Freedom of Expression and the Communication Networks

Strasbourg, June 1998 CC-Cult (98) 18

Council of Europe
Council for Cultural Co-operation -- www.culturelink.org/review/25/cl25ce.html

Document prepared for the Electronic Publishing, Books and Archives Project

Report prepared by:
Mr Paul Sturges

Department of Information and Library Studies
Loughborough University, United Kingdom

Acknowledgements

The author wishes to thank the following for their assistance in various ways, but in each case speaking in their own capacity, not on behalf of their organizations.

> *Barbara Buckley, British Library,* Research and Innovation Centre, and Coalition for Public Information (CoPI).
> *Alan Cooper,* Library Association.
> *Graham Cornish,* IFLA Universal Availability of Publications Office.
> *Michael Day,* UK Office for Library and Information Networking (UKOLN).
> *John Feather,* Loughborough University.
> *John Lindsay,* Kingston University and British Computer Society.
> *Ian Murray,* Loughborough University.
> *Andrew Oldfield,* International Electronic Publishing Research Centre (IEPRC).
> *Frank Parry,* Loughborough University Library.
> *Mark Perkins,* Overseas Development Institute.
> *Alan Poulter,* Loughborough University.
> *Ross Shimmon,* Library Association.

Particular thanks to *Goff Sargent* who provided valuable guidance and support.

Part One:
reedom of Expression
and Public Access Points

1. Introduction

The appearance of electronic networks has transformed the environment for the delivery of information to users in ways that deeply concern the players in the traditional Book Economy. There is a commonly expressed sentiment that information and ideas are more than ever before a free currency which cannot and should not be interfered with. At the same time the widespread ability to gain access to, and use, the technology is a source of anxiety to governments, security agencies, defenders of orthodoxies and fixed concepts of public decency which see networks as a threat to their vision of society. The monitoring of electronic communication and the interference with freedom of expression is much discussed and restrictions are frequently proposed.

The Internet itself includes many Web sites and newsgroups devoted to this debate. Professional and other organisations have produced codes of practice and other documentation on this issue, discussion has appeared in magazine and newsletter articles, and to a lesser extent in books and journals from across the literature of computing, law, politics, information management and librarianship, science and technology, not to mention the popular newspaper and magazine press. Some of these writings can justly be described as contributions to a moral panic. It is therefore important that an organization like the Council of Europe, should form soundly-based views on the subject.

The 5th European Ministerial Conference on Mass Media Policy, held at Thessaloniki, Greece, 11-12 December, 1997, responded to the commitment of the Second Summit of the Council of Europe held at Strasbourg, 10-11 October 1997 to seeking common responses to the development of the new information technologies, by taking as its theme 'The Information Society: a challenge for Europe'. The Conference produced a declaration and two resolutions with many implications for communications and information networks. These documents stress self-regulation by information providers and operators, and public education in the new technologies. This is emphasis is coupled with concern about the misuse of technology by those who promote violence and intolerance and show no respect for human dignity. The idea of 'universal community service' is invoked as a guiding principle for the resolutions, and this idea could also be taken as an implicit principle behind the content of the present report.

The report is written from the perspective that every citizen needs to have free access to information and the ability to express opinion as freely as possible, so that society itself can react dynamically to change and continue to mature. It is also the writer's opinion that this applies almost as strongly to children as it does to adults. They need to be able to find answers to the questions that trouble them, and must at some stage in their development be allowed to judge for themselves what knowledge they need. That some people should wish to avoid unnecessary exposure to certain forms of expression on their own behalf, and on that of their children, is, however, natural. This is not a justification for the general suppression of any category of expression. It is a reason why it should be accepted as a legitimate exercise of choice for individuals, families and organizations like schools, youth groups, and even libraries, which take on some of the role of families, to seek methods to limit their own exposure to certain forms of expression.

1.1 Aims and objectives

The purpose of this report is:

> To examine the present state of and prospects for freedom of expression in communications networks, so as to identify the key issues which affect current practice and which form the content of debate.
>
> To draw attention to experiences, practical initiatives and proposals which have affected or may come to affect the ability of users of networks to

exercise their freedom of expression.

To reflect experience and opinion, as far as possible, globally and cross-sectorally (including publishing, multimedia and communications industries, the library and information world, and other relevant professional and intellectual domains).

1.2 Definitions

There may not be complete mutual understanding of terminology between those who work with information through media like the Internet and those whose main concerns are ethical and human rights issues. Therefore a slightly more detailed description of what is meant by 'networks' (the Internet in particular) for the purposes of this report, and an indication of the sense in which terms like 'freedom of expression' and 'censorship' are used, is provided here.

1.2.1 Networks

Networks link computers, within a single site (local area network, or LAN) or via telecommunications systems to link geographically dispersed sites (wide area network, or WAN). Such networks may provide users with access to shared facilities (files, software, databases, printers, fax machines), but may also provide access to communications (email and conferencing). Networks can be linked through gateways to other networks. Where this uses the common protocol and addressing system tcp/ip, an internet is created. The global, public access network, known as The Internet, is the sum of all such networks that are in communication with one another. The significant thing about the Internet as a carrier of information, is that it has no centre and no controlling authority. It grows in an organic way as more networks are added. The early Internet had a primarily military function in the USA, and its distributed structure, both in terms of communication routes and information input, make it resistant to military attack or control. This robustness, combined with the international character of the Internet, also makes it difficult for civilian authorities to control.

Matters concerning the Internet protocols and other network-wide issues, such as domain names and the IP addresses of networked computers, are dealt with by the Internet Society. The effectiveness of the whole system of communication is dependent on users accepting the guidance of the Society. The user obtains access to the Internet through some kind of access provider, typically an academic institution or a commercial organization dedicated to this form of service. The user's navigation of the Internet is facilitated by various providers who may offer some form of directory, sites which promote a range of information providers, or the search engines which compile information on sites so that the user can perform a keyword search for relevant content. Internet content is made available by content providers who vary from individual enthusiasts to the largest commercial organizations, many of them looking to the Internet as a source of profit. Whilst most content is in the form of text, there is an increasing quantity of more technically demanding content in forms such as audio, animation, or video-conferencing. Content is either accessed in real time, or downloaded on to the user's computer. Questions of intellectual property, liability for information content, and the means for monitoring and charging for commercial transactions are major issues associated with Internet content. Internet hosts, or servers, provide the computer capacity either for their owners' information, or only, as in the case of Usenet news servers, provide facilities for others.

For most users certain sources of information and communication available via the Internet are more important than others. Newsgroups are highly significant as a means of public communication. Users post messages to one or more of the thousands of groups which deal with specific subject areas, often as contributions to a continuing thread of discussion. This is a comparatively ephemeral mode of communication, as material is generally removed after a time interval. Messages are, however, frequently re-posted, usually without the explicit consent of their originators, to one or more other groups. More permanent information public sources are generally on the World Wide Web. Web sites provide access to files in HTML (Hypertext Markup Language) and are connected by hypertext links. Electronic publishing via the Internet is comparatively easy for anyone with access to a server and the ability to work with HTML. Thus both informal communication and publishing on the Internet are democratically accessible to an unusual degree. This is, in turn, the source of the strength of the official and popular anxieties about the Internet as a means of expression.

The Internet is, however, a means for purposive individual enquiry. Although accidental discovery of information does happen frequently on the Internet, this is not the same thing as the casual exposure to images and ideas that inevitably occurs with mass media. This likelihood of casual exposure is central to a rationale for the control of the content of mass media, but it is not applicable to networked information to anything like the same extent. Rather than concentrating on the dangers arising from some networked information, it would be better to stress the value of the access to information on a very wide range of topics, in detail, with little restriction, which the Internet offers. There are risks associated with false, misleading, inappropriate, or, what may be judged by some as, harmful information which is available on the Internet. These have to be accepted as a reverse side to the benefits of freedom of expression in society generally, and the Internet is no exception to this.

1.2.2 Freedom of Expression and Censorship.

Freedom of expression is effectively defined in Article 10 of the European Convention on Human Rights, in other international conventions, and in the constitutions and legislation of various countries. Most notable is the USA, whose Constitution, in its First Amendment,

prohibits Congress from 'abridging the freedom of speech, or of the press'. The protection of personal privacy, which is provided for by the European Convention in its Article 8, is also highly significant, particularly in the development and articulation of unorthodox and unofficial viewpoints. It is quite clear that the declarations in favour of freedom of expression are intended to protect both popular and unpopular ideas, but certain limitations on the scope of the freedoms offered are almost invariably specified. Thus Article 10 of the European Convention refers to national security, prevention of disorder and crime, protection of health and morals, etc.

