alt.2600 on its Usenet newsfeed, thus potentially disseminating material which could allow others to access computer and telecommunications systems without authorisation.

---

79 Such as <http://www.playboy.com> and <http://www.penthouse.com>.

80 e.g. alt.binaries.pictures.erotica and alt.binaries.pictures.blondes

81 And, it must be said, apparently due to massive overloads on the machines concerned as individuals attempted to access the pictures.

82 Although there have been interesting developments with regard to 'jurisdiction hopping' by law enforcement agencies, see a recent US case reported last year (28 July 1994) on the cyberia-l mailing list

"Jury Convicts Couple in Computer-Porn Trial" MEMPHIS, Tenn. (AP) -- A federal jury convicted a California couple today of transmitting obscene pictures over a computer bulletin board. The case has raised questions, in this age of international computer networks, about a 1973 Supreme Court ruling that defines obscenity by local community standards. Prosecutor Dan Newsom, an assistant U.S. attorney, said the trial was the first he knows of for computer bulletin board operators charged under federal law with transmitting pornography featuring sex by adults. Robert and Carleen Thomas, both 38, of Milpitas, Calif., were convicted of transmitting sexually obscene pictures through interstate phone lines via their members-only Amateur Action Bulletin Board System. The Thomases were convicted on 11 criminal counts, each carrying maximum sentences of five years in prison and $250,000 in fines. Thomas was acquitted on a charge of accepting child pornography mailed to him by an undercover postal inspector. The Thomases refused to comment after the verdict. They remain free on $20,000 bond to await sentencing, for which no date was set. Defense lawyer Richard Williams said his clients will appeal, arguing the jury was wrongly instructed on how to apply the Supreme Court's standard on obscenity. The trial raised questions of how to apply First Amendment free-speech protections to "cyberspace," the emerging community of millions of Americans who use computes and modems to share pictures and words on every imaginable topic. Williams argued unsuccessfully before trial that prosecutors sought out a city for the trial where a conservative jury might be found. "This case would never have gone to trial in California," he said. During the week-long trial jurors were shown photographs carried over the Thomases bulletin board featuring scenes of bestiality and other sexual fetishes. Their conviction also covers videotapes they sent to Memphis via United Parcel Service. The videotapes were advertised over the bulletin board.

83 (Unreported). He received an 18 month jail sentence for those activities in November 1995.

The unauthorised access and alteration of webservers or webpages, and the interception of information collected by WWW mechanisms, would both appear to be covered by existing criminal law.[84] In such cases, any institution which plays unwitting host to a hacker is unlikely to be held liable for his actions, particularly where precautions have been taken to both minimise unauthorised user access, and to inform legitimate users of their responsibilities. By way of example, most universities, which were once easy access points to the Internet for would-be hackers because of their open access ethos, have taken action to severely restrict or deny guest user access to their systems, and made it very clear to *bona fide* users that where unauthorised access to other computer systems from a university system is discovered, it will be both investigated and punished..

Racial Hatred

It has been suggested that certain sections of the Public Order Act 1986[85] may also be relevant to any discussion of criminal liability on the Internet. Sections of that Act that are concerned with racial hatred state that an individual who publishes or distributes written material which is abusive, threatening or insulting to the public, or to a section of the public, or who has such material intending it to be displayed published or distributed, will be guilty of an offence if that person intends to stir up racial hatred, or if, in the circumstances racial hatred is likely to be stirred up.[86] Racial hatred is defined as hatred of any group of persons in the UK, whether they are defined by reference to their colour, their race, their nationality, their citizenship or their ethnic or national origins.[87] The provisions appear, on their face, to be applicable to webpages that are overtly racist. It is also possible that a webpage which is not expressly racist, but which has links to other webpages that are, may be covered by the Act. In that case, as with libel, the important issue would be proving whether the owner of the linking webpage knew that the material linked to was "threatening, abusive or insulting". However, the issue remains theoretical, as at present, relatively little use appears to have been made of this law in electronic, or indeed any other, forums.

Contempt of Court

In England,[88] a distinction is drawn between "civil" and "criminal" contempts. Civil contempt relates to circumstances where parties breach an order of court made in civil proceedings, for example injunctions or undertakings, and as such are not relevant here. Criminal contempt deals with various types of conduct which if allowed to go unchecked, would have the effect of interfering with the administration of justice, and is designed to have a punitive and deterrent effect.[89]
Criminal contempts essentially fall into five categories:

- Publications prejudicial to a fair criminal trial
- Publications prejudicial to fair civil proceedings
- Publications interfering with the course of justice as a continuing process
- Contempt in the face of the court
- Acts which interfere with the course of justice.

---

84 Particularly s1-3 of the Computer Misuse Act 1990, and the Interception of Communications Act 1985

85 See s42 for those sections of the Act applicable to Scotland.

86 See The Public Order Act 1986 s18-19, 23.

87 *Ibid.* s17

88 But not in Scotland.

89 See Bailey, S.H., Harris, D.J. & Jones B.L. *Civil Liberties: Cases and Materials* 3rd ed. Butterworths 1991 - Chapter 6, Freedom of Expression: contempt of court & Smith, G. (ed.) *Internet Law and Regulation* FT Law and Tax 1996 .

While the law of the contempt of court was developed by the judiciary through the common law, it has been modified to some extent by the Contempt of Court Act 1981[90] which makes it an offence of strict liability to publish a

> "…publication [which] includes any speech writing, broadcast, cable programme or other communication in whatever form, which is addressed to the public at large, or any section of the public"[91]

where such a publication

> "… creates a substantial risk that the course of justice in the proceedings in question will be seriously impeded or prejudiced."[92]

The fact that it is a "strict liability" offence means that an offence occurs even where the person making the publication did not intend to interfere with the course of justice. The broad definition of "publication" would cover USENET messages, e-mail messages sent to mailing lists and WWW pages. The publication of material relating to a case will only be an offence, where it occurs when the case is still *sub judice.* The statutory "strict liability" rule is only applied during the period that the case is "active" and the definition of "active" is laid down in the Act. However, where an individual knows or has good reason to believe that proceedings are imminent, and publishes material which is likely or calculated to impede or prejudice the course of justice before the point laid down in the Act as the time when the case is "active" this may be a common law contempt.

Actions which would commonly draw charges of contempt include:

- Publication of material which prejudges the case, especially where it makes the express or tacit assumption that the accused in a criminal trial is guilty.[93]
- Publication of material which is emotive or disparaging, especially where there is an insinuation of complicity or guilt by association
- Publication of material which is likely to be inadmissible at trial, such as previous convictions, or mention of evidence likely to be excluded as having been improperly obtained.[94]
- Publication of material such as a photograph of the defendant, where the issue of identification forms part of the trial proceedings.
- Publication of material hostile or abusive towards potential witnesses with the intention of coercing them into not testifying, or disclosure of witnesses' names following a court order that their names should not be disclosed if there was a danger that lack of anonymity would prevent them from coming forward.[95]
- Publication of jury deliberations
- Publication of material breaching reporting restrictions in cases such where in open court there is identification of children involved in the proceedings, or identification of rape victims.[96]
- Publications of material relating to court proceedings closed to the public, including where there is an issue of national security.

Defences to the "strict liability" offence:

---

90 However the CCA 1981 does not codify or replace entirely the common law. It does however apply to Scotland (s15).

91 S2 (1) CCA 1981.

92 S2 (2) CCA 1981.

93 See *A-G v TVS Television* (1989) The Times 7 July, (DC).

94 See *S-G v Henry* [1990] COD 307.

95 See *R v Socialist Worker Printers and Publishers Ltd, Ex parte A-G* [1975] QB 637 (DC).

96 See *Pickering v Liverpool Daily Post and Echo Newspapers plc* [1991] 1 All ER 622 (HL).

- A person is not guilty of contempt of court under the strict liability rule as the publisher of any matter to which that rule applies if at the time of publication (having taken all reasonable care) he does not know and has no reason to suspect that the relevant proceedings are active.[97]
- A person is not guilty of contempt of court under the strict liability rule as the distributor of a publication containing any such matter if at the time of publication (having taken all reasonable care) he does not know that it contains such matter and has no reason to suspect that it is likely to do so.[98]
- A person is not guilty of contempt of court under the strict liability rule in respect of a fair and accurate report of legal proceedings held in public, published contemporaneously and in good faith.[99]

The enforcement of the law of contempt has been rendered more difficult in modern times, by the ability of individuals to publish material, in both traditional[100] and digital media,[101] in countries outside the court's jurisdiction. The Internet has in many ways exacerbated this situation. It has been suggested with regard to the Internet, that where the court cannot bring contempt proceedings against the original publisher, it may seek to do so against the Internet Service provider which distributed the material within the court's jurisdiction. Such an approach would, however, potentially create similar problems to those found in libel cases, where Internet Service Providers have argued that the sheer volume of e-mail traffic, or the vast number of WWW pages on their systems make it impossible to check them all for possible libellous statements. As with libel, the courts are likely to treat rather more favourably (with regard to punitive measures) those ISPs and website owners who, once notified that material likely to constitute the basis for a contempt offence, is held on their systems, do everything in their power to remove it as rapidly as possible.

---

97 S3 (1) CCA 1981

98 S3 (2) CCA 1981

99 S4 (1) CCA 1981

100 Consider, for instance, the *Spycatcher* saga, where the book in question was freely available outside the UK, but could not be published or excerpted in the UK.

101 A good example of this concerns the trials in Ontario, Canada, of Karla Homolka and Paul Bernado. During the trial of Karla Homolka for the murders of two teenaged girls, Kristen French and Leslie Muhaffy, the court ordered a publication ban on reports of the trial in Ontario, in order to ensure a fair trial for her husband Paul Bernado (a.k.a. Paul Teale), also charged with the murders (See Action No. 125/93, [R. v. Bernardo], [1993] O.J. No. 2047 at < http://www2.magmacom.com/~djakob/censor/mediaban.txt>). Despite the ban, information was widely available, due to coverage by US newspapers, cable and TV stations, and at least one Website based at a US University < http://www.cs.indiana.edu/canada/karla.html>. A UseNet newsgroup set up to disseminate and discuss information about the trial, <alt.fan.karla-homolka> was censored by many Canadian Universities.<http://www.cs.indiana.edu/canada/BannedInCanada.txt>.

Data Protection

One of the most attractive aspects of the WWW is the relative ease with which even users with limited on-line experience can access and download data. The challenge of providing them with information which is actually worth browsing and downloading has been taken up enthusiastically in many quarters, not least by academic institutions, who increasingly see having an official webserver containing information about their courses, staff, and other attractions, as an important part of their public relations package. At the other end of the scale, the more proficient webpage providers are developing ever more sophisticated methods of collecting data from individuals browsing their output. At the simplest level this data collection may simply involve asking people accessing a page or set of pages to "sign the visitors' book" by leaving their name, institution, and possibly an e-mail address. More complex operations, using web servers that support more secure encryption methods may go further, offering goods for sale, and accepting names, addresses and credit card numbers via the "forms" mechanism offered by some browsers.[102]

Praiseworthy as all these efforts are, there is a danger that in the enthusiasm to place information on the WWW, or to run viable business operations via webservers, the law relating to data protection is either pushed to the back of people's priorities, or entirely overlooked. In modern society, the collection of data about individuals has become of increasing importance, as our ability to sort it into meaningful patterns with the aid of computers has developed. The ability to profile individuals via records such as electoral rolls, credit records, use of store loyalty cards, magazine subscriptions, and the like has become a lucrative industry. More often than not we do not know who holds information on us, to whom they may have passed it, and the purposes to which it is being used.[103] The data protection laws go some way towards redressing that balance by creating a set of rules by which data processors should operate, and which give individuals some limited powers to ensure that at the very least the information that others hold on them in electronic form is accurate. It is widely acknowledged that the existing UK Data Protection Act 1984 (hereafter the DPA 1984) is a less than perfect solution to the problems that exist, and it will be interesting to see if the recent adoption of a somewhat more rigorous regime by the European Community in its Directive on Data Protection[104] will have any greater effect when finally implemented into UK law.

A brief overview of the Data Protection Act 1984

What is personal data ?

The DPA 1984 first defines data as "information recorded in a form in which it can be processed by equipment which operates automatically, in response to instructions given for that purpose."[105] Data therefore includes information processed by a computer, or information processed by mechanical means. Thus the Act applies to automatically processed information, but not to manually held information, which is contained in files or other paper records.

The Act then proceeds to define personal data as being data which consists of information which relates to a living individual (the data subject[106]), who can be identified from that information by

---

102 e.g. Hot Hot Hot at <http://www.hot.presence.com/g/p/H3/__03a0e2fc/h3-home.html> which specialises in hot sauces.

103 See for various examples, Branscomb, A.W. *Who Owns Information ? From Privacy to Public Access* (Harper Collins/Basic Books 1994).

104 OJ 1992 C311/04 (adopted 24 July 1995). This should result in new UK legislation around 1998.

105 S1(2).

106 S1(4)

itself, or when it is coupled with other information held by the person holding that data[107] (the data user[108]). Such data would include any expression of opinion about the individual. This definition clearly excludes both individuals who are deceased, and legal entities such as companies, universities and charities.

Some kinds of data which would appear to fall within the above definition are specifically exempted from the regime prescribed by the Act. Such data does not need to be registered, and the individual concerned will not have any right of access to the information.

Table 4:Data which is exempt from the provisions of the Data Protection Act 1984

Information required for the purpose of safeguarding national security (Article 27)
Information held for payroll, pensions, and accounts purposes, under certain circumstances. (Article 32)
Personal data held only for domestic or recreational purposes (Article 33)
Information relating to unincorporated members clubs, which relates only to members of the club who have been asked whether they object to the personal data being held for such a purpose and have not objected (Article 33)
Mailing lists consisting only of names, addresses, and other details required for distribution, where the data subjects have been asked whether they object to the personal data being held for such a purpose and have not objected. (Article 33)
Information that the law requires to be made public. (Article 34)

What obligations does the Act impose ?

Individuals who hold personal data, defined as 'data users' in the Act, are obliged to register with the Data Protection Registrar[109], and to use the data that they hold in accordance with what are known as the Data Protection Principles.[110] Failure to register as a data user when holding personal data is an offence.[111] Once a person has an entry on the register, it is also an offence for a person to:

- hold personal data of any description other than that specified in their entry.
- hold any data, or use any data held, for a purpose other than the purposes described in their entry.
- obtain data, or information to be contained in the data to be held, from any source which is not described in their entry
- disclose the data held to any person who is not described in their entry
- directly or indirectly transfer data held to any country or territory outside the UK other than those named or described in their entry.[112]

However, at present, the take-up rate for registration is estimated to be less than 50% of those required to do so, and given the current under-resourcing of the Data Protection Registrar's office, the likelihood of an action for minor non-compliance with the Act remains limited.

---

107 S1(3).
108 S1(5)
109 S5 (1).
110 See Schedule 1, DPA 1988
111 S5 (5).
112 S5 (2)(a) - (e), S5 (5)

Table 5: The Eight Data Protection Principles

1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purposes
3. Personal data held for any purpose shall not be used or disclosed in a manner which is incompatible with that purpose or those purposes.
4. Personal data held for any purpose or purposes must be adequate, relevant and not excessive in relation to that purpose or purposes.
5. Personal data shall be accurate and, where necessary, kept up to date.
6. Personal data held for any purpose must not be kept for longer than is necessary for that purpose or those purposes.
7. An individual shall be entitled, at reasonable intervals, and without undue delay or expense, to be informed by any data user whether he holds personal data of which that individual is the subject, and; the individual is also entitled to have access to any such data held by a data user and; where appropriate, to have such data corrected or erased.
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.

What rights does the Act give to individuals

The Act provides that individuals have the right to find out whether a data user has personal data recorded on computer which relates to them, and that they have the right to be provided with a copy of that information in a form which is intelligible to them.[113] These rights are subject to a number of provisos including that:

- the request must be in writing, and the data user may charge a limited fee for the service.[114]
- the data user must be provided with sufficient information for him to be satisfied as to the identity of the person making the request[115]
- if the information requested results in the disclosure of information relating to another individual who can be identified from that information, the data users must be satisfied that that other individual consents to its disclosure. However, the data user cannot withhold all the information if such a third party disclosure can be avoided simply by the removal of names or other identifying particulars,[116]

The data subject also has the right to challenge the accuracy of the information and, if necessary, obtain a court order for:

- the rectification or erasure of inaccurate data, and any other data or expressions of opinion which appear to the court to be based on the inaccurate data.[117]

113 S21 (1).
114 S21 (2)
115 S21 (4).
116 *Ibid*.
117 S24 (1).

- the right to enter onto the record a supplemental statement of the true facts relating to the matters dealt with by the data.[118]

In limited circumstances, a data subject may claim compensation for damage suffered as a result of inaccuracies in the data, loss or destruction of the data, or its unauthorised disclosure.[119]

Personal Data on Webservers

With regard to the current situation, if an institution has webpages which:

- contain personal data which is linked to specific and identifiable individuals, or
- contain data which cannot by itself be used to identify an individual, but when allied with other information held by the institution, does permit such identification

it would be wise for the person responsible for those webpages, or the webserver, to check the provisions of the DPA 1984 with regard to whether or not it is necessary to be registered with the Data Protection Registrar. It is unclear from the wording of the DPA 1984 as to whether the additional information which may be used to link an individual to otherwise anonymous data on a computer must itself be held in a form in which it can be processed automatically e.g. on another computer. The important thing to ascertain is not just that an institution is registered to hold certain types of personal data, but also that the particular personal data which is to be placed on the webpage is permitted to be used in that manner under the terms of the registration.

A particular question with regard to the WWW lies in the obligations on registered data users not to "disclose the data held to any person who is not described in their entry" or "directly or indirectly transfer data held to any country or territory outside the UK other than those named or described in their entry."

With regard to the latter issue, the DPA 1984 does not define what is meant by 'transfer', but it would seem entirely possible to argue that the process by which data is passed on demand from a webserver, to the RAM or harddisk cache of a machine being used to browse that webserver, goes further than mere 'disclosure'. If it is accepted that this is 'transfer', it would seem to follow that if personal data is held on an open access webserver, i.e. a webserver that is not in some way domain restricted, there would appear to be no way for the owner of that webserver to avoid the transfer of that personal data to any individual with full Internet access in any number of countries outside the UK.

Thus, when one looks at both those obligations, it is difficult to see how a open access webpage containing personal data could successfully stay within the letter of the law, unless it were possible to have entries in the register of "all other web users", and "the world" respectively. Such a solution would, however, seem to be so wide-ranging as to render the DPA 1984 meaningless. It is therefore interesting to speculate for example whether educational institutions that have placed details (such as name, work address, telephone number, e-mail address, academic interests and publications) of all their members on-line, either on the X500 database or the WWW, are actually adhering strictly to the letter of their registration.

As far as those UK sites which actively collect personal data are concerned, they would seem to fall into a grey area of the law, with the significant factor being what is done with the personal data

---

118 S24 (2)

119 S23 (1). There are also criminal sanctions for procuring disclosure of, and selling, computer-held personal information - s161 Criminal Justice and Public Order Act 1994.

collected. If an individual has a personal webpage with an embedded form being used as a 'visitors' book', their intention being to simply collect names, e-mail addresses, occupations and comments of visitors to the webpage for their own personal edification, it would seem that while they are obviously holding personal data, this would appear to fall under the recreation exemption. On the other hand if an institution collects the same personal data, it appears that the holding of that personal data would require registration, and at the time that it was obtained, the data subject would have to be informed both that it is being collected, and any purpose to which it might be put. This would be particularly relevant if the institution intended to use the personal data in a study,[120] or to sell it on to an interested third party.

A final thought concerns the use of search engines, webcrawlers and the like on the WWW and data retrieval mechanisms in other on-line resources. Given the ability to carry out searches on the names of individuals i.e. John Major, it may be possible for a person to download and then process information from one or more on-line sources which would qualify as personal data for the purposes of the DPA 1984. At that point that person would become a data user, and should register as such - however, as the volume of accessible electronic data increases, it remains to be seen just how feasible the requirement of registration becomes in such circumstances, given the present difficulty of getting larger data users to register correctly, or indeed at all.

[120] Subject to certain exemptions in Schedule 1, Art. 7, DPA 1984

Encryption

The issue of encryption technologies does not, as yet, appear to raise any major problems for UK educational sites. The UK government has, thus far, shown little interest in attempting to regulate or prohibit the creation, use, or export, of computer encryption technologies. This, however, is not true of other jurisdictions. Several countries regard encryption technology as potentially harmful and have taken steps to reduce or prevent that perceived harm. One aspect of this is demonstrated by the People's Republic of China which has banned encryption technology, presumably on the grounds that it would make it more difficult for the present authorities to monitor their citizens' communications.

In contrast, the United States offers a two pronged attack on the free availability of secure encryption technology. A number of law enforcement agencies, not least the Federal Bureau of Investigations (FBI) have been pushing legislation, which while it would not ban the encryption of electronic communications entirely, would attempt to ensure that the law enforcement agencies would have a "back-door" facility which would allow them to continue to monitor electronic communications where they could persuade a court that it was necessary.[121] So far, despite the increasingly emotive arguments about whether unrestricted encryption would allow child pornographers and drug dealers to communicate with absolute security, no US legislation has been forthcoming.[122]

The second prong of the attack, and the one of which most WWW users will have seen the result, is the US legislative ban on the export of certain encryption technology. Encryption software is classed under US law as 'munitions' and is thus subject to US export controls. Such controls include the banning of the passing of encryption technologies to certain blacklisted countries and individuals. The position of the US government as to the level of enforcement of these export controls is unfortunately unclear. This may be demonstrated by the recent decision of US Justice Department not to take any legal action against Philip Zimmermann, the inventor of the encryption software Pretty Good Privacy (PGP) over the release of that software to the wider Internet community.[123] However, it is these export controls which are responsible for the clause in the Netscape licence which states:

> EXPORT CONTROLS. None of the Software or underlying information or technology may be downloaded or otherwise exported or reexported (i) into (or to a national or resident of) Cuba, Iraq, Libya, Yugoslavia, North Korea, Iran, Syria or any other country to which the U.S. has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. By downloading or using the Software, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list.
>
> In addition, if the licensed Software is identified as a not-for-export product (for example, on the box, media or in the installation process), then the following applies: EXCEPT FOR EXPORT TO CANADA FOR USE IN CANADA BY CANADIAN CITIZENS, THE SOFTWARE AND ANY UNDERLYING TECHNOLOGY MAY

---

121 Denning, D.E. "Resolving the Encryption Dilemma: The Case for Clipper" *Technology Review* July 1995. <http://web.mit.edu/afs/athena/org/t/techreview/www/articles/july95/Denning.html>

122 See Froomkin, A.M. "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution" (1995) 143 *U. Pa. L. Rev.* 709.

123 Jeff Licquia, PGP FAQ: Frequently Asked Questions--alt.security.pgp. <http://www.prairienet.org/~jalicqui/pgpfaq.txt>

> NOT BE EXPORTED OUTSIDE THE UNITED STATES OR TO ANY FOREIGN ENTITY OR FOREIGN PERSON AS DEFINED BY U.S. GOVERNMENT REGULATIONS, INCLUDING WITHOUT LIMITATION, ANYONE WHO IS NOT A CITIZEN, NATIONAL OR LAWFUL PERMANENT RESIDENT OF THE UNITED STATES. BY DOWNLOADING OR USING THE SOFTWARE, YOU ARE AGREEING TO THE FOREGOING AND YOU ARE WARRANTING THAT YOU ARE NOT A FOREIGN PERSON OR UNDER THE CONTROL OF A FOREIGN PERSON.