Exceptions to the universality of the principle can all be supported by strong arguments, but it needs to be remembered that these are also precisely the arguments brought forward to justify systems of official censorship. In the context of libraries, the American Library Association (ALA Intellectual Freedom Committee, 1986) has referred to censorship as:

> the change in the access status of material, made by a governing authority or its representatives. Such changes include, exclusion, restriction, removal, or age/grade level changes.

Official censorship can be a formal manifestation of the widespread popular fears of freedom of expression which do exist. These fears emerge strongly in the context of particular subjects (child pornography, for example), or particular modes of communication (the Internet, for instance). Prompted by such fears, groups associated with a particular religion, lifestyle, philosophy, economic interest, or political tendency, can seek to persuade legislators, courts of law, or the public at large to suppress a certain form of expression. This report will draw attention to numbers of such organizations, lobbying and pressure groups, and putative censors. It will also discuss the work of organizations supporting freedom of expression.

It should also be remembered that there is a range of non-censorship constraints on the freedom of expression and the freedom of information. Whilst in a mature, democratic society such constraints may not have the overwhelming influence that they exercise in less developed countries, they are still present. Prominent amongst such constraints are intellectual property rights and other mechanisms which arise from the ownership of information, the ownership of the media through which information is disseminated, and the associated costs to the user of access to information. The present easy and comparatively inexpensive access to the Internet, and freedom to use it, may be looked back on as a golden age from the vantage point of a future more commercially-constrained communication environment. This type of issue related to access presents too large and complex a group of topics to be mentioned more than tangentially in this report.

1.3 Methods

The report is based on a sampling of current sources of opinion and news. This was carried out through:

Review of literature (including relevant press coverage) and websites;

Consultations with members of relevant organizations and independent observers, and dialogue via email, telephone and letter with others;

Examination of documentation from interested professional bodies, trade associations, pressure groups;

Assessment of progress of specific proposals (legal or self-regulatory) which are intended to moderate flows of information through networks.

1.4 Expected outcomes

The intention was to produce a report which contained:

An outline of the essential issues arising from freedom of expression in communications networks, illustrated from cases wherever possible;

Discussion and assessment of the initiatives, proposals and threats, particularly those in the form of legislation, and self regulation through filtering systems and rating systems;

Suggestions for further research, experimentation and discussion which could contribute towards the formulation of a Recommendation or 'Charter' for freedom of expression in electronic publishing.

2. Debates on Freedom and Control

2.1 History of the debate

Networks are widely perceived as being largely in the hands of their users, especially since the Internet itself has no central control. In this, networks resemble the printing press, which, because access to it is entirely decentralized, has always been a medium for dissent. Networks are, however, notably different from the broadcast media which, because they rely on a central means of transmission, have usually been successfully subjected to some level or other of regulation. The fact that the majority of the population, even in the industrialized countries, either only knows the Internet by repute, or has a limited personal acquaintance with it, means that fears and panics related to it can develop easily. Many of the journalists and other writers who comment on it, and the law enforcement officers whose responsibilities include matters of communication, also reveal a very limited knowledge and understanding of the Internet. This has made the short history of the Internet a fairly turbulent one.

Fears which have been expressed include:

threats to national and corporate security from the activities of hackers;

use of networks for extreme political causes, both for the public circulation of opinions and for encrypted private communication;

availability of dangerous material, on topics such as drugs, weapons, etc.;

circulation of indecent material, most notably child pornography;

use of networks to infringe against intellectual property rights in text, audio, visual, software and other forms;

personal attacks and abuse directed towards individuals, organizations, social, ethnic and other groups.

Such fears have found expression in some notable public cases, of which one or two examples will give the flavour.

In the late 1980s the US Secret Service was regularly monitoring electronic bulletin boards for communications which related to the activities of hacker groups, believed to intend largescale sabotage of telecommunications networks. (Sterling, 1992) A false bulletin board had also been created in the hope of obtaining incriminating messages about suspected illegal activities. In connection with this, a raid (code-named Sun Devil) against suspected hackers had been organized, during which 28 premises were entered and more than 40 computers and 23,000 disks impounded. A company, Steve Jackson Games, which appeared to have only the most distant connection with the alleged offences, was investigated and a game that they were

developing was claimed by the investigators to be a 'manual for computer crime'. The company and its employees then had to become involved in long and expensive efforts to obtain the return of their property, confiscated on suspicion.

In 1991 a newsgroup was set up under the title alt.religion.scientology for the purpose of discussing this cult or religion. Members objected to this and from December 1994 onwards began to take various hostile actions against the newsgroup. These included claiming that messages posted to the group contained material which was copyright, and eventually trying to close the group down on these same grounds. It also took court action against individuals involved in the criticism of scientology via the newsgroup. Whilst the scientologists have not had marked success in the courts with their complex series of legal actions, these have indeed threatened to inhibit free discussion and criticism. In fact the effect has been more or less the opposite, with discussion and quotation from the documents of scientology multiplying and spreading because of the notoriety of the case. (Wallace and Mangan, 1996)

In July 1993 two Californian citizens, Robert and Carleen Thomas, who supplied pornographic material via their 'Amateur Action Bulletin Board System' were investigated by Tennessee-based post office officials. They were then charged with a number of offences in the latter state, mainly involving the interstate transport of files containing obscene material. The case, and the conviction of the accused raised a number of issues including whether the material was actually obscene, whether it was likely to be seen by unwilling viewers, and whether when made available via a network it was actually 'sent' to those who obtained it. (Wallace and Mangan, 1996)

The general trend of these and other cases was that communication on networks by certain individuals, or small and otherwise insignificant groups, attracted the attention of state agencies, or other powerful bodies. A variety of enforcement measures, based on different legal enactments was then taken, resulting in alleged injustices which aroused the interest of organizations set up to defend free expression. The Steve Jackson Games case drew together a group of issues connected with free speech, allegedly 'dangerous' information and computer crime, and Computer Professionals for Social Responsibility used the US Freedom of Information Act to obtain details of the Secret Service activities. Although the accused in the Thomas case were quite open about making their living from pornography, their case was taken up by bodies including the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU). This was because of the implication of the convictions that Internet communications that were legal when made in one jurisdiction could be found illegal when received in another. In the Church of Scientology case, the EFF intervened to suggest that litigation should be avoided because of the adverse effect on small providers.

Probably the issue which produced the most public polarization of views arose from a study of pornography available on the Internet by Martin Rimm, of the Department of Electrical Engineering Department at Carnegie Mellon University. In 1994 he claimed that he had identified over 900,000 images with sexual content available over the network during a short period. He drew this to the attention of the University administration, which reacted by denying access via the University's computers to areas of the system, including Usenet groups designated alt.sex. This was opposed by the ACLU and other freedom of expression pressure groups, on grounds of principle, and because it also incidentally denied access to much valuable and entirely legal material (for instance discussions of safe sex). There was also disquiet about the effect on other institutions because of Carnegie Mellon's pivotal position in cooperative academic computer activities. (Faucette, 1995) Despite some publicly expressed doubts about Rimm's figures, they and the University's response have entered public debate as benchmarks of a kind. (Hoffman and Novak, 1995)

The press has frequently published inflammatory stories about the alleged dangers of the Internet, often citing cases such as that at Carnegie Mellon. Again a few examples must suffice. *Time* magazine carried a cover story by Philip Elmer-DeWitt based on Rimm's findings, which has been cited as a key document in arousing public anxiety in the USA. (Elmer-DeWitt, 1995) *The Observer* (UK) of 25th August 1996 named people who it called 'pedlars of child abuse' over the Internet. It damned the defence offered by providers that they were avoiding 'unacceptable censorship', saying that,

> What they plead for is not liberty but society's licence to permit unalloyed horror. The argument is inadmissible. The Observer unhesitatingly backs those - from the police to children's groups - calling for control and prohibition. (Pedlars, 1996)

The Daily Mail (UK) 6th Oct 1997 alleged that the Internet undermined nation sovereignty and presented a threat to commerce, morals, peace, law enforcement and social cohesion. The article argued that,

> The entrepreneurs who are making billions out of the Internet will have to spend more of their profits on policing the material that flows through their systems. And if they are reluctant to do that then we will need a cyberspace police force with powers to peek over everyone's shoulder and wipe away the filth. (Jeffreys, 1997).

The volume of comment has been high. There has been some action against alleged offenders by law enforcement bodies, or by those who consider themselves in some way harmed by activities over the Internet. The sentiment that 'something should be done about it' has often been heard.

2.2 The US Communications Decency Act

The Communications Decency Act (CDA) which was introduced in 1995, as part of a series of telecommunications reforms, was an explicit reaction to the anxieties which were being expressed in the press, and by various pressure groups. The measure, sponsored by Senators Exon and Gorton, effectively criminalized obscene material sent through electronic networks and provided for fines of up to $10,000 and imprisonment of up to two years. Specifically, it prohibited knowingly using 'an interactive computer service' either to 'send', or to 'display', any 'patently offensive' material to a person under 18. It was passed on February 1st 1996 and signed into law by President Clinton on February 8th. On the same day a group of organizations led by the American Civil Liberties Union (ACLU), called the Citizens Internet Empowerment Coalition (CIEC), filed a lawsuit challenging its constitutionality. Their detailed case against the

CDA is summarized by Lappin (1996). The outcome of the legal actions was the decision of the Supreme Court known as Reno v ACLU which, on June 26th 1997, ruled the CDA unconstitutional under the provisions of the First Amendment to the US Constitution, arguing that:

> As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of free speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefits of censorship.

Whilst the CDA was under debate, and the subsequent legal actions were in process, the Act focused discussion of the regulation of networks not only in the USA but throughout the world. After its defeat, President Clinton immediately called the White House Internet Decency Summit of July 16th 1997. At this meeting the emphasis was shifted to forms of regulation such as labelling and rating, filtering and blocking systems. There has already been an attempt to reinforce this approach by legislation, when Senator McDade of Pennsylvania introduced a Family Friendly Internet Access Bill, which requires Internet Service Providers to provide content screening software free, or at cost. This post-CDA phase of the debate may seem to represent the triumph of the free expression lobby, but the new emphasis on labelling, filtering, and blocking of sites has been described as more insidious and as dangerous. (ACLU, 1997; Lessig, 1997)

2.3 Key players

The debate involves governments, law enforcement agencies, various libertarian political interests (including advocates of freedom of expression), churches, morality lobbyists, media, telecommunications and computer industry corporations and their representative bodies, librarians and other information professionals. As far as governments are concerned, a desire to deal with the dangers of information on networks is not confined to the USA. On July 30th 1996, the G7 Group of the industrialized nations and Russia agreed the principle of controls on the Internet including action against encryption that governments cannot break.

Other political opinion may divide in unexpected ways. A conference on 'Cyberspace and the American dream' held at Aspen Colorado in August 1995, was promoted by the Progress and Freedom Foundation, a thinktank closely associated with US Speaker Newt Gingrich and the rightwing libertarian tendency in the Republican Party. (Right turn, 1995) Speakers at the conference included members of the Electronic Freedom Foundation (EFF), previously associated with President Clinton's Democratic Party government, but disillusioned by official policy on a range of freedom of expression issues. The analysis and conclusions of those present was overwhelmingly anti-regulatory and anti-Government.

Network regulation is strongly advocated by religious and family-oriented groups which express concern over the material which might be accessed by children. For instance, the reaction of one such, the Family Research Council, to the Reno v ACLU ruling was that:

> The floodgates remain open to purveyors of smut. With no legal liability for

> those who pursue children with graphic images and language on the Internet, we need to act fast and firmly to ensure that our country does not give pornography special rights. (Family Research Council, 1997)

There are also feminist groups which strongly support Internet regulation. Because they feel that a free speech orthodoxy dominates the Internet, they call for strict regulation of a medium they feel can lead to an escalation of violations of women's rights. It is also true that there are feminists who oppose this line on the grounds that creating or endorsing powers to censor one kind of expression 'pornography' also hands the power to censor feminist speech to the same official sources, which they argue are dominated by sexist and anti-feminist opinion. (Carol, 1996)

The anti-censorship lobby is represented by a number of loosely allied pressure groups, some of which are concerned with free expression as one of the human rights which they defend, and others which are specifically concerned with information and communication issues. The ACLU is an example of the former and the EFF of the latter. The ACLU was founded in 1920 to protect and expand American constitutional rights and civil liberties. It has a distinguished record in many important campaigns and court cases. Another example of such an organization with broader concerns which involves itself deeply with Internet freedom is People for the American Way, which was set up in 1980 to monitor and counter the agenda of the Religious Right political movement.

The EFF, which has taken an important role in asserting the case for an unregulated Internet, describes itself as 'a non-profit civil liberties public interest organization working to protect freedom of expression, privacy, and access to online resources and information'. Its line is thoroughly libertarian and its statements often represent the thinking of John Perry Barlow, the author of 'A declaration of the independence of cyberspace', drawn up on 8th Feb, 1996, the date President Clinton signed the CDA into law. (Dority, 1996) EFF has local chapters in various parts of the world, and has launched the Blue Ribbon campaign, which encourages sites favouring freedom of expression to carry the blue ribbon motif. An allied organization, the Global Internet Liberty Campaign (GILC) is more explicitly international and links 38 member organizations, principally in the USA and Europe.

The lawsuit against the CDA drew together a group which consisted both of such bodies, and also interested commercial organizations. The list is instructive:

American Library Association
America Online Inc
American Booksellers Association
American Booksellers Foundation for Free Expression
American Society of Newspaper Editors
Apple Computers Inc
Association of American Publishers
Association of Publishers, Editors and Writers
Citizens Internet Empowerment Coalition
Commercial Internet Exchange Association
CompuServe Inc
Families Against Internet Censorship
Freedom to Read Foundation

HotWired Ventures
Interactive Services Association
Microsoft Corporation
Microsoft Network
Netcom Online Communication Services Inc
Newspaper Association of America
Opnet Inc
Prodigy Services Co
Society of Professional Journalists
Wired Ventures Ltd

Closer links can be seen in some cases. The EFF shares computer space, with Computers and Academic Freedom, which maintains an archive on information access in the academic environment. The Center for Democracy and Technology is concerned with public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies. It shares an address in Washington DC with the Citizens Internet Empowerment Coalition. The CIEC, which was set up in February 1996 specifically to fight the CDA, describes itself as a broad coalition of library and civil liberties groups, online service providers, newspaper, book, magazine, and recording industry associations, and over 56,000 individual members.

3. Controversial Content on Networks

3.1 Sexual content

It is apparent from any analysis of the searches made on the Internet that materials with sexual content are the most commonly sought. 'Sex' itself is the most common search term, and various permutations of 'pornography', 'erotica' , the names of magazines such as *Playboy* and *Penthouse*, and related terms predominate. (Markkula Center, 1997) As early as 1994, three of the most used Usenet groups were sexual in content. (Faucette, 1995) It is indisputable that there are both text and images available via the Internet which are sufficiently specific to satisfy any imaginable vagary of human sexual curiosity. That this is the case should be no surprise at all. One recent estimate of the annual turnover of the American sex industry (including printed, video and other materials) puts it at $8 billion. Some of this turnover represents illegal activities, but much takes place quite legally through shops, bookstalls, cinemas and mail order companies. It should also be noted that although American television largely excludes very explicit sexual content, pornographic material is an increasingly large element of the transmissions of television stations in countries including Germany and France. What happens on the Internet is therefore no different in principle from what takes place in the other media of communication.

Sexual content is, however, the chief issue raised in the campaign to control communication on the Internet. Groups such as the National Campaign to Combat Internet Pornography, or People Against Pornography,(see list of Web sites) concentrate on this issue, which was the focus of the CDA's provisions. Their chief anxiety concerns child pornography, but feminist groups also express strong objection to pornography on the grounds that it is a means to demean and control women. Contributions to the Conference on Policing the Internet in London in February, 1997, by Gerstendorfer, Hughes, Kelly, Butterworth, and Muhonen developed this theme. (Policing the Internet, 1997)

The core of the case for control of offensive material on the Internet is that whilst such material is bad in itself, it is particularly insidious on the Internet because of the way that it enters homes, schools and libraries. It is also alleged that it is possible for users, including children, to meet explicit sexual content inadvertently. It is certainly true that the major search engines will without difficulty retrieve sexual content for the searcher who asks for it. The extent to which the more explicit images, which arouse the most strong objection, can be found and viewed by the incautious or merely curious user is more open to debate. (Faucette, 1995) It may, indeed, seem like a rather convenient argument for those who fear freedom to justify restriction.