This has caused some consternation at UK educational establishments, with regard to their legal position when distributing Netscape software to their staff and students either by electronic means, or on media such as floppy disks. A discussion of the issues raised by that licence is included in the Appendices.

International Issues

The growth of the Internet, and in particular the expansion of the WWW has led many countries to examine whether their existing law is able to cope with the potential problems that may arise. In the main, however, countries have refrained from rushing to create Internet specific laws. This is due in part to the volatility of the current situation, whereby it is impossible to predict either the speed of development or the direction of this medium. Many countries are unwilling to pass legislation which might have the effect of damaging their ability to take advantage of the commercial opportunities which may arise from the changes.
The US has been a significant exception to this, most notably with the passage of the Communications Decency Act 1996. (hereafter the CDA) [124] This Act sought to criminalise the activities of anyone who:

> "(B) by means of a telecommunications device knowingly -
>
> "(i) makes, creates, or solicits, and
> "(ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent knowing that the recipient of the communication is under 18 years of age regard less of whether the maker of such communication placed the call or initiated the communication;"

or

> "(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or
>
> (B) uses any interactive computer service to display in a manner available to a person under 18 years of age,
>
> any comment, request suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or
>
> "(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

The one of the main problems with the CDA was the use of the terms "indecent" and "patently offensive" which appeared to fall foul of the First Amendment to the US Constitution,[125] in that they were too broad in scope and unduly restricted freedom of speech.

"The constitutional challenge to the Communications Decency Act has been grounded in four basic arguments -- that the law is unconstitutionally overbroad (criminalizing protected speech), that it is

---

124 See <http://www.cpsr.org/cpsr/nii/cyber-rights/web/cda/cda.final.html> for the text of the CDA 1996.

125 **Amendment I**
Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

unconstitutionally vague (making it difficult for individuals and organizations to comply), that it fails what the judiciary calls the "least restrictive means" test for speech regulation, and that there is no basic constitutional authority under the First Amendment to engage in this type of content regulation in any nonbroadcast medium." [126]

The Act attracted a great deal of controversy during its passage through the US legislature, and an action to have it declared unconstitutional was filed by the American Civil Liberties Union shortly after it was signed into law by the US President.

On June 12 1996, Philadelphia's federal court (US District Court for the Eastern District of Pennsylvania) sitting as a three judge panel found the CDA to be unconstitutional on the grounds that it breached the U.S. constitutional guarantees of freedom of speech and of the press.[127] However, at the time of writing, it appears that the US government may be planning an appeal of the judgment to the United States Supreme Court, as a provision of the Telecommunications Reform Act of 1996 of which the CDA is a part allows such a direct appeal when a provision of that act is found unconstitutional in a lower court.

The saga of the CDA demonstrates that there is considerable concern about the impact of the Internet and the WWW, and the most effective methods of regulating on-line communications. If the Philadelphia court's judgment is overturned by the US Supreme Court (although most commentators seem to feel this is unlikely), America's pre-eminence on the Internet means that there may be repercussions at the international level. While it seems unlikely that the US courts would be willing, or able, to extend their jurisdiction under the Act to nationals of other countries, WWW content providers would still have to consider very carefully the material that they were intending to make available globally on the WWW, if they wished to maintain an effective presence there.

Despite the attention paid in this document to the provisions of UK law, it is important never to forget the international nature of the WWW. A webpage is usually accessible world-wide, and when putting either institutional or personal webpages on the WWW, it is worth considering who may view them. While there are jurisdictions more liberal than our own with regard to freedom of speech, such as the US, where pornography may, under certain circumstances, attract First Amendment protection, there are many that are not. At present, due to a lack of international agreement over Internet jurisdictional issues, it seems unlikely that a webpage on a machine at an educational institution in the UK, considered offensive or obscene by nationals of another country, would result in a successful (in terms of a penal sanction actually being applied) criminal prosecution being brought there, or in the UK. However, such a webpage might prove costly with regard to other activities of the educational institution, such as overseas student recruitment and research ventures, because of the negative publicity.

Looking to the future, as national law enforcement agencies world-wide develop new co-operative agreements in combating criminal activity such as child pornography, it seems likely that organised multi-jurisdictional investigations and jurisdiction hopping, to find the most favourable national venue for a successful prosecution, may yet become more prevalent. In such a co-operative climate, webpage owners may have to be prepared to deal sympathetically with the laws and values of countries other than their own, as the traditional print publishers have had to do, or consider restricting the accessibility of their material to specific Internet domains.

---

126 EFFector Online Volume 09 No. 08, June 12 1996. A Publication of the Electronic Frontier Foundation ISSN 1062-9424

127 AMERICAN CIVIL LIBERTIES UNION et al. v. JANET RENO, Attorney General of the United States. NO. 96-963. AMERICAN LIBRARY ASSOC. INC., et al. v. UNITED STATES DEP'T OF JUSTICE, et al. NO. 96-1458

Codes of Practice and Guidelines

Introduction

A useful starting point for consideration of the approach to be taken to the legal issues facing HE institutions in the UK is the Joint Academic Network's (JANET) Acceptable Use Policy. JANET provides links between most HE institutions in the UK, and the Policy states that the system should not be used for the following purposes:

- the creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- . the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- . the creation or transmission of defamatory material
- . the transmission of material such that this infringes the copyright of another person.

In addition, HE institutions are required to "take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of JANET does not occur. The discharge of this responsibility must include informing those at the Organisation with access to JANET of their obligations in this respect." Thus the Policy lays out some broad pointers as to what is considered unacceptable use of the system, and more importantly, places the onus for informing the end user, on the individual HE institutions. It is useful to note the "catch-all" nature of the second category, as use of such "catch-all" provisions in institutional regulations can provide the flexibility required to adequately regulate a rapidly changing environment.

Writing a code of practice.

It is important to remember when considering an institutional approach to the setting up and use of WWW servers and homepages, that the unwritten first rule of civil litigation is "never sue poor people". Thus, if a plaintiff is given the choice between suing a student or staff member, and suing an HE institution, they are unlikely to pursue the student or staff member. As a result, when writing an institutional code of practice, it is advisable to place precise restrictions on who may set up a Webserver on any machine within the institution - the fewer the Webservers that exist, the easier it is to develop effective regulation. Similarly, it is wise to maintain a clear separation between official institutional webpages and personal webpages. This may be achieved by restricting the use of official logos and designations to institutional webpages, and by placing a notification and disclaimer page between institutional webpages and links to personal webpages at the institution and all other webpages beyond the control of the institution. It is important to have a coherent structure of responsibility in place, particularly where an institution has a Webserver with multiple official departmental homepages or multiple official departmental Webservers. In such circumstances there should be a designated staff member within each of those departments with responsibility for their maintenance and content, and a staff member with the power to remove potentially damaging material from both institutional and personal webpages, as soon as it is brought to the attention of the institution, until such time as it can be verified whether or not some civil or criminal liability may be incurred by its display.

At present, if an institution allows personal webpages to be held on its machines, it is desirable to have both the notification and disclaimer page mentioned above, and also a statement in the code of practice to the effect that the institution does not exercise any editorial control over personal webpages. This may allow for a defence of "innocent dissemination" in circumstances where staff or students publish defamatory statements. However, this should be accompanied by a statement that where the institution is notified by third parties that defamatory, infringing or criminal material is being held on its machines it will

take all reasonable steps to ensure its removal in a timely manner. This approach may become less practicable if the current draft Defamation Bill being circulated by the Lord Chancellor's Department becomes law, as this would require the institution to take reasonable steps to ensure defamatory material was not published. There is a considerable degree of uncertainty at present as to whether such reasonable steps would entail an institution monitoring all web pages held on its machines, potentially an impossible task.. If that were to be the case, it would seem likely that most HE institutions would follow the lead already taken by several of their number, and simply ban all personal webpages from machines under their control.

The code of practice should also make clear the penalties for unacceptable use. Such penalties would usually include the statement that where there is a breach of the code of practice, or where an individual's webpage is deemed by the authorities at the institution to bring the name and/or reputation of that institution into disrepute, this may result in the temporary or permanent withdrawal of computer services.

As an adjunct to any code of practice, there should be a set of clear guidelines for individuals wishing to maintain webpages. These guidelines should contain advice as to the design and content of webpages, including use of university logos. They should also contain advice as to the type of sites which the institution considers it inappropriate or unacceptable for pages maintained on its machines to link to. These would probably include sites known to contain pornography, defamatory materials, illegally copied software and other copyrighted works, as well as other inappropriate materials, such as hacker manuals, and racist and sexist tracts. It should be noted that institutions have a wide discretion in deciding what is not appropriate, and may thus ban links to material which is not illegal *per se*. It may be helpful to put the institution's policy into context by including the JANET Acceptable Use Policy, as this demonstrates that the institution is to a large extent bound by its obligations to JANET, and that the restrictions imposed are not merely an arbitrary whim of the institution's computer services department or administration. The guidelines should also provide a brief summary of the relevant laws, in particular those relating to libel, obscenity, intellectual property and data protection.

Prospective users of an institution's computer systems should be provided with a copy of the code of practice and the guidelines, and informed that use of the institution's computer systems will be taken as acceptance of the institutional rules contained within them. Login screens may also refer the user to their acceptance of the code of practice and guidelines each time they access the computer systems.

In a large HE institution, it is next to impossible to effectively monitor the use of WWW facilities by staff and students. However, a carefully thought-out code of practice combined with an effective regulatory system can be used to shield the institution from the majority of legal risks posed by the WWW, and it will ill behoove any HE institution to fail to take advantage of that protection in the coming years.

Considerations when creating a Code of Practice

A code of practice should:

- Reflect a clear institutional approach to the setting up and use of Webservers and Webpages
- Ensure a clear separation between institutional Webpages and personal Webpages, including notification and disclaimer when a user leaves the institutional Webpages.
- Provide for a coherent internal structure of responsibility for general institutional and departmental Webpages, and the ability to respond quickly to remove potentially damaging material.
- State that the institution does not exercise direct editorial control over personal Webpages.
- Provide for sanctions for breach of the code of practice, including, where necessary, temporary or permanent removal of computer services.
- Provide clear guidelines for WWW use for all institutional users.

Institutional Guidelines for using the World Wide Web.

The guidelines should:

- Provide clear advice on the design and content of Webpages.
- Provide clear advice as to types of sites considered unacceptable to link to.
- Include the JANET Acceptable Use Policy.
- Include a brief summary of the relevant laws, especially those relating to libel, obscenity, intellectual property and data protection.

Draft Institutional Code of Practice

1. The [name of institution] has the following Code of Practice and Guidelines with regard to the setting up and use of Webservers and Webpages, which should be read in conjunction with the JANET Acceptable Use Policy and the University's Regulations on Use of Computer Services [or equivalent].

2. Staff and students may only set up a Webserver on machinery owned by, or on the premises of, the [name of institution] with the written permission of [insert individual's name here]. They must be registered and have signed a declaration that they have read and understood both the Code of Practice and Guidelines for Users. All pages must include the name of their author (real name, not just username), and must be linked (by means of <a href="">) to the hypertext tree that has the staff member's or student's home page at its root.