3.2 Hate speech

The Internet is undoubtedly used for outpourings of abusive and threatening words, which are often directed at a particular race, religion, or sexual orientation. For example, anti-Jewish sentiments are common and virulent. Materials from the Institute for Historical Review (IHR), a

California based organization devoted to the denial of the Nazi Holocaust which resulted in the deaths of millions of Jews and other minorities, are widely available through various Web sites. There are also Usenet groups which focus on this theme, with one (alt.revisionism) wholly devoted to it. Abusive terminology is habitually used to refer to Jewish people in exchanges in such groups, and versions of the blood libel appear, often in forms familiar from the fictitious document 'The Protocols of the Elders of Zion' which has circulated in print for decades. (Capitanchik and Whine, 1996) Other forms of racism, misogyny, anti-gay, anti-religious and similar abuse can also easily be encountered on the Internet. Whilst this is cause for general concern, it has been more addressed by organizations representing the abused groups than by the campaigners for control of the Internet.

3.3 Heterodox politics

Use of the Internet to voice hate speech is closely related to its use for political discussion and organization by fringe and extremist groups. Neo-Nazi groups communicate via bulletin boards and newsgroups such as the Resistance Bulletin Board Service, and in the USA the Liberty Lobby, a racist umbrella group, sponsors the Logoplex BBS. (Capitanchik and Whine, 1996) The American religious right makes prolific use of the Internet, and the home page of Pat Buchanan (former US presidential candidate) containing his thoughts on family, faith and freedom, can be reached by links provided by Web sites on gun control, white supremacy, abortion and the other key themes of far right politics. (Newey, 1996) The *Euskal Herria Journal*, an online journal supporting Basque independence, has been accused of favouring the terrorist organization ETA. (Watson, 1997) Anarchist groups are enthusiastic users of the Internet, relishing its distributed and uncontrolled structure as a matter of conviction. (Atton, 1996) Examples of controversial political content could be multiplied.

The effectiveness of political use of the Internet has been argued in relation to the disturbances in Serbia, 1996-7. (Bennahum, 1997) Described as 'The Internet Revolution' this campaign of political action and civil disobedience had to contend with strict control of the established communications media by the Milosevic government.

Although there were only an estimated 10,000 possible Internet users in the country, their political significance was disproportionate to their number, most being students. They used the Internet in various ways. Demonstrations were called and coordinated through a service called SezamPro, even though it only had 22 dial-up lines and 3000 users. A radio station, Radio B92, which supported the opposition, was banned, but its broadcasts were re-routed via the Internet, using RealAudio. Overseas reporting of events was much improved by information communicated on the Internet, thus putting pressure on the regime.

3.4 Dangerous topics (Drugs, weapons, etc.)

The Internet carries its share of information on topics relating to dangerous subjects and devices. There is, of course, much content relating to weaponry posted by gun lobby and similar groups in the USA. Shin Bet, the Israeli intelligence agency, is said to believe that encrypted instructions from Hamas, the militant Palestinian group, on terrorist attacks,

> including maps, photographs, directions, codes and even technical details of how to use bombs, are being transferred through the Internet. (Borger, 1997)

There is also publicly available information of an obviously dangerous kind available on the Internet. For instance, a bomb-making manual, *The big book of mischief - the terrorists' handbook*, has been available via the newsgroup rec.pyrotechnics. (Capitanchik and Whine, 1996) A Web site, provided by someone using the alias Candyman, is a collection of information on topics such as drugs, phone phreaking, techniques for killing people with the bare hands, and bombs. His justification for this is couched in freedom of expression terms. He claims that,

> My actions are those of a librarian or archivist of information. The action of authoring, archiving, or publishing information is protected in the United States Constitution under the First Amendment. (Wallace and Mangan, 1996)

Despite such assurances, these examples illustrate why there is anxiety.

3.5 Defamation

The Internet, particularly Usenet groups, is known for the freedom with which opinions of individuals are expressed and the abusive language that is often used. The practice of 'flaming' consists of subjecting individuals who have given offence in some way to uninhibitedly abusive public messages. This can easily contain material which is libellous. Although there have been only a small number of cases of libel actions resulting from statements communicated via the Internet, this certainly fails to measure the volume of libellous content. Anyone sufficiently determined to distribute a 'defamatory' statement across the system can deter prosecution by the sheer ubiquitousness of the material.

For instance, McDonalds' took out a libel action in the UK against two people who had distributed leaflets criticizing the company. Whilst this was in progress, the original statements and much other arguably defamatory material were placed on a Web site called McSpotlight. This was held on servers in Holland, Australia, New Zealand and the

USA, with the potential to distribute it even more widely if the need arose. (Katz, 1997) In another example, a poem by James Kirkup, which had been condemned in the British courts as a 'blasphemous libel' (it was a homosexual meditation on the crucifixion of Christ) was found on a US Web site. The UK Crown Prosecution Service attempted to take action against the Lesbian and Gay Christian Movement on the grounds that their Web site contained a link to the offending American site. The Prosecutor was unable to sustain this action and the case was dropped.

3.6 Official Secrets

Similarly, the ability of the Internet to make official secrets public exceeds that of the media previously available. Once posted, a message tends to be re-posted in other Usenet groups or Web sites. 'Mirror sites' in countries other than that of an original posting are frequently used to evade attempts to suppress a particular item. The potential of this was exploited by Richard Tomlinson, a former member of the British secret service agency MI6, who wished to publish a book telling of his experiences with the agency. When the British Official Secrets Act was invoked to prevent him, he threatened to release the text on the Internet from a secret computer source where it was held in readiness for distribution. (Katz, 1997)

In another case, Nottinghamshire County Council (UK)'s Joint Enquiry Team Report (JET) into the 1988 Broxtowe 'Satanic Ritual Abuse' case was not released for public attention. However, it was unofficially published on the Internet by a group that argued that its content was important public knowledge. Nottinghamshire took legal action for breach of copyright in June 1997, immediately after the report was posted. A total of 35 mirror sites were created around the world, forcing the Council to withdraw the action as hopeless. (UK Jet Report Controversy, 1997)

3.7 Privacy

It must not be forgotten that networks carry a great deal of private communication as email, and in other forms such as computer conferencing. A proportion of the controversy over networked communication concerns freedom of private rather than public expression.

3.7.1 Surveillance

Privacy of communication over networks is protected by the US law, and similar enactments in some other countries. In countries where the rule of law is precarious, such legislation is habitually infringed by law enforcement and intelligence agencies, and in countries where the law is formally respected, permission for 'wire-tapping' can be legally obtained if good cause is shown. The American National Security Agency (NSA) and Britain's GCHQ are alleged to intercept enormous numbers of international messages each year, ostensibly to prevent the use of networks for criminal purposes such as drug-trafficking, paedophilia and terrorism. Thus a senior British police office alleged that,

> Some people are sending porn down the Internet together with the instructions as to how to use encryption to safeguard yourself. You need to know the key to unscramble it. (Elliott, 1995)

3.7.2 Encryption

The quotation above was a reference to public key encryption, a system by which the potential receiver of messages makes public a key with which the messages can be encrypted. The receiver holds a private key which is the only means by which a message encrypted by the public key can be decoded. The use of such a method is a natural response to the real or imagined sense that surveillance is likely to break the secrecy of some message or other. Secure public key encryption for ordinary users is obtainable through the use of a freely available program called Pretty Good Privacy (PGP). It is significant, however, that its creator Phil Zimmermann was arrested and prosecuted by the FBI on the grounds that his program would be available to America's enemies, who might use it for some such purpose as espionage.

To persuade or oblige network users to trade part of the security PGP gives to them, the US government has offered alternative, and even more secure, means of encryption. The US Congress is currently debating a Security and Freedom through Encryption measure, known as SAFE. This would impose controls on the manufacture and use of encryption in the USA. No encryption product could be marketed unless it contained a feature that allowed immediate decryption of a user's messages, without the user's knowledge. (New FBI Draft, 1997) The British government (before the change of control in May 1997) issued a Consultation Paper on 'Licensing of Trusted Third Parties for the Provision of Encryption Services' which followed a broadly similar line. (First Report, 1997)

4. Law and Networks

Legislation is the first of three main types of response to the problems presented by controversial content of the kinds outlined in Section 3. The others are filtering and labelling systems (Section 5), and ethical approaches (Section 6). The failure of the US CDA has re-directed attention to the other approaches. This does not mean that the law is irrelevant, or that people do not still look for solutions through the making of new laws.