Or

2. Staff and students may not set up Webservers, or place Webpages on any University Computing equipment, other than that designated. All staff and students wishing to place Webpages on designated University Computing equipment must be registered and have signed a declaration that they have read and understood both Code of Practice and Guidelines. All pages must include the name of their author (real name, not just username), and must be linked (by means of <a href="">) to the hypertext tree that has the staff member's or student's home page at its root.

3. There must be a clear separation between institutional Webpages and personal Webpages, to this end, only official institutional Webpages may use University logos, or other copyrighted or trademarked University materials, and when users leave the official institutional pages, they should be informed of this fact by a notification and disclaimer. Authors of personal homepages have no authority to designate, represent or hold out such pages as being official institutional University webpages, to use such pages for official University business, or to use such pages to enter into contracts which purport to bind the University.

4. Institutional and personal webpages may not:
   - contain, or be used to distribute, or have direct links to, material which is sexist, racist, homophobic, xenophobic, pornographic, or similarly discriminatory and/or offensive.
   - contain, or be used to distribute, or have direct links to, text or images to which a third party holds a intellectual property right, without the express written permission of the rightholder.
   - contain, or be used to distribute, or have direct links to, defamatory material, that is, they may not contain material which falsely states or implies something about an identifiable individual that will result in that individual being held in lower esteem by others as a result.
   - contain, or be used to distribute, or have direct links to, material that could be used in order to breach computer security, or to facilitate unauthorised entry into computer systems.
   - contain, or be used to distribute, or have direct links to, material which is likely to prejudice or seriously impede the course of justice in criminal or civil proceedings.
   - contain personal data (as defined by the Data Protection Act 1984) about third parties, unless their explicit permission has been given, or the information is properly registered

with the Data Protection Registrar, or the information is covered by a relevant exemption under the Data Protection Act 1984.

In particular, institutional and personal webpages may not contain, or be used to distribute, or have direct links to, material which breaches, or is likely to likely to breach:
The Obscene Publications Act 1959, The Sex Discrimination Act 1975, The Race Relations Act 1976, The Protection of Children Act 1978, The Contempt of Court Act 1981, The Data Protection Act 1984, The Telecommunications Act 1984, The Public Order Act 1986, The Copyright, Designs and Patents Act 1988, The Computer Misuse Act 1990, The Trademarks Act 1994.

5. Personal webpages may not be used for placing and distribution of commercial advertisements.

Or

5. If advertisements are placed on personal homepages, they must comply with the Code of Practice for Advertisers issued by the Advertising Standards Authority which requires in summary that all advertisements should be `legal, decent, truthful and honest'.

6. The University has an internal structure of responsibility for the administration of institutional, departmental and personal Webpages. Complaints and comments should be directed to [insert individual's name or position here] who will ensure that, they are promptly dealt with by the relevant responsible individuals named below, and that any necessary disciplinary action against members of the University is taken.
The following are responsible for dealing with queries and complaints about their respective areas. They have the authority to remove webpages within their respective areas of responsibility which infringe, or may infringe, the University Code of Practice, or University Regulations on use of Computer Services:
[insert individual's name or position here and area of responsibility]
[insert individual's name or position here and area of responsibility]

Or

6. The University has an internal structure of responsibility for the administration of institutional, departmental and personal Webpages. Complaints and comments should be directed to [insert individual's name or position here] who will ensure that, they are promptly dealt with by the relevant responsible individuals named below, and that any necessary disciplinary action against members of the University is taken.
The University's Institutional Webpages are administered by [insert individual's name or position]. He/She has the authority to remove webpages which infringe, or may infringe, the University Code of Practice, or University Regulations on use of Computer Services.
Staff and student personal webpages are administered by [insert individual's name or position]. He/She has the authority to remove webpages which infringe, or may infringe, the University Code of Practice, or University Regulations on use of Computer Services.

7. The above sections notwithstanding, the University does not exercise direct editorial control over personal Webpages, and accepts no liability for material contained in them, or links which are made from them to other material either at, or outside, the University. However, in the event of a complaint, the University will act to ensure that the material or link in question is removed, as soon as practically possible, until the complaint is either substantiated or dismissed.

8. Failure to observe this code of practice by either students or staff will be considered a serious matter by the University. Where University regulations are breached the University will invoke the appropriate disciplinary procedures. For students this could involve fines, suspension of access to computing facilities or, in extreme cases, termination of their studies. Breaches of the criminal or civil law are beyond the remit of the University, but where criminal offences have been committed, the University will report these to the authorities. If the DPP decides upon a criminal prosecution this will be a matter for the department or individual concerned.. Similar considerations apply to any civil law cases.

Draft Institutional Guidelines for Personal Webpages

1. You may only set up a WWW server on machinery owned by, or on the premises of, the [name of institution] with the written permission of [insert individual's name here]. You must be registered and have signed a declaration that you have read and understood both the Code of Practice and Guidelines for Users. All your pages must include the your name (real name, not just username) and must be linked (by means of <a href="">) to the hypertext tree that has the your home page at its root.

   Or

1. You may not set up WWW servers, or place WWW pages on any University Computing equipment, other than that designated by the University. If you wish to place WWW pages on designated University Computing equipment you must register to do so, and have signed a declaration that you have read and understood both the Code of Practice and Guidelines for Users. All pages must include your name (real name, not just username) and must be linked (by means of <a href="">) to the hypertext tree that has your home page at its root.

2. Only official institutional Webpages may use University logos, or other copyrighted or trademarked University materials. Thus, you may not incorporate the University logo or any School, Departmental, Unit, Institute or Centre logo into your webpage. Equally materials published by the University, including the contents of brochures, handbooks and other publicity materials may not be used. You are not permitted to designate, represent or hold out your pages as being official institutional University webpages, to use your pages for official University business, or to use your pages to enter into contracts which purport to bind the University.

3. Personal webpages may not:
   - contain, or be used to distribute, or have direct links to, material which is sexist, racist, homophobic, xenophobic, pornographic, or similarly discriminatory and/or offensive
   - contain, or be used to distribute, or have direct links to, text or images to which a third party holds a intellectual property right, without the express written permission of the rightholder. Thus copyrighted material, such as novels, poetry, non-fiction books, letters, memoranda, directories, e-mail messages, photographs, paintings, films, video, sound recordings, cartoons etc. should be used with only where you are sure that copyright has expired, or that you have explicit permission to use them; and trademarked logos such as those used by Microsoft®, Coca Cola®, and Camel® should not be used without permission.
   - contain, or be used to distribute, or have direct links to, defamatory material,. That is, they may not contain material which falsely states or implies something about an identifiable individual that will result in that individual being held in lower esteem by others as a result.
   - contain, or be used to distribute, or have direct links to, material that could be used in order to breach computer security, or to facilitate unauthorised entry into computer systems. This includes, but is not limited to: viruses; virus creation kits; User IDs and passwords obtained without authorisation, or which you have no authority to disclose to others; and "hacker manuals".
   - contain, or be used to distribute, or have direct links to, material which is likely to prejudice or seriously impede the course of justice in UK criminal or civil proceedings. This includes: material which prejudges a case, especially where it makes the express or tacit assumption that the accused in a criminal trial is guilty; material which is emotive or disparaging, especially where there is an insinuation of complicity or guilt by association; material which

is likely to be inadmissible at trial, such as previous convictions, or mention of evidence likely to be excluded as having been improperly obtained; material such as a photograph of the defendant, where the issue of identification forms part of the trial proceedings; material hostile or abusive towards potential witnesses with the intention of coercing them into not testifying, or disclosure of witnesses' names following a court order that their names should not be disclosed material disclosing information about jury deliberations; material breaching reporting restrictions in cases such where in open court there is identification of children involved in the proceedings, or identification of rape victims; material relating to court proceedings closed to the public, including where there is an issue of national security.

- contain personal data (as defined by the Data Protection Act 1984) about third parties, unless their explicit permission has been given, or the information is properly registered with the Data Protection Registrar, or the information is covered by a relevant exemption.

In particular, personal webpages may not contain material which breaches, or is likely to likely to breach:

The Obscene Publications Act 1959, The Sex Discrimination Act 1975, The Race Relations Act 1976, The Protection of Children Act 1978, The Contempt of Court Act 1981, The Data Protection Act 1984, The Telecommunications Act 1984, The Public Order Act 1986, The Copyright, Designs and Patents Act 1988, The Computer Misuse Act 1990, The Trademarks Act 1994.

If you are in any doubt as to the acceptability or legality of material which you wish to place on your personal webpages you should contact [insert individual's name or position here] for advice.

6. Personal webpages may not be used for placing and distribution of commercial advertisements.

Or

6. If advertisements are placed on personal homepages, then they must comply with the Code of Practice for Advertisers issued by the Advertising Standards Authority which requires in summary that all advertisements should be `legal, decent, truthful and honest'.

7. You should be aware of and abide by the regulations that apply to you as a user of a Web Server at the [name of institution] and as a user of University Computing Services. These include:

   - UKERNA's JANET Acceptable Use Policy.
   - The University Code of Practice with regard to the setting up and use of Webservers and Webpages.
   - Such University regulations as govern the use of University Computer resources.

   Failure to observe the University Code of Practice by either students or staff will be considered a serious matter by the University. Where University Regulations are breached the University will invoke the appropriate disciplinary procedures. For students this could involve fines, suspension of access to computing facilities or, in extreme cases, termination of their studies. Any breaches of the criminal or civil law are beyond the remit of the University, but where criminal offences have been committed, the University will report these to the authorities. If the DPP decides upon a criminal prosecution this will be a matter for the department or individual concerned.. Similar considerations apply to any civil law cases.

8. If you believe that a member of the University has personal web pages which contravene these conditions, you should report your concern by email, indicating the location and nature of the

offending material, to [insert individual's name or position here] who will ensure that it is are promptly dealt with by the relevant individual responsible for the area at issue, and that any necessary disciplinary action is taken.

Draft Campus Wide Information Server (CWIS) /Official Institutional Webserver Committee Guidelines.

1. The CWIS should have a properly constituted Committee or Editorial Board within which responsibility for particular administrative action is clearly allocated. In particular, an individual or individuals with responsibility for handling complaints about the content of the CWIS and the power to remove or amend such content as necessary, and an individual or individuals with responsibility for maintaining the register described in section 7 should be clearly prescribed.

2. The CWIS must meet the standards set in the [name of institution]'s Code of Practice for its Webservers, notably that it is free from material which is defamatory, infringes intellectual property rights, infringes the Data Protection Act, or is sexist, racist, homophobic, xenophobic, pornographic, or similarly discriminatory and/or offensive.

3. With regard to copyright, the CWIS Committee or Editorial Board should endeavour ensure that the [name of Institution] obtains all intellectual property rights in the material to be used. Where the owner of the intellectual property rights in material cannot be definitely ascertained, that material should not be used, and this applies especially to material obtained from the Internet.

4. The copyright in work carried out on the CWIS by the [name of institution]'s employees during the normal course of their employment will normally vest in the [name of institution]. Where there is any doubt as to whether the work is carried out during the normal course of their employment, agreement of ownership of the intellectual property rights should be obtained in advance.

5. When external providers of information and other materials are used, agreement of ownership of the intellectual property rights should be obtained in advance. Ideally the [name of institution] will ask for an assignment of all intellectual property rights from the external provider. Where this is not possible permission to use the material by way of licence should be obtained in writing.

6. When external providers of information and other materials are used, indemnities should be sought in advance by the [name of institution] that the material is free from third party intellectual property rights, and that it is not of a defamatory nature. Such indemnities should, in the event of legal action, endeavour to pass as much of the liability as possible to the external provider.

7. A centrally maintained register of all third party supplied materials should be kept by [name of individual or administrative position], containing relevant assignments of intellectual property rights, the terms and conditions of any intellectual property licences obtained, and all indemnities.

8. Guidelines for all external providers of information and other materials with regard to the [name of institution]'s position on intellectual property rights and indemnities should be produced and supplied to the external providers, in advance of material being commissioned.

Appendices

Telecommunications Act 1984 s42-43
Interception of Communications Act 1985 s1-2
Computer Misuse Act 1990 s1-6, 8-10,12,15,17
Criminal Justice and Public Order Act 1994 s84-86, s161-162
Duration of Copyright and Rights in Performances Regulations 1995 s23-25
Opinion on the terms of the Netscape User Licence

Telecommunications Act 1984

s42. Fraudulent use of telecommunication system

(1) A person who dishonestly obtains a service to which this subsection applies with intent to avoid payment of any charge applicable to the provision of that service shall be guilty of an offence and liable--

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(b) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

(2) Subsection (1) above applies to any service (other than a service to which section 53 of the Cable and Broadcasting Act 1984 applies) which is provided by means of a telecommunication system the running of which is authorised by a licence granted under section 7 [of this Act].

s43 Improper use of public telecommunication system

(1) A person who--

(a) sends, by means of a public telecommunication system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or

(b) sends by those means, for the purpose of causing annoyance, inconvenience or needless anxiety to another, a message that he knows to be false or persistently makes use for that purpose of a public telecommunication system, shall be guilty of an offence and liable on summary conviction to a fine not exceeding level 3 on the standard scale.

(2) Subsection (1) above does not apply to anything done in the course of providing a [programme service (within the meaning of the Broadcasting Act 1990)] . . .

Annotations: Commencement order: SI 1984 No 876.

Sub-s (2): words in square brackets substituted by the Broadcasting Act 1990, s 203(1), Sch 20, para 38(4); words omitted repealed by the Cable and Broadcasting Act 1984, s 57, Sch 5, para 45, Sch 6.

Interception of Communications Act 1985

1 Prohibition on interception

(1) Subject to the following provisions of this section, a person who intentionally intercepts a communication in the course of its transmission by post or by means of a public telecommunication system shall be guilty of an offence and liable-

(a) on summary conviction, to a fine not exceeding the statutory maximum;

(b) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

(2) A person shall not be guilty of an offence under this section if-

(a) the communication is intercepted in obedience to a warrant issued by the Secretary of State under section 2 below; or

(b) that person has reasonable grounds for believing that the person to whom, or the person by whom, the communication is sent has consented to the interception.

(3) A person shall not be guilty of an offence under this section if-

(a) the communication is intercepted for purposes connected with the provision of postal or public telecommunication services or with the enforcement of any enactment relating to the user of those services; or

(b) the communication is being transmitted by wireless telegraphy and is intercepted, with the authority of the Secretary of State, for purposes connected with the issue of licences under the Wireless Telegraphy Act 1949 or the prevention or detection of interference with wireless telegraphy.

(4) No proceedings in respect of an offence under this section shall be instituted--

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) In Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland

2 Warrants for interception

(1) Subject to the provisions of this section and section 3 below, the Secretary of State may issue a warrant requiring the person to whom it is addressed to intercept, in the course of their transmission by post or by means of public telecommunication system, such communications as are described in the warrant; and such a warrant may also require the person to whom it is addressed to disclose the intercepted material to such persons and in such manner as are described in the warrant.

(2) The Secretary of State shall not issue a warrant under this section unless he considers that the warrant is necessary--

(a) in the interests of national security;

(b) for the purpose of preventing or detecting serious crime or;

(c) for the purpose of safeguarding the economic well-being of the United Kingdom.

(3) The matters to be taken into account in considering whether a warrant is necessary as mentioned in subsection (2) above shall include whether the information which it is considered necessary to acquire could reasonably be acquired by other means.

(4) A warrant shall not be considered necessary as mentioned in subsection (2)(c) above unless the information which it is considered necessary to acquire is information relating to the acts or intentions of persons outside the British Islands.

(5) References in the following provisions of this Act to a warrant are references to a warrant under this section.

Computer Misuse Act 1990

Computer misuse offence

1.--(1) A person is guilty of an offence if-

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at-

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

2.--(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent--

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences--

(a) for which the sentence is fixed by law; or

(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable--

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

3.--(1) A person is guilty of an offence if--

(a) he does any act which causes an unauthorised modification of the contents of any computer, and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing--

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at--

(a) any particular computer;

(b) any particular program or data or particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection(1)(b)above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.
(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.
(6) For the purposes of the Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.
(7) A person guilty of an offence under this section shall be liable--
(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Jurisdiction
4.--(1) Except as provided below in this section. it is immaterial for the purposes of any offence under section 1 or 3 above--
(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or
(b) whether the accused was in the home country concerned at the time of any such act or event.
(2) Subject to subsection (3) below, in the case of such an offence at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed.
(3) There is no need for any such link to exist for the commission of an offence under section I above to be established in proof of an allegation to that effect in proceedings for an offence under section 2 above.
(4) Subject to section 8 below, where--
(a) any such link does in fact exist in the case of an offence under section I above; and
(b) commission of that offence is alleged in proceedings for an offence under section 2 above;
section 2 above shall apply as if anything the accused intended to do or facilitate in any place outside the home country concerned which would be an offence to which section 2 applies if it took place in the home country concerned were the offence in question.
(5) This section is without prejudice to any jurisdiction exercisable by a court in Scotland apart from this section.
(6) References in this Act to the home country concerned are references--
(a) in the application of this Act to England and Wales, to England and Wales
(b) in the application of this Act to Scotland, to Scotland; and
(c) in the application of this Act to Northern Ireland, to Northern Ireland.

5.--(1) The following provisions of this section apply for the interpretation of section 4 above.
(2) In relation to an offence under section 1, either of the following is a significant link with domestic jurisdiction--
(a) that the accused was in the home country concerned at the time when he did the act which caused the computer to perform the function, or
(b) that any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the home country concerned at that time.
(3) In relation to an offence under section 3, either of the following is a significant link with domestic jurisdiction--
(a) that the accused was in the home country concerned at the time when he did the act which caused the unauthorised modification- or
(b) that the unauthorised modification took place in the home country concerned

6.--(1) On a charge of conspiracy to commit an offence under this Act the following questions are immaterial to the accused's guilt
(a) the question where any person became a party to the conspiracy; and
(b) the question whether any act, omission or other event occurred in the home country concerned.
(2) On a charge of attempting to commit an offence under section 3 above the following questions are immaterial to the accused's guilt--
(a) the question where the attempt was made; and
(b) the question whether it had an effect in the home country concerned .
(3) On a charge of incitement to commit an offence under this Act the question where the incitement took place is immaterial to the accused's guilt.
(4) This section does not extend to Scotland.

[material omitted]

8.--(1) A person is guilty of an offence triable by virtue of section 4(4) above only if what he intended to do or facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.
(2) A person is guilty of an offence triable by virtue of section 1 (1A) of the Criminal Law Act 1977 only if the pursuit of the agreed course of conduct would at some stage involve--
(a) an act or omission by one or more of the parties; or
(b) the happening of some other event;
constituting an offence under the law in force where the act, omission or other event was intended to take place.
(3) A person is guilty of an offence triable by virtue of section 1 (1A) of the Criminal Attempts Act 1981 or by virtue of section 7(4) above only if what he had in view would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.
(4) Conduct punishable under the law in force in any place is an offence under that law for the purposes of this section, however it is described in that law.
(5) Subject to subsection (7) below, a condition specified in any of the subsections (1) to (3) above shall be taken to be satisfied unless not later than rules of court may provide the defence serve on the prosecution a notice--
(a) stating that, on the facts as alleged with respect to the relevant conduct, the condition is not in their opinion satisfied;
(b) showing the grounds for that opinion; and
(c) requiring the prosecution to show that it is satisfied.
(6) In subsection (5) above "the relevant conduct" means--
(a) where the condition in subsection (1) above is in question, what the accused intended to do or facilitate:
(b) where the condition in subsection (2) above in question, the agreed course of conduct; and
(c) where the condition in subsection (3) above is in question, what the accused had in view.
(7) The court, if it thinks fit, may permit the defence to require the prosecution to show that the condition is satisfied without the prior service of a notice under subsection (5) above.
(8) If by virtue of subsection (7) above a court of solemn jurisdiction in Scotland permits the defence to require the prosecution to show that the condition is satisfied, it shall be competent for the prosecution for that purpose to examine any witness or to put in evidence any production not included in the lists lodged by it.
(9) In the Crown Court the question whether the condition is satisfied shall be decided by the judge alone.
(10) In the High Court of Justiciary and in the sheriff court the question whether the condition is satisfied shall be decided by the judge or, as the case may be, the sheriff alone.

9.--(1) In any proceedings brought in England and Wales in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a British citizen at the time of any act, omission or other event proof of which is required for conviction of the offence.
(2) This section applies to the following offences--
(a) any offence under this Act;
(b) conspiracy to commit an offence under this Act;
(c) any attempt to commit an offence under section 3 above; and
(d) incitement to commit an offence under this Act.

Miscellaneous and general
10.--Section 1(1) above has effect without prejudice to the operation--
(a) in England and Wales of any enactment relating to powers of inspection, search or seizure; and
(b) in Scotland of any enactment or rule of law relating to powers of examination. search or seizure.

[material omitted]

12.--(1) If the trial on indictment of a person charged with--
(a) an offence under section 2 above; or
(b) an offence under section 3 above or any attempt to commit such an offence;
the jury find him not guilty of the offence charged, they may find him guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence brought before the expiry of any time limit under section 11 above applicable to such proceedings.
(2) The Crown Court shall have the same powers and duties in relation to a person who is by virtue of this section convicted before it on an offence under section 1 above as a magistrates' court would have on convicting him of the offence.
(3) This section is without prejudice to section 6(3) of the Criminal Law Act 1967 (conviction of alternative indictable offence on trial on indictment).
(4) This section does not extend to Scotland.

[material omitted]

15. The offences to which an Order in Council under section 2 of the Extradition Act 1870 can apply shall include--
(a) offences under section 2 or 3 above;
(b) any conspiracy to commit such an offence; and
(c) any attempt to commit an offence under section 3 above.

[material omitted]

17.--(1) The following provisions of this section apply for the interpretation of this Act.
(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he--
(a) alters or erases the program or data;
(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
(c) uses it; or
(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);
and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform--
(a) causes the program to be executed; or
(b) is itself a function of the program.
(4) For the purposes of subsection (2)(d) above--
(a) a program is output if the instructions of which it consists are output; and
(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.
(5) Access of any kind by any person to any program or data held in a computer is unauthorised if--
(a) he is not himself entitled to control access to the kind in question to the program or data; and
(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.
(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.
(7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer--
(a) any program or data held in the computer concerned is altered or erased; or
(b) any program or data is added to its contents;
and any act which contributes towards causing such a modification shall be regarded as causing it.
(8) Such a modification is unauthorised if--
(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and
(b) he does not have consent to the modification from any person who is so entitled.
(9) References to the home country concerned shall be read in accordance with section 4(6) above.
(10) References to a program include references to part of a program.

[material omitted]

Criminal Justice and Public Order Act 1994

PART VII
OBSCENITY AND PORNOGRAPHY AND VIDEOS

Obscene publications and indecent photographs of children

Indecent pseudo-photographs of children

84.—(1) The Protection of Children Act 1978 shall be amended as provided in subsections (2) and (3) below.