4.1 Relevance of existing law

John Perry Barlow's claim that cyberspace is independent and that existing governments have no right to rule there, expresses a common sentiment, even a fear. As he put it,

> We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based upon matter. There is no matter here. (Dority, 1996)

This is, however, simply a romantic vision of cyberspace. The British lawyer Graham Smith suggests a harder reality:

> The suggestion that the Internet has no law is born of wishful thinking more than of cogitation. Local laws of each jurisdiction do apply to activities

> conducted using the Internet. While enforcing such laws presents new challenges, the pan-political nature of the Internet may in fact render it vulnerable rather than immune to the laws of jurisdictions around the world. (Smith, 1996)

It is true that in many cases the appropriate jurisdiction, or jurisdictions, may be extremely difficult to identify. In an attempt to deal with such difficulties, the British Computer Misuse Act of 1990 explicitly claims jurisdiction over an alleged offence whether it was the accused, the computer, or the offence itself that was in Britain at the relevant time. None of the relevant laws which might be used in the many jurisdictions where the Internet is used have actually been called upon very often. Therefore there is only a comparatively small body of case law arising from court actions related to communication on the Internet. (Diamond and Bates, 1995) Major texts on the applicability of existing law to cyberspace are in print, and no doubt others are being written. (Cavazos and Morin, 1994; Smith, 1996) Furthermore, despite the failure of the CDA there is fresh legislative and regulatory activity.

4.2 Proposed Legislation and Regulatory Systems

4.2.1 US States

The level of legislative activity in US States relating to networks is at such a high level that a complete survey is inappropriate here. A few examples will illustrate the nature of this activity in state legislatures:

> Alabama had a Bill to prohibit electronic transmission of obscene material to minors;
>
> Connecticut passed a Bill criminalizing various aspects of Internet communication, including the kind of abusive language used in flaming:
>
> Florida had amendments to existing statutes on pornography which could potentially make online transmitters of sexual content liable to pay compensation to victims of sex crimes shown to have involved use of their materials;
>
> Maryland had a Bill which in re-asserting the criminality of distributing obscene material online to minors made system operators liable for the actions of their users;
>
> New Jersey passed a Bill on child pornography which even applied to images in which did not actually use real children.

Other states have also had measures which shared features with the examples listed here. So far, it seems not to have been possible to enforce the measures which have been passed by the state legislatures. Certainly some of them are subject to challenges in the courts on the same grounds that were used against the CDA.

4.2.2 European Union

The Union has succeeded in keeping the essential issues in mind despite the intensity of feeling which has influenced legislative action elsewhere. Concern was voiced in the

European Parliament in April 1997, with a call for European and international action to drive pornography, paedophilia, and racist material off the Internet. However, the Union has so far avoided issuing Directives, which would have the force of law in the member states, on this issue. The debate in April called for a common legal understanding across the Union's member states as to exactly what constitutes illegal content, so that it can be made the subject of prosecution wherever the provider is based.

In a major policy document, the 'Communication on Harmful and Illegal Material on the Internet' issued in February 1996 the European Commission had already set out views on this. (European Commission, 1996) The Communication summarised the complexity of the legal situation in Europe and of the problems to be addressed. It made a clear statement of the

importance attached to the economic role of Internet service providers and re-asserted that the responsibility for content lies with authors and content providers. Action against service providers was seen as jeopardizing the ability of users to obtain access to other, legally protected, content. The Communication suggests that:

> The law may need to be changed or clarified to assist access providers and host service providers, whose primary business is to provide a service to customers.

This line of thinking was developed further in July 1997 at a European Ministerial Conference in Germany. The Conference issued the 'Bonn Declaration' which contained a clear statement on legal controls applying to the Internet. It emphasized the importance of clear definition of the various Internet players' differing legal responsibilities for content. In particular it was recognized that there is a need for a clear distinction between the responsibility of those who produce and circulate content, and the Internet Service Providers who act as intermediaries. Since then, the European Parliament, at its session on Oct 24th, has recommended testing of filtering and screening devices, and called for a programme to inform parents on how to protect children from harmful content.

Since then, various aspects of this developing European Policy have been drawn together in a very comprehensive 'Action Plan on promoting safe use of the Internet'. (European Commission, 1997) This outlines the issues and the state of policy development within the Union, then sets out a plan with four action lines. These are:

1. Creating a safe environment (by encouraging self-regulation of the industry);
2. Developing filtering and rating systems (particularly as regards their usability in Europe);
3. Encouraging awareness actions (to promote safe Internet use to families, schools, etc.);
4. Support measures (including monitoring and assessing the developing legal situation).

The Action Plan was issued on November 26th 1997, and has to be considered by the European Parliament and the Council of Ministers, before it can be adopted.

It is significant that the Thessaloniki Ministerial Conference of the Council of Europe (see

Section 1) in December 1997 passed Resolutions and approved an Action Plan broadly complementary to The EU Action Plan. Whilst the thrust of the EU Action Plan was 'safe use of the Internet', that of the Council of Europe was directed towards 'freedom of expression and information'. The EU Action Plan shows a strong concern for commercial issues, particularly seeking to protect service providers. This leads to an emphasis on community safety, and a strong emphasis on the testing of filtering devices. The Thessaloniki Action Plan concentrates on promoting freedom of expression, whilst studying misuse of networks and exploring possible action against misuse. Both Plans are strongly directed towards self-regulation, the developing of public awareness, and support measures through work on legislation. Although the two plans approach matters such as filtering and new legislation from rather different directions, they both call for work on the same areas, and suggest nothing that could not reconciled with the other's approach.

4.2.3 Individual European countries

European governments have approached the issue both through taking legal action, and by encouraging self-regulation. The German government felt itself obliged by its laws against the spreading of race hate, and against aspects of pornography, to take action against certain Usenet groups. In December 1995, at the behest of the Bavarian prosecutor's office, it ordered CompuServe to prevent access to various sources of illegal pornographic and race hate material. To comply, CompuServe had to temporarily suspend the relevant newsgoups worldwide. All of the groups, except a few whose content was very specifically identified as illegal, were subsequently reinstated. CompuServe began, at this time, to offer the use of CyberPatrol filtering software so that parents and schools could control access to content generally. The German government also tried to bar access to race hate material on Web sites from Canada, but backed down when alternative access was offered by a number of mirror sites in the USA. In response to these and other similar instances, the German Federal Government has drafted a 'Law to Regulate the Conditions for Information and Communication Services'. This asserts the liability of information service providers for material passing through their services. (Kuner, 1996)

The Netherlands and Britain, in contrast, have favoured self-regulation (sometimes in a form better described as self-policing). In the Netherlands it has been felt necessary to try to limit the spreading of paedophile material, and the authorities have sought to do this within the provisions of existing legislation. In January 1996, NILP, an association of Dutch service providers was encouraged to set up a foundation to monitor offending material. The foundation seeks to persuade offending providers to remove illegal material, reporting the offence to the police if it continues. (Vitiello, 1997)This balance between continuing respect for free expression and the upholding of the law is more or less paralleled in Britain. The Internet Watch Foundation (originally Safety Net Foundation) was set up in September 1996 by the two leading associations of service providers ISPA and LINX. (See list of Web sites for URL)IWF pursues the three goals of rating, reporting and responsibility. The reporting element means encouraging the public to report offensive sites to them, so that they can request police action if necessary. The number of British-based sites reported has been small and there have been no prosecutions in the courts. As another element of its programme the foundation continues to press the case for ratings systems. (Watson, 1997)

4.2.4 Asian countries

Asia provides examples of the whole spectrum of policies towards the Internet. Thailand, at one extreme, makes little restriction and has the highest levels of use in South East Asia. Burma, at the other extreme, completely outlaws Internet access. Restrictive policies are more common in Asia than liberal approaches. In November 1997 Vietnam granted licences to four organizations to sell Internet services from a single state-controlled provider. Before this stage was reached, the party politburo had hesitated because it feared both the introduction of information about 'unhealthy cultures and lifestyles' into Vietnam, and the theft of national secrets. Traffic on the Internet is to be monitored and filtered by government agencies and the exchange of encrypted information is outlawed. (Jellinek, 1997) Singapore has adopted an approach designed to reconcile its aim to make the country the most wired in the world with its authoritarian attitude towards dissent. Since 1996, service providers must be registered, users are legally responsible for the material they receive and send, and much content is blocked on political, moral, and religious grounds. The development of the Internet in Singapore is a kind of laboratory experiment in controlling information whilst trying to obtain the benefits of the widest access to information resources. (Ang and Nadarajan, 1996)

In China, since 1996, all Internet users have had to register with the police in a complex and (by Chinese standards) expensive way. Additionally, the single service provider, China Internet, blocks political material, and there is a high level of surveillance of Internet activity accompanied by intervention when activity is deemed inappropriate. The number of people with computers, the money to afford access, and the command of English required to make effective of the Internet is small at present, so close control of their usage is comparatively feasible. This pattern of restricting access to Internet content is referred to as the 'firewall'. The longterm aim of policy seems to be to combine these restrictions with a Chinese alternative to the WWW, the China Wide Web, which will be a commercial network, but also subject to control. (Usdin, 1997; Barme and Ye, 1997))