(2) In section 1 (which penalises the taking and distribution of indecent photographs of children and related acts)-

(a) in paragraph (a) of subsection (1) -

(i) after the word "taken" there shall be inserted the words "or to make", and the words following "child" shall be omitted;

(ii) after the word "photograph" there shall be inserted the words "or pseudo-photograph";

(b) in paragraphs (b), (c) and (d) of subsection (1), after the word "photographs" there shall be inserted the words "or pseudo-photographs";

(c) in subsection (2), after the word "photograph" there shall be inserted the words "or pseudo-photograph"; and

(d) in paragraphs (a) and (b) of subsection (4), after the word "photographs" there shall be inserted the words "or pseudo-photographs".

(3) In section 7 (interpretation)—

(a) in subsection (3), at the end, there shall be inserted the words "and so as respects pseudo-photographs", and

(b) for subsection (4) there shall be substituted the following subsection—

"(4) References to a photograph include—

(a) the negative as well as the positive version, and

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

(c) after subsection (5) there shall be inserted the following subsections—

"(6) 'Child', subject to subsection (8), means a person under the age of 16.

(7) 'Pseudo-photograph' means an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph.

(8) If the impression conveyed by a pseudo-photograph is that the person shown is a child, the pseudo-photograph shall be treated for all purposes of this Act as showing a child and so shall a pseudo-photograph where the predominant impression conveyed is that the person shown is a child notwithstanding that some of the physical characteristics shown are those of an adult.

(9) References to an indecent pseudo-photograph include—

(a) a copy of an indecent pseudo-photograph, and

(b) data stored on a computer disc or by other electronic means which is capable of conversion into a pseudo-photograph.".

(4) Section 160 of the Criminal Justice Act 1988 (which penalises the possession of indecent photographs of children) shall be amended as follows—

(a) in subsection (1), after the word "photograph" there shall be inserted the words "or pseudo-photograph" and the words from "(meaning" to "16)" shall be omitted, and

(b) in paragraphs (a), (b) and (c) of subsection (2), after the word "photograph" there shall be inserted the words "or pseudo-photograph"; and

(c) in subsection (5), the reference to the coming into force of that section shall be construed, for the purposes of the amendments made by this subsection, as a reference to the coming into force of this subsection.

(5) The Civic Government (Scotland) Act 1982 shall be amended as provided in subsections (6) and (7) below.

(6) In section 52 (which, for Scotland, penalises the taking and distribution of indecent photographs of children and related acts)—

(a) in paragraph (a) of subsection (1)— (i) after the word "taken" there shall be inserted the words "or makes", and (ii) for the words from "of a" to the end there shall be substituted the words "or pseudo-photograph of a child"

(b) in paragraphs (b), (c) and (d) of subsection (1), after the word "photograph" there shall be inserted the words "or pseudo-photograph"; and

(c) in subsection (2), at the beginning there shall be inserted "In subsection (1) above "child" means, subject to subsection (2B) below, a person under the age of 16, and"

(d) after subsection (2), there shall be added—

"(2A) In this section, "pseudo-photograph" means an image, whether produced by computer-graphics or otherwise howsoever, which appears to be a photograph.

(2B) If the impression conveyed by a pseudo-photograph is that the person shown is a child, the pseudo-photograph shall be treated for all purposes of this Act as showing a child and so shall a pseudo-photograph where the predominant impression conveyed is that the person shown is a child notwithstanding that some of the physical characteristics shown are those of an adult.

(2C) In this section, references to an indecent pseudo-photograph include—

(a) a copy of an indecent pseudo-photograph;

(b) data stored on a computer disc or by other electronic means which is capable of conversion into a pseudo-photograph.".

(e) in subsection (3)— (i) in paragraph (a), for the words "3 months" there shall be substituted the words "6 months"; and (ii) in paragraph (b), for the words "two years" there shall be substituted the words "3 years";

(f) in subsection (4), and in paragraphs (a) and (b) of subsection (5), after the word "photograph" there shall be inserted the words "or pseudo-photograph"; and

(g) for subsection (8)(c) there shall be substituted—

"(c) references to a photograph include—

(i) the negative as well as the positive version; and

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

(7) In section 52A (which, for Scotland, penalises the possession of indecent photographs of children)—

(a) in subsection (1), for the words from "of a" to "16)" there shall be substituted the words "or pseudo-photograph of a child";

(b) in subsection (2), in each of paragraphs (a) to (c), after the word "photograph" there shall be inserted the words "or pseudo-photograph"

(c) in subsection 63)— (i) after the word "to" there shall be inserted the words "imprisonment for a period not exceeding 6 months or to"; and (ii) at the end there shall be added the words "or to both.";

(d) in subsection (4), after the word "(2)" there shall be inserted the words "to (2C)"

(8) The Protection of Children (Northern Ireland) Order 1978 shall be amended as provided in subsections (9) and (10) below.

(9) In Article 2 (interpretation)—

(a) in paragraph (2)—

(i) in the definition of "child", after "child" there shall be inserted the words "subject to paragraph (3)(c)"

(ii) for the definition of "photograph" there shall be substituted the following definitions—

"indecent pseudo-photograph" includes—

(a) a copy of an indecent pseudo-photograph; and

(b) data stored on a computer disc or by other electronic means which is capable of conversion into a pseudo-photograph;

"photograph" includes—

(a) the negative as well as the positive version, and

(b) data stored on a computer disc or by other electronic means which is capable of conversion into a photograph; "pseudo-photograph" means an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph;";

(b) in paragraph (3)—

(i) in sub-paragraph (a), after the word "photograph" there shall be inserted the words "or pseudo-photograph"

(ii) in sub-paragraph (b), at the end, there shall be inserted the words "and so as respects pseudo-photographs, and"

(iii) after sub-paragraph (b) there shall be inserted the following sub-paragraph—

"(c) if the impression conveyed by a pseudo-photograph is that the person shown is a child, the pseudo-photograph shall be treated as showing a child and so shall a pseudo-photograph where the predominant impression conveyed is that the person shown is a child notwithstanding that some of the physical characteristics shown are those of an adult.".

(10) In Article 3 (which, for Northern Ireland, penalises the taking and distribution of indecent photographs of children and related acts)—

(a) in sub-paragraph (a) of paragraph (1)—

(i) after the word "taken" there shall be inserted the words "or to make"

(ii) after the word "photograph" there shall be inserted the words "or pseudo-photograph"

(b) in sub-paragraphs (b), (c) and (d) of paragraph (1), after the word "photographs" there shall be inserted the words "or pseudo-photographs"

(c) in sub-paragraphs (a) and (b) of paragraph (3), after the word "photographs" there shall be inserted the words "or pseudo-photographs".

(11) Article 15 of the Criminal Justice (Evidence, etc.) (Northern Ireland) Order 1988 (which, for Northern Ireland, penalises the possession of indecent photographs of children) shall be amended as follows—

(a) in paragraph (1), after the word "photograph" there shall be inserted the words “pseudo-photograph" and the words from "(meaning" to "16)" shall be omitted

(b) in sub-paragraphs (a), (b) and (c) of paragraph (2), after the word "photograph" there shall be inserted the words "or pseudo-photograph: and

(c) in paragraph (6), the reference to the coming into operation of that Article shall be construed, for the purposes of the amendments made by this subsection, as a reference to the coming into force of this subsection.

Arrestable offences to include certain offences relating to obscenity or indecency

85.—(1) The Police and Criminal Evidence Act 1984 shall be amended as follows.

(2) In section 24(2) (arrestable offences), after paragraph (e), there shall be inserted the following paragraphs—

"(f) an offence under section 2 of the Obscene Publications Act 1959 (publication of obscene matter);

(g) an offence under section 1 of the Protection of Children Act 1978 (indecent photographs and pseudo-photographs of children);".

(3) At the end of Part II of Schedule 5 (serious arrestable offences mentioned in section 116(2)(b)) there shall be inserted the following paragraphs—

"Protection of Children Act 1978 (c. 37)

14. Section 1 (indecent photographs and pseudo-photographs of children)

Obscene Publications Act 1959 (c. 66)

15. Section 2 (publication of obscene matter).".

(4) The Police and Criminal Evidence (Northern Ireland) Order 1989 shall be amended as provided in subsections (5) and (6) below.

(5) In Article 26(2) (arrestable offences), after sub-paragraph (e), there shall be inserted the following sub-paragraph—

"(f) an offence under Article 3 of the Protection of Children (Northern Ireland) Order 1978 (indecent photographs and pseudo-photographs of children).".

(6) At the end of Part II of Schedule 5 (serious arrestable offences mentioned in Article 87(2)(b)) there shall be inserted the following paragraph—

"Protection of Children (Northern Ireland) Order 1978 (1978 N.I. 17)

13. Article 3 (indecent photographs and pseudo-photographs of children).".

Indecent photographs of children: sentence of imprisonment

86.—(1) In section 160(3) of the Criminal Justice Act l988 (which makes a person convicted of certain offences relating to indecent photographs of children liable to a fine not exceeding level 5 on the standard scale) there shall be inserted after the word "to" the words "imprisonment for a term not exceeding six months or" and at the end the words ", or both". (2) In Article 15(3) of the Criminal Justice (Evidence, etc.) (Northern Ireland Order 1988 (which makes a person convicted in Northern Ireland of certain offences relating to indecent photographs of children liable to a fine not exceeding level 5 on the standard scale) there shall be inserted after the word "to" the words "imprisonment for a term not exceeding 6 months or" and at the end the words ", or both".

[Material omitted]

Obtaining computer-held information

Procuring disclosure of, and selling, computer-held personal information

161.—(1) In section 5 of the Data Protection Act 1984 (prohibitions in relation to personal data, including disclosure), after subsection (5), there shall be inserted the following subsections—

(6) A person who procures the disclosure to him of personal data the disclosure of which to him is in contravention of subsection (2) or (3) above, knowing or having reason to believe that the disclosure constitutes such a contravention, shall be guilty of an offence.

(7) A person who sells personal data shall be guilty of an offence if (in contravention of subsection (6) above) he has procured the disclosure of the data to him.

(8) A person who offers to sell personal data shall be guilty of an offence if (in contravention of subsection (6) above) he has procured or subsequently procures the disclosure of the data to him.

(9) For the purposes of subsection (8) above, an advertisement indicating that personal data are or may be for sale is an offer to sell the data.

(10) For the purposes of subsections (7) and (8) above selling, or offering to sell, in relation to personal data, includes selling, or offering to sell, information extracted from the data.

(11) In determining, for the purposes of subsection (6), (7) or (8) above, whether a disclosure is in contravention of subsection (2) or (3) above, section 34(6)(d) below shall be disregarded. .

(2) In consequence of the amendment made by subsection (1) above—

(a) in subsection (5) of that section, after the word other there shall be inserted the word “foregoing”; and :

(b) in section 28 (exemptions: crime and taxation), in subsection (3)—

(i) after the words “section 26(3)(a) above” there shall be inserted the words “or for an offence under section 5(6) above”; and

(ii) after the words “to make” there shall be inserted the words “or (in the case of section 5(6)) to procure”.

Access to computer material by constables and other enforcement officers

162.—(1) In section 10 of the Computer Misuse Act 1990 (offence of unauthorised access not to apply to exercise of law enforcement powers), after paragraph (b), there shall be inserted the following words—

“and nothing designed to indicate a withholding of consent to access to any program or data from persons as enforcement officers shall have effect to make access unauthorised for the purposes of the said section 1(1).

In this section "enforcement officer" means a constable or other person charged with the duty of investigating offences; and withholding consent from a person "as" an enforcement officer of any description includes the operation, by the person entitled to control access, of rules whereby enforcement officers of that description are, as such, disqualified from membership of a class of persons who are authorised to have access.".

(2) In section 17(5) of that Act (when access is unauthorised), after paragraph (b), there shall be inserted the following words—

"but this subsection is subject to section 10.".