4.3 Role of law enforcement agencies

Some of the examples of policy discussed above involve roles for the police and other law enforcement agencies in administering Internet access on a day to day basis. In other cases the police might only be involved when there is some specific complaint which is to be brought to the courts. However, between these two distinct approaches there can still be police involvement. The Clubs and Vice Unit of London's Metropolitan Police has been pro-active in encouraging Internet service providers to prevent the circulation of obscene material, particularly that with paedophiliac content. In August 1996, the Unit called a meeting for ISPs at New Scotland Yard. In the words of Superintendent Martin Jauch they were told that 'We thought they were breaking the law and it was time for the industry to address that problem.' (Policing the Internet, 1997 p.30) This approach places the ISPs under threat and seems intended to encourage them to take on the role of censor, when neither does the state itself take censorship powers, nor have the courts made rulings on whether material is illegal or not. Reportedly, a number of newsgroups were removed by ISPs as a result of this pressure, even though most of their content would be legal in Britain. (Rodrigues, 1997)

This form of policing purports to be encouraging self-regulation, but it actually deputes a censorship role to commercial organizations. Even if this were, in principle, a reasonable thing to ask, the ISPs have neither the will nor the legal expertise to perform the role effectively. A somewhat different approach now seems to have replaced this form of indirect police intervention. This is the setting up of the Internet Watch Foundation, referred to in 4.2.3 above. Although this is constituted as a self-regulatory body, controlled by a management board drawn from the Internet industry, educational, consumer media and libertarian groups, it is still described by some as a permanent threat and inducement to censorship at the ISP level. What is more, police intervention still seems to continue. The Campaign for Internet Freedom UK, had its site shut down by the providers Easynet in September 1997, ostensibly at the behest of the 'Anti-terrorist branch' of the police. (Watson, 1997) The site is now viewable via an American provider (See list of URLs), but it is important to remember that it was closed not by direct government censorship, or by formal agreement within an industry self-regulatory body, but as the result of pressure placed on a service provider.

5. Filtering and Labelling

5.1 The Metadata Dimension

Filtering and labelling are discussed here essentially in the context of excluding access to material. However, they can also be regarded as part of the major movement to attach metadata to information on the Internet so as to enhance access. (Dempsey and Heery, forthcoming 1998) The World Wide Web Consortium (W3C), which is the main standards forum for the Web, has been working on an architecture to accommodate metadata. This Resource Description Framework (RDF) is intended to provide for the very wide range of different metadata needs experienced by those creating and using material on the Web. What is required of the RDF is that it should support a variety of resource description models devised to satisfy all these distinct needs. RDF will use XML, the markup language which is being developed as a successor to SGML, as what is described as its transfer syntax. This will make it possible to take advantage of the various tools which are being developed around XML. PICS, which will be discussed later in this chapter, is one example of a metadata activity taking place in this context. Another important illustration of these resource description models are those being worked on under the name of the Dublin Core.

The Dublin Core is a metadata set with 15 elements, which is intended to enable searchers to discover electronic resources on the Web. It is intended to be: simple (much simpler than library systems such as AACR2) so that it can be used by non-cataloguers; interoperable between different disciplines which have their own differing standards for resource description; internationally acceptable; flexible, to the extent that it can be used in associated with more elaborately structured forms of description if required; and, finally, capable of coexisting with other metadata packages (which might relate to such matters as the privacy status of the resource, or terms and conditions for use of intellectual property). These characteristics are typical of what might be looked for in an effective metadata package and most of them could just as reasonably be looked for in a package, like PICS, designed to identify material which a user did not want to see, or did not want others to see.

Metadata can be applied to resources in various ways. The most obvious way is to embed it in HTML documents themselves, using the <META> tag which is provided. The HTML 4.0 specification released in July 1997 permits a richer form of description than previously under the <META> tag. The data provided in this way is an integral part of the resource and is picked up by the agents which index a Web resource, along with all the resource's other elements. Alternatively an organization which collects and manages metadata records which are not embedded in the resources themselves (in just the way that libraries catalogue their holdings) can label resources for additional purposes. Such purposes could include rating of content according to suitability for different user groups. Finally, it is possible to envisage the management of metadata records by a single agency which would ensure that various descriptive models were interoperable to the extent that users could identify precisely the form and content of resource they required using a single query model.

5.2 Content filtering and recommendation systems

Having set labelling in a metadata context, it is necessary to look at the filtering process which is made possible by the availability of suitable metadata. This is also a much broader activity than the mere filtering out of distasteful content (although this is the usual sense in which the term is used in the context of discussions of freedom of expression). The bewildering wealth of resources on the Internet, and the difficulty of assessing their relevance and quality, has led to explorations of filtering systems, using software developed for the purpose. Such software can use various means to identify resources on behalf of the user who installs it or takes advantage of services which provide assistance with the filtering of information. Early developments of this kind were often referred to as collaborative filtering systems. It is now more common to refer to recommender systems, as the term 'filtering' does have some connotation of exclusion, and not all such systems are truly 'collaborative'. (Recommender Systems, 1997)

5.2.1 Filtering for recommendations

Recommender systems are, in spirit, the same as the published consumer reports which test and assess products and services such as restaurants and hotels. They pass on the assessment made by one or more individuals, expert or non-expert, for the benefit of others. Symbolic awards of stars or rosettes are often used to sum up the results of this process. The recommendations, whatever the form in which they are expressed, are a type of metadata.

Electronic recommender systems usually work by aggregating inputs from interested people and directed the aggregated information to those who seek guidance. Their distinctive contribution may lie in the aggregation itself, or in their ability to make good matches between recommenders and those needing advice. Recommendations may be entered into the system explicitly, but some systems gather the evaluations implicit in recommenders's use of resources (in the form of references to URLs in Usenet postings, personal bookmark lists, or the amount of time users spend with a resource). The recommendations may be anonymous, pseudonymous, or tagged with the recommender's identity. The aggregation may take into account a system of voting weighted according to some scheme such as past agreement between recommenders, or personalized weighting. In some systems evaluations and content analysis may be combined to produce a recommendation.

The recommendations can then be used in various ways, such as to filter out resources that are not recommended; to sort and present lists of resources according to numeric evaluations; or to present evaluations in a display with the items to which they refer. This may seem to apply best to the recommendation of Websites, but it is claimed that even Usenet news articles, which are very numerous and have short lifespans, have been effectively rated and recommended. A number of existing products and services provide recommendations using a mixture of the methods referred to above. They include GroupLens, Fab, ReferralWeb, PHOAKS, and Siteseer, all of which are described and analyzed in some detail in an issue of *Communications of the ACM*. (Recommender Systems, 1997)

5.2.2 Filtering to exclude content

Having demonstrated that filtering is merely one application of metadata, and only one aspect of the filtering and recommendation function, it is, nevertheless, a central feature of the discussion of how to deal with offensive content on networks. Even before the US Supreme Court rejected the CDA in June 1997 filtering was discussed as an important alternative to government intervention by legislative action. It is now central to the debate. This approach has been described as 'the privatizing of censorship', (Lasica, 1997) and there are two main routes by which it can be achieved.

> First, there is the application of blocking software at the level of individual users. Various products such as, Cyber Patrol, Cyber Sitter, Net Nanny, Net Shepherd, Smart Filter, Surfwatch, and Websense, are available on the market. When using this type of product, users are mainly dependent on the methods and standards chosen by the software supplier. Whilst these could be based on a ratings system of some kind, at present they tend to be based on the exclusion of specified keywords, sites, and types of graphic image. Users do have some scope to tune the software to meet their own particular preferences, but this is not usually described as particularly easy or convenient.
>
> Second, there is reliance on ratings attached to content either by content and service providers themselves, or by some external agency. This agency might itself create the rating scale which it uses, or use a standard offered by a ratings bureau, such as the (US) Recreational Software Advisory Council's RSACi, or the system offered by SafeSurf. The users can set their preferences in relation to the scale offered by their chosen rating system.

The means used to make this possible is the Platform for Internet Content Selection (PICS). PICS is an HTML standard which makes it possible to filter material on the Internet. (Resnick, 1997) It establishes a consistent way to express content ratings, which can then be attached to specific resources according any one of the systems which might be available. The user can then filter out any content which is revealed not to meet self-set criteria of acceptability. PICS is not itself directed against any category of material: it provides the means by which content rating schemes from the whole range of possible sources can be operated. The intention is that individuals, families, organizations, ISPs, or even nations, will be able to select the content rating systems they prefer, and use PICS to put them into operation. (Resnick, 1997) This is also the position of the European Commission, which discussed content rating systems, in 1996 and endorsed the value of a multiplicity of such systems in allowing users to select the one which reflects their values. (European Commission, 1996)

The creators of browsers and search engines, including Netscape and Microsoft declared their agreement to provide PICS capabilities in their systems at the Fifth International

WWW Conference in Paris in 1996. Also CompuServe expressed the intention to use PICS to put ratings on its content as it moves on to the Web, and to provide CyberPatrol software for its members's use. The swift acceptance of PICS by the industry as a whole has led to explorations of the extension of its use to cover code signing, privacy and intellectual property rights management. PICS's own Web pages (see list of URLs) provide the basic details, connect the reader to other related information and deal with a number of key FAQs.

The filtering software which makes use of the ratings which PICS presents, so as to block access to certain resources, is a crucial element in this whole system. A number of products are named above. One of the first and best publicized is SurfWatch. It has its own Web page, which proclaims that 'it is a real alternative to Internet censorship, giving parents and educators the opportunity to limit unwanted material locally without restricting the access rights of other Internet users'. (Internet Censorship, 1997)

There are two main objections to filtering software. First, the exact methods by which products identify material to be blocked may not be fully transparent. Second, products are often alleged to block valuable material implicated only by the crudity of these methods. For instance, Web sites for English pubs were blocked because of references to alcohol; a real estate site was blocked because it used the same Internet access provider as a pornography site; part of the US White House site was blocked because it referred to the Clintons and Gores as 'couples'. (Robot as Censor, 1997)

What is clear is that large numbers of sites are blocked by many of the products. A list of the number of sites that were alleged to be blocked has been posted on a Web site (although it is possible that this information may not be reliable). The list suggested that, on various different count dates, CyberPatrol blocked 13,000 sites; SurfWatch 4,500; the Internet Filter 107; NetNanny 801; and CyberSitter 820. (Censorware Search Engine, 1997) An organization which supports filtering, Filtering Facts, has tested and (so far) recommends four products, Bess, CyberPatrol, SurfWatch, and Websense, as meeting its criteria, which are:

1. Stoplist must be reasonably accurate and effective at stopping pornography;
2. Stoplist must be customizable so as to block only pornographic content;
3. It must be possible to add and delete sites from the stoplist;
4. It must be possible to override the filter;
5. It must be possible for keyword blocking to be turned off;
6. It must be able to unblock incorrectly blocked sites quickly;
7. The vendor must be able to demonstrate that it makes only accurate claims about the product and conducts public relations in a responsible manner.

5.3 Rating and Labelling Systems

Ratings or labels can be applied to resources either by some bureau designated for that purpose (a third party), or they can be applied voluntarily by the creators or the distributors of the resources.

5.3.1 Third Party Rating

PICS's creators in W3C envisage that there will be a multiplicity of ratings services, covering shades of opinion from across the whole spectrum of human preference. Out of these, people can choose one which reflects their own values. Certainly it seems possible that all kinds of bodies with a religious, moral, political or ideological viewpoint will be interested in devising a scale or matrix for ratings. This is, however, a different issue from actually examining resources and deciding on a rating for each example. The likelihood that any but a major, industry- or government-funded agency could do more than apply ratings to a proportion of the most permanent and high-profile sites seems low. (Marshall, 1997) The expenditure of time and money required to rate tens of thousands of Web sites, let alone Usenet contributions, would not be available to small organizations. Existing systems which rate audio-visual products deal with much more manageable numbers, such as feature films for cinema distribution, videos for public sale or rental, and computer games and simulations.

The use of third party rating is long established in the audio-visual industries. For instance, the British Board of Film Certification (BBFC), previously known as the British Board of Film Censors, has applied ratings to films which are to be shown to the public in cinemas for decades. The system has no legal force, but the local authorities which are responsible for the licensing of cinemas use it as their standard, only occasionally making specific decisions to permit the showing of an unrated film, or not allow the showing of a rated film. It is notionally enforced by the cinemas themselves. Films are viewed by the Board and awarded a distribution certificate essentially suggesting the age at which it is felt that they would be appropriate for young viewers. The certificate for a film indicates a suggested age, such 12 or 15, as appropriate for viewers, or designates it PG (Parental Guidance). In practice cinemas seem to regard the certification as being addressed more to parents than to themselves.

One major rating system intended specifically for Internet use has been devised by the Recreational Software Advisory Council, a body which originally concerned with computer and video games. The system is called RSACi (with the 'i' standing for Internet) It rates resources on a scale of 0-4 on four content categories: violence, nudity, sex, and language. Thus a product with a rating with the structure 4 3 2 1 would be expected to contain: wanton and gratuitous violence; non-sexual frontal nudity; clothed sexual touching; and mild expletives. Alternatively the structure 0 1 2 3 would suggest: harmless conflict with some damage to objects; revealing attire, clothed sexual touching; and strong, vulgar language, obscene gestures, and racial epithets.

5.3.2 Voluntary self-rating

If, as suggested earlier, extending rating by a third party right across the vast, and growing, number of Internet resources proves to be impossible, a system of self-rating offers a more practical possibility. In such a system, a site voluntarily compares itself with a set of criteria of the kind described above, and then indicates this rating on the site. Filtering software in the home could be adjusted to accept only sites which bore a rating, and amongst them only sites with certain levels of rating. The scale of activity this would demand is enormous. By October 1997 45,000 sites out of the millions available, had rated themselves according to some criteria such as those provided by RSACi. (Arthur, 1997) The implications of self-rating for free speech are also enormous. The holders of controversial opinions are either likely to be excluded from communicating with many people if they rate themselves honestly according to the crude and imprecise categories offered by ratings schemes, or discouraged from full and free expression by the need to show a bland rating for their material. (ACLU, 1997)

Legislation to make rating mandatory has been discussed in the USA, and it seems a natural consequence of such a system. Certainly, without a penalty system to back it up, self-rating is likely to be subverted by some providers who would rate their sites in a deliberately deceptive manner. Within the Internet community there is no agreement on how to administer a self-rating system so as to avoid compulsion. There is also no clear idea for a means to ensure that all creators of sites, wherever they came from in the world, could be drawn into the system of self-rating. Unless they were, their sites would be filtered out by many users for no good reason other than being unrated.

5.4 Authentication of users

A final element in systems of rating is what amounts to the rating of users themselves. The creator of a Web site or the moderator of a newsgroup could restrict access to all but authenticated users (effectively the members of a club, or registered customers). This would prevent access by children to material in sites only open to those with adult authentication.. (Cormack, 1997) The administration of this could be done in one of four main ways.

> Verification of users' IDs and the issue of passwords. This would require that potential users offered some proof of identity, age and perhaps other aspects of themselves, before being granted the right of access to a resource. Those accepted would be password identified, and only they would be able to visit a site or take part in a newsgroup.
>
> Address filtering by information providers, so that for instance only academic or educational users might be given access to a site.
>
> Validation by proxies. All requests for access would pass through a validation process by an outside body before being sent on to a site.
>
> Cryptographic certificates. These would be an electronic IDs to present to service providers when required. There are regarded as clumsy, because they must installed in a browser before use and removed afterwards.

Whilst discussion of authentication is mainly a privacy issue, it will be seen from the above that it does have a logical place in the discussion of filtering access to resources. By placing responsibility for who accesses a site firmly in the hands of information providers, it answers some problems inherent in other means of dealing with the issue. What it does is to get providers to police access to their resources in rather the same way that the proprietors of 'sex shops' in Britain are required to limit entry to those over 18, and bars in many American states have to check driving licences to ensure that their customers are all over 21.