Duration of Copyright and Rights in Performances Regulations (SI 1995 No 3297)

Part III Savings and Transitional Provisions: Copyright

s23 - Revived copyright: saving for acts of exploitation when work in public domain,

(1) No act done before commencement shall be regarded as infringing revived copyright in a work.
(2) It is not an infringement of revived copyright in a work—
(a) to do anything after commencement in pursuance of arrangements made before 1st January 1995 at a time when copyright did not subsist in the work, or
(b) to issue to the public after commencement copies of the work made before 1st July 1995 at a time when copyright did not subsist in the work.
(3) It is not an infringement of revived copyright in a work to do anything after commencement in relation to a literary, dramatic, musical or artistic work or a film made before commencement, or made in pursuance of arrangements made before commencement, which contains a copy of that work or is an adaptation of that work if--
(a) the copy or adaptation was made before 1st July 1995 at a time when copyright did not subsist in the work in which revived copyright subsists, or
(b) the copy or adaptation was made in pursuance of arrangements made before 1st July 1995 at a time when copyright did not subsist in the work in which revived copyright subsists.
(4) It is not an infringement of revived copyright in a work to do after commencement anything which is a restricted act in relation to the work if the act is done at a time when, or is done in pursuance of arrangements made at a time when, the name and address of a person entitled to authorise the act cannot by reasonable inquiry be ascertained.
(5) In this Regulation "arrangements" means arrangements for the exploitation of the work in question.
(6) It is not an infringement of any moral right to do anything which by virtue of this Regulation is not an infringement of copyright.

s 24 - Revived copyright: use as of right subject to reasonable royalty

(1) In the case of a work in which revived copyright subsists any acts restricted by the copyright shall be treated as licensed by the copyright owner, subject only to the payment of such reasonable royalty or other remuneration as may be agreed or determined in default of agreement by the Copyright Tribunal.
(2) A person intending to avail himself of the right conferred by this Regulation must give reasonable notice of his intention to the copyright owner, stating when he intends to begin to do the acts.
(3) If he does not give such notice, his acts shall not be treated as licensed.
(4) If he does give such notice, his acts shall be treated as licensed and a reasonable royalty or other remuneration shall be payable in respect of them despite the fact that its amount is not agreed or determined until later.
(5) This Regulation does not apply if or to the extent that a licence to do the acts could be granted by a licensing body (within the meaning of section 116(2) of the 1988 Act), whether or not under a licensing scheme.
(6) No royalty or other remuneration is payable by virtue of this Regulation in respect of anything for which a royalty or other remuneration is payable under Schedule 6 to the 1988 Act.

s25 - Revived copyright: application to Copyright Tribunal

(1) An application to settle the royalty or other remuneration payable in pursuance of Regulation 24 may be made to the Copyright Tribunal by the copyright owner or the person claiming to be treated as licensed by him.
(2) The Tribunal shall consider the matter and make such order as it may determine to be reasonable in the circumstances.
(3) Either party may subsequently apply to the Tribunal to vary the order, and the Tribunal shall consider the matter and make such order confirming or varying the original order as it may determine to be reasonable in the circumstances.
(4) An application under paragraph (3) shall not, except with the special leave of the Tribunal, be made within twelve months from the date of the original order or of the order on a previous application under that paragraph.
(5) An order under paragraph (3) has effect from the date on which it is made or such later date as may be specified by the Tribunal.

Opinion for the UK Universities and Colleges Information Systems Association on the terms of the Netscape Navigator WWW browser end user licence agreement.

DISCLAIMER: This opinion is offered without the author accepting any liability either for the accuracy or appropriateness of the contents. It is not offered in an expert capacity.

Introduction

I have been asked by Mr P. Dewar, Treasurer of the UK Universities and Colleges Information Systems Association, in a letter dated 16th December 1995, to examine the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT and provide an opinion on the EXPORT CONTROLS section of that license. The letter states the following:

"The product referred to, Netscape, is a software program which can be used to navigate the Internet from computing equipment suitably configured and attached to University computing networks (and therefore onto the international Internet). It is the intention of the United Kingdom Higher Education Institutions to make copies of this software, under the terms of the attached License, available to their institutional students and staff, so the product can be used in pursuance of academic study.

The difficulty we can see is with the EXPORT CONTROLS section of the License and in particular with the practicalities of policing its terms on University campuses, since UK HE Institutions will include in their student (and staff) populations, nationals of the nominated excluded countries.

There are two methods for distributing software products such as this item on an individual campus: by manual or automatic (file transfer) means. Bearing those options in mind, could you advise on the following questions."

There then follow the three questions listed here.

"1) Is there an obligation under this form of License for an Institution to maintain a record of individuals who are distributed copies of the software, and what would be the implications of not doing so ?

2) If an automated distribution method were to be used on a University campus, would it be sufficient to incorporate questions regarding the nationality of the person requesting the distribution copy and barring the copy attempt for the appropriate answer.

3) If a manual distribution method were chosen, would it be sufficient to have the individual requesting the copy sign an appropriate declaration, and if so what would the appropriate wording be ?"

Background.

It is clear both from the research that I have done in this area, anecdotal evidence available on Internet mailing lists, and a brief discussion with Mr David Shickle of Netscape Communications UK that the inclusion of an EXPORT CONTROLS clause in the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT relates primarily, if not exclusively, to the incorporation of RSA encryption software in the NETSCAPE NAVIGATOR software. Encryption software is classed in the US as 'munitions' and is thus subject to US export controls. Such controls include the banning of the passing of encryption technologies to certain blacklisted countries and individuals. The position of the US government as to the level of enforcement of these export controls is unfortunately unclear. This may be demonstrated by the recent decision of US Justice Department not to take any legal action against Philip Zimmermann, the inventor of the encryption software Pretty Good Privacy (PGP) over the release of that software to the wider Internet community.

At issue here is the problem of attempting to enforce export controls over a medium such as the Internet. In virtually all cases, when software is offered to the Internet Community via anonymous FTP, the individual, institution, or business so offering it essentially loses practical control over the future distribution by third parties.

There are possible technical solutions which may help control the initial spread of software by electronic means, including limiting access to the FTP site to users from particular Internet domains. For example, some academic sites limit distribution of software and other electronic material to users within their own institutional domain (i.e. those users within the domain <mit.edu> or <hull.ac.uk>), or to the US or UK academic domain (i.e. those users with <.edu> or <.ac.uk> addresses). However such systems do not constitute a foolproof method of preventing the spread of software outside of those domains, or indeed a method of preventing parties from blacklisted states from obtaining it. Individuals may unilaterally decide to pass on the software or electronic material to friends, relatives, and place it on wider distribution mechanisms such as Internet mailing lists or Usenet groups, irrespective of the terms and conditions of any license agreement Equally, academic institutions often have a wide range of nationalities represented within their staff and student bodies, including individuals from blacklisted countries.

With regard to the specific case of the NETSCAPE NAVIGATOR software, it appears that Netscape Communications, in its free distribution of the software from both its home site in California, and from other sites around the world, does not take any special technical precautions to prevent the export of that software to particular domains. They also do not attempt to prevent the export of that software to particular individuals (probably because this would be impossible to achieve). The only major distinction that appears to be made at their home site is between educational users and all others. At mirror sites even this distinction is blurred. Requests to mirror sites in the US, Sweden, and Austria as to their legal position vis a vis the EXPORT CONTROLS clause in the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT, and any information they may have received on this matter from Netscape Communications have so far elicited only one response, which suggested that the matter was best taken up with Netscape Communications. To this end I have initiated communications with the UK subsidiary of Netscape Communications with a request that they clarify the position with regard to the EXPORT CONTROLS clause. They have proved difficult to contact due to fax problems and thus I await further developments in this area.

With this in mind, and taking into account the fact that Netscape Navigator is widely available from a number of international sites on the WWW with few, if any, checks upon the nationality of the individual downloading it, I would be reluctant to advise the Universities and Colleges Information

Systems Association to undertake potentially expensive, time consuming and otherwise onerous administrative controls on distribution, unless these are absolutely imperative reasons for doing so. The following opinion examines the law relating to this area, and outlines possible solutions regarding compliance with the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT.

Opinion

The questions asked by the UK Universities and Colleges Information Systems Association

Is there an obligation under this form of License for an Institution to maintain a record of individuals who are distributed copies of the software, and what would be the implications of not doing so ?

On the evidence available with regard to the electronic distribution methods adopted by Netscape Communications and its mirror sites, via the Internet, I am of the opinion that no such recording obligation is required by, or can be inferred from, the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT.

If an automated distribution method were to be used on a University campus, would it be sufficient to incorporate questions regarding the nationality of the person requesting the distribution copy and barring the copy attempt for the appropriate answer.

On the evidence available with regard to the electronic distribution methods adopted by Netscape Communications and its mirror sites, via the Internet, it would seem that such an approach would be unnecessary, undesirable, and might well raise issues of discrimination under UK law. The approach taken by Netscape Communications appears to be one of 'self policing':

"BY CLICKING ON THE "ACCEPT" BUTTON, YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, CLICK THE "DO NOT ACCEPT BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE"

As such, I would be of the opinion that a more practical approach would be simply to force the user to download the software via an institutional WWW page on which the terms of the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT are outlined. It would then be up to the user to decide if they could legitimately download the software, as is the case with the approach taken by Netscape Communications and its mirror sites.

If a manual distribution method were chosen, would it be sufficient to have the individual requesting the copy sign an appropriate declaration, and if so what would the appropriate wording be ?"

This seems to be a practical and not particularly onerous device, particularly if the individual were obliged to produce some method of identification (i.e. a library card, student ID card or staff card) at that point. This check would **NOT** be to ascertain nationality, simply to determine whether or not the individual is a legitimate educational user. Again the ultimate responsibility for deciding whether they can agree to all the terms and conditions in the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT should be left to the user.

Supplemental question

What is the position with regard to the EXPORT CONTROLS clause in the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT attached to copies of the software already distributed by members of the UK Universities and Colleges Information Systems Association?

Earlier versions of the NETSCAPE NAVIGATOR software which did not include the embedded encryption technology at issue are obviously not a problem in this regard. Copies of the beta NETSCAPE NAVIGATOR software which did include the embedded encryption technology and were available for distribution appear to have been time-limited, that is they contained instructions in the software which cause it to stop working after a certain date. Where such software has already been distributed, therefore, any potential problems attendant upon the use of such software would seem to end at the point when that time limit is reached.

Suggested Solutions

There are a variety of technical and practical solutions which can be offered as a result of the foregoing discussion. These are as follows:

- All institutions wishing to supply the NETSCAPE NAVIGATOR software to their staff and students, via electronic delivery systems, may apply to Netscape Communications UK for permission to act as mirror sites for the software, subject to whatever terms and conditions Netscape Communications choose to impose. Institutions may wish to restrict FTP access to the NETSCAPE NAVIGATOR software to users at their own institution, or to users within the UK education domain. Users might be required to access a WWW page or download an electronic message outlining the terms of the NETSCAPE NAVIGATOR END USER LICENSE and their implications prior to downloading the software.

- All institutions wishing to supply NETSCAPE NAVIGATOR to their staff and students via floppy disks or other electronic storage media do so on the condition that those to whom the software is supplied sign a form which states that:

> I, {full name}, am a student, faculty member or staff member of {the relevant educational institution} and I agree to be bound by all terms in {the licence agreement} contained in, or attached to, the software package {name of software}.
>
> I understand that in the event that I am unable to be bound by any of the above mentioned terms, that I have no right to install, or otherwise use, the {name of software} software.
>
> I understand that, under the {the licence agreement}, in the event of my leaving {the relevant educational institution} and not remaining a member of an educational institution, my right to install, or use, the {name of software} software under the terms agreed for educational users is terminated.
>
> Signature …….

So for example:

> I, John Smith, am a student, faculty member or staff member of the University of Hull and I agree to be bound by all terms in the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT contained in, or attached to, the software package NETSCAPE NAVIGATOR.
>
> I understand that in the event that I am unable to be bound by any of the above mentioned terms, that I have no right to install, or otherwise use, the NETSCAPE NAVIGATOR software.
>
> I understand that, under the NETSCAPE NAVIGATOR END USER LICENSE AGREEMENT, in the event of my leaving the University of Hull and not remaining a member of an educational institution, my right to install, or use, the NETSCAPE NAVIGATOR software under the terms agreed for educational users, is terminated.
>
> Signature …….

Select Bibliography and Further Reading

General

Boyle, J. *Shamans, Software and Spleens:Law and the Construction of the Information Society* Harvard University Press 1996.
Cavazos, E. A.& Morin G. *Cyberspace and the Law: Your Rights and Duties in the On-line World* MIT Press 1994.
Henry, M. *Publishing and Multimedia Law* Butterworths 1994.
Lloyd, I. *Information Technology Law* Butterworths 1993.
Smith, G. (ed.) *Internet Law and Regulation* FT Law and Tax 1996.

Cairns, R. "Opportunities, Risks and Some Intellectual Property Constraints Surrounding the provision and Use of On-line Services" (1996) 4 *International Journal of Law and Information Technology* 19.
Reed, C. & Walden I. "Legal Problems of Electronic Bulletin Board Operators" " (1994) 2 *International Journal of Law and Information Technology* 287.

Intellectual Property

Annand, R. & Norman, H. *Blackstone's Guide to the Trade Marks Act 1994*, Blackstone Press, 1994.
Bainbridge, D. *Intellectual Property* 3rd ed. Pitman Publishing 1995.
Dworkin, D. & Taylor, R.D. *Blackstone's Guide to the Copyright Designs and Patents Act 1988* Blackstone Press 1989.

Burk, D.L. "Trademarks Along the Infobahn" (1995) 1 Richmond J.L. & Tech.
<http://www.urich.edu/~jolt/v1i1/burk.html>
Burk, D.L. "Transborder Intellectual Property Issues on the Electronic Frontier" (1994) 6 Stan. L. & Pol'y Rev.
<gopher://gopher.gmu.edu/00/academic/colleges-depts-insts-schools/law/working/dburk2>
Kervegant, C. "Are Copyright and Droit d'Auteur Viable in the light of Information Technology (1996) *International Review of Law Computers and Technology* 55.
Samuelson, P. "The Copyright Grab" 4.01 *Wired* January 1996 135.
Samuelson, P. "Intellectual Property Rights and the Global Information Economy" (1996) 39 *Communications of the ACM* 23.

Domain Name Disputes
<http://www.law.georgetown.edu/lc/internic/recent/rec1.html>

Defamation

Carter-Ruck, P. *Libel and Slander* 4th ed 1992.
Norrie, K. *Defamation and related actions in Scots Law* Butterworths 1995.

Arnold-Moore, T. "Legal Pitfalls in Cyberspace: Defamation on Computer Networks" (1994) 5 *Journal of Law and Information Science* 165.
Auburn, F. "Usenet News and the Law" (1995) 1 *Web Journal of Current Legal Issues* <http://www.ncl.ac.uk/~nlawwww/articles1/auburn1.html>
Braithwaite, N. "The Internet and Bulletin Board Defamations" (1995) 145 *New Law Journal* 1216.
Cutrera, T.A. "Computer Networks:Libel and the First Amendment" (1992) 11 *Computer Law Journal* 557.
Dooley, S. "Specific Risks on the Internet: Defamation" (1995) *Computers and Law*, Oct/Nov, 10.

Naughton, E.J. “Is Cyberspace a Public Forum? Computer Bulletin Boards, Free Speech and State Action” (1992) 81 *Georgetown Law Journal* 409.
Pearson, H. “Liability of Bulletin Board Operators” [1995] 2 *CTLR* 54.
Trubow, G.B. “System Operator Liability for Defamatory Statements Appearing on an Electronic Bulletin Board” (1986)19 *J. Marshall L. Rev.* 1107.
Mike Godwin, Libel, Public Figures, and the Net, Internet World, June 1994, at 62.
<http://www.eff.org/pub/Legal/net_public_figures_godwin.article>
Mike Godwin, Internet Libel: Is the Provider Responsible?, Internet World, Nov./Dec. 1993.
<http://www.eff.org/pub/Legal/net_libel_godwin.article>

Criminal Liability

Bailey, S.H., Harris, D.J. & Jones B.L. *Civil Liberties: Cases and Materials* 3rd ed. Butterworths 1991 - Chapter 6, Freedom of Expression: contempt of court.
Smith, J.C. & Hogan B. *Criminal Law* 7th ed. Butterworths 1992 - Chapter 19, Computer Misuse Offences; Chapter 20 Section 3 Obscene Publications; Chapter 21 Offence Against Public Order
Wasik, M. *Crime and the Computer* Oxford 1991.

Charlesworth, A. “Between Flesh and Sand: Rethinking the Computer Misuse Act 1990” (1995) 9 *International Yearbook of Law, Computers and Technology* 31.
Gibbons, T. “Computer Generated Pornography” (1995) 9 *International Yearbook of Law, Computers and Technology* 83.
Gassman, G.L. “Sysop, User and Programmer Liability: The Constitutionality of Computer Generated Child Pornography” (1995) 13 *J. Marshall J. Computer & Info. L.* 481.

Data Protection

Slee, D. “Privacy and the European Union: an examination of the provenance and content of the forthcoming Data Protection Directive and its likely impact on UK data protection law (1995) 4 *Law, Computers and Artificial Intelligence* 277.
Tapper, C., ‘New European Directions in Data Protection’ (1992) 3 *Journal of Law and Information Science* 9.

Financial Transactions

Steven Levy, E-Money (That's What I Want), *Wired* 2.12, Dec. 1994, at 174.
<http://www.mcs.net/~sorkin/wired/emoney.html>
<http://www.hotwired.com/Lib/Wired/2.12/features/emoney.html>

Jim Miller, Digital Cash Mini-FAQ.
<http://draco.centerline.com:8080/~franl/crypto/digicash-minifaq.html>

Jon W. Matonis, Digital Cash & Monetary Freedom, Paper Presented at INET'95, June 27-30, 1995.
<http://inet.nttam.com/HMP/PAPER/136/html/paper.html>

Stephen Crocker et al., CyberCash: Payments Systems for the Internet, Paper Presented at INET'95, June 27-30, 1995.
<http://inet.nttam.com/HMP/PAPER/181/abst.html>

Encryption

Baker, S.A. “Don't Worry, Be Happy: Why Clipper Is Good For You” *Wired* 2.06, June 1994, at 92.
<http://www.mcs.net/~sorkin/wired/baker.html>

Barlow, J.P. “Jackboots on the Infobahn” *Wired* 2.04, Apr. 1994.
<http://www-swiss.ai.mit.edu/6095/articles/clipper/barlow-jackboots.html>

Denning, D.E. “Resolving the Encryption Dilemma: The Case for Clipper” Technology Review, July 1995.
<http://web.mit.edu/afs/athena/org/t/techreview/www/articles/july95/Denning.html>

Froomkin, A.M. “The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution” (1995) 143 *U. Pa. L. Rev.* 709 .
<http://www.law.miami.edu/froomki.html>(temporary site)

Godwin, Mike - A Chip over my Shoulder:The Problems with Clipper, *Internet World* July/August 1994.

Legislation

UK

Data Protection Act 1984 (c. 35) NB: This is the text of the original Act and does not appear to include recent amendments.
<http://www.publications.hmso.gov.uk/hmso/document/Acts/00984035/dataprot.htm>

EC

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ 1996 L77/20.
<http://www2.echo.lu/legal/en/ipr/database/database.html>

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, OJ 1995 L281/31.
<http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html>

Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, OJ 1993 L290/9
<http://www2.echo.lu/legal/en/ipr/termprot/termprot.html>

Council Directive 93/83/EEC of 27 September 1993 on the co-ordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, OJ 1993 L248/15.
<http://www2.echo.lu/legal/en/ipr/cablesat/cablesat.html>

Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property, OJ 1992 L346/61. Articles 11 & 12 were repealed by Directive 93/98.
<http://www2.echo.lu/legal/en/ipr/rentlend/rentlend.html>

Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ 1991 L122/42.
<http://www2.echo.lu/legal/en/ipr/software/software.html>

US

The Communications Decency Act of 1996
<http://www.cpsr.org/cpsr/nii/cyber-rights/web/cda/cda.final.html>

Other

Information Infrastructure Task Force. Working Group on Intellectual Property Rights. *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights.* 1995.
<http://www.uspto.gov/web/ipnii/>

Commission of the European Communities *Copyright and Related Rights in the Information Society* Brussels, 19.07.1995 COM(95) 382 final.
<http://www2.echo.lu/legal/en/ipr/ipr.html>

JANET Acceptable Use Policy
<http://www.ja.net/documents/use.html>

Cases

American Civil Liberties Union et al. v. Janet Reno, Attorney General of the United States. Motions for preliminary injunction - United States District Court for the Eastern District of Pennsylvania.
<http://www.eff.org/Alerts/HTML/960612_aclu_v_reno_decision.html>

Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).
<http://www.jmls.edu/cyber/cases/frena.txt>

Sega Enterprises v. Maphia, 857 F. Supp. 679 (N.D. Cal. 1994).
<http://www.jmls.edu/cyber/cases/sega.txt>

MTV Networks v. Curry, 867 F. Supp. 202 (S.D.N.Y. 1994).
<http://www.jmls.edu/cyber/cases/mtv.txt>

United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994).
<http://www.jmls.edu/cyber/cases/lamacchi.txt>

Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
<http://www.cpsr.org/cpsr/free_speech/cubby_v_compuserve.txt>

Stratton Oakmont, Inc. v. Prodigy Services Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).
<http://www.cpsr.org/cpsr/free_speech/so_v_prodigy_1995.txt>
<http://www.eff.org/pub/Legal/Cases/Stratton_Oakmont_Porush_v_Prodigy/stratton-oakmont_porush_v_prodigy_et-al.decision>

Stern v. Delphi Internet Services Corp., 626 N.Y.S.2d 694 (N.Y. Sup. Ct. 1995).
<http://www.jmls.edu/cyber/cases/stern.txt>

Rindos v. Hardwick, no. 1994 of 1993 (W. Austl. Sup. Ct. Mar. 31, 1994).
<http://www.jmls.edu/cyber/cases/rindos.html>
<http://www.law.auckland.ac.nz/cases/Rindos.html>

United States v. Jake Baker, 890 F. Supp. 1375 (E.D. Mich. 1995).
<http://www.jmls.edu/cyber/cases/baker.html>
<http://ic.net/~sberaha/baker.html>

United States v. Morris, 928 F.2d 504 (2d Cir. 1991).
<http://www.jmls.edu/cyber/cases/morris.txt>

Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994).
<http://www-swiss.ai.mit.edu/6095/assorted-short-pieces/sjg-appeal.txt>

Educational Webpage Policies.

Birmingham University
<http://www.bham.ac.uk/webmaster/conduct.html>

Cranfield University
<http://www.cranfield.ac.uk/docs/publish_code.html>

Computing Services, Southampton University
<http://www.soton.ac.uk/devpages/rules.html>

Edinburgh University
<http://www.ed.ac.uk/about_edinfo/index.html#rules>

Department of Computing Science, University of Glasgow.
< http://students.dcs.gla.ac.uk/conditions/>

Imperial College:
<http://www.anglia.ac.uk/htbin/notes?data_protection+85.2>