There are websites, such as Adult Check, Adult Pass, Adult Sights, which offer verification services. Adult Check claims to be used by nearly 3000 websites which have 'adult' content. The way it works is that those who wish to have their status as adults authenticated for this purpose, respond to the site's request for details of name, address, and credit card. If these are accepted a password is issued for a payment of $12.95 per year. Even if the procedures used by those responsible for the site are sufficient to ensure that this information is accurate and consistent before the password is issued, it would be easy for a child to provide genuine details of an adult and then use this false identity. There is also evidence that the information held by these services is not secure, and that there are no means within the system to prevent one person using another's ID. (Markkula Center, 1997)

5.5 Research findings

A good deal of commentary on filtering centres upon its obvious or alleged technical imperfections. Opponents of filtering regularly cite the imperfect way in which filters work as a key element of their case. This is usually based on fairly casual testing of the system. For instance, a small investigation at the Markkula Center, Santa Clara University, tested whether filters would block sexually-explicit sites, sex education sites, safe sex sites, sites with factual material on lesbianism, similar sites with gay information. It found that the filters it tested blocked all sites in the first category, permitted access to sex education sites, had mixed results with safe sex sites, allowed material on lesbianism through, but blocked gay sites. These interesting but inconclusive findings are reasonably typical of those mentioned in discussions of the topic. So far there has been little independent research which thoroughly explores the effectiveness of Internet filtering, and its implications for the use of the Internet as an information resource.

An exception is the Internet Filter Assessment Project (TIFAP) which, although imperfect in a number of admitted ways, does provide a good deal of interesting information about the effects of filtering systems on the information seeker. This small project tested 18 examples of filtering software, looking at the way in which they blocked material by: keywords identified within their content; the names of particular sites ('intellectual de-selection' is what TIFAP calls this); and by protocols (all Usenet groups, IRC, or Telnet). Blocking sites was unsatisfactory because new sites spring up all the time, and until their content is identified as problematic they remain fully available. Blocking by protocols was revealed as extremely crude and over-inclusive.

Blocking by keywords was tested by attempting to obtain answers from the Internet to over 100 questions typical of those asked in libraries, while the software was in operation. The questions explored the software's treatment of eleven topic areas,

1. sex and pornography,
2. anatomy,
3. drugs, alcohol and tobacco,
4. gay issues,
5. crime (including paedophilia and child pornography),
6. obscene and 'racy' language,
7. culture and religion,
8. women's issues,
9. gambling,
10. hate groups and intolerance,

11. politics.

The questions approached these areas directly (by asking for research material on controversial topics) and tangentially (by 'inadvertently' asking for terms which might be blocked, such as recipes for chicken breasts, or cultivation of rape seed). The testers found that the filters blocked information needed to answer questions in over 35 per cent of cases, reacting to keywords and blocking sites with necessary information on topics such as safe sex, organizations for gay teenagers, and arguments for and against the legalization of drugs. The significance of this was that all the filters were, to some extent at least, doing more than their intended role of preventing inadvertent or deliberate access to material that was offensive or indecent. They were actually hindering legitimate and useful information searching.

5.6 The Debate

The debate on filtering has been carried on at a high rate of intensity ever since the defeat of the CDA seemed likely. As evidenced by the number of Websites representing organizations wholly or partially concerned with the issue, there is wide interest in the issue and a sharp polarization of opinion. The division seems to be between advocates of untrammelled free expression on the one side, and a spectrum of groups ranging from those pro-censorship to those anti-censorship, but favouring enhanced ability to avoid offensive material, on the other. A good deal of the debate centres on the use of filtering software in libraries on behalf of users, rather than on their use by families in the home.

The ACLU and the American Library Association were not merely key actors in the campaign against the CDA, but they both oppose filtering very strongly. Their position is based on a respect for individuals' and families' right to make up their own minds what they look at, and a conviction that filtering hinders this. Other sources of argument against filtering are to be found in the Web sites of Censorware Search Engine, Cyber-Rights & Cyber Liberties (UK), Ethical Spectacle, MIT SAFE, and Peace Fire. (See list of Web sites for URLs). There have also been a number of press reports and magazine articles drawing attention to the possible implications of filtering, of which the following are a selection. (Kleiner, 1997; Lasica, 1997; Wallich, 1997; Watson, 1997; Winner, 1997) A thorough review of the issues and technology from this perspective is Cyber-Rights and Cyber-Liberties (UK)'s report 'Who watches the watchmen: Internet content rating systems and privatized censorship'. (Cyber-Rights, 1997)

The basic technical case in favour of filtering is made very strongly by those responsible for PICS, particularly Paul Resnick of AT&T Labs, Chair of the PICS Working Group of W3C. (Resnick and Miller, 1996) Filtering is supported strongly by Filtering Facts, which is chiefly concerned with the use of filters in libraries. Its criteria for filterware selection listed in section 6.2.2 were devised largely for use by libraries. David Burt of Filtering Facts has countered a number of the arguments against filtering, including those arising from the admitted anomalies produced by the operation of products currently available. (Burt, 1997) Other sites which promote the case for filtering are Family Friendly Libraries, Enough is Enough, Library Watch, National Coalition for the Protection of Children and Families. (See list of Web sites for URLs) The form that the debate can take within the library community, between those who have chosen to filter or not to filter, is well illustrated by a published debate between the librarians of Austin (Tex) and Monroe County (Mich). (Branch and Conable, 1997)

6. Ethical Approaches

The common tendency to portray the Internet as a kind of anarchy ignores a considerable will amongst many users to encourage responsible use. It also fails to take account of the way in which the public organizations providing Internet access, service providers and, not least, the library community, have developed policies for purposeful and considerate community and family access to Internet content. The quality of the work done by librarians on ethical alternatives to the regulation and policing of the Internet is widely recognized by informed commentators. For those who reject both the formal regulation of the Internet, and the use of technology to restrict access to content, these explorations of ethical approaches hold the best possibilities of convincing the general public and political leaders that the Internet is actually a force for good, rather than some kind of threat to the structure of society.

6.1 Netiquette and acceptable use policies

6.1.1 Netiquette

The flooding of newsgroups, mailing lists or other elements of the network with messages publicizing the views of an individual, or advertising some product or service (spamming), and the sending of abusive mail (flaming) are one aspect of network use. Counterbalancing this is an evolving sense of the good manners which are required to make network use convenient and unthreatening for all. Codes of good manners for network users are referred to as 'netiquette' (sometimes nettiquette). Most of what they contain is unremarkable, amounting to a restatement of the elements of considerate conduct which apply in society generally. One widely-available codification of netiquette (Shea, 1994) is structured round 10 rules:

1. Remember the human;
2. Adhere to the same standards of behaviour online that you follow in real life;
3. Know where you are in cyberspace;
4. Respect other people's time and bandwidth;
5. Make yourself look good online;
6. Share expert knowledge;
7. Help keep flame wars under control;
8. Respect other people's privacy;
9. Don't abuse your power;
10. Be forgiving of other people's mistakes.

That such lists are more than just preaching by a few concerned users is evidenced by the numbers of outraged messages that appear in reaction to what are considered gross violations of good network behaviour. Intricate discussions within newsgroups of the rights and wrongs of some particular alleged infringement of the code are also not difficult to find. However, this concern with ethics is not the dominant tone of exchanges on the Internet. As one commentator points out,

> The fragmented nature of the Internet has prevented any formal ethical philosophy developing. Long-established users may follow the unwritten rules,

> but they are rapidly being diluted by the huge influx of new and inexperienced users. (Langford, 1995)

The obvious implication is that there is a need for something more carefully worked out and widely accepted than the rather vague goodwill expressed in netiquette.

6.1.2 Acceptable use policies

Whilst netiquette is essentially a guide for individual behaviour, acceptable use policies are the guidelines and requirements laid down by organizations relating to the conduct of users within their systems. The effort which has been put into creating such policies is considerable, and cumulatively they reveal a considerable consensus on what is reasonable use of the Internet. If all users followed the precepts of these policies, the perceived problems of Internet content would almost vanish overnight. Policies exist in enormous numbers. Many examples from schools, for instance, can be found on the Internet.A large number are listed in the Web site of Robbinsdale, Minnesota, School District. (See list of URLs) Advice is available for those compiling such documents, and one adviser discusses the issues under the following headings:

1. Intellectual freedom;
2. Ownership - intellectual and 'real';
3. Limits on resources;
4. Plausible denial (otherwise known as 'escape clauses', denying liability). (Wolf, 1994)

Other academic institutions, providers and networks also have their policies. The UK Joint Academic Network (JANET) set out a policy in April 1995 which effectively applies to all British academic users. In its ninth clause it spells out what is considered unacceptable use:

> 9.1 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;
>
> 9.2 the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
>
> 9.3 the creation or transmission of defamatory materials;

9.4 the transmission of materials such that this infringes the copyright of another person;

> 9.5 the transmission of unsolicited commercial or advertising material either to other User Organizations, or to organizations connected to other networks;
>
> 9.6 deliberate unauthorized access to facilities or services accessible via JANET;
>
> 9.7 deliberate activities with any of the following characteristics:

wasting staff effort or networked resources, including time on end systems accessible via JANET and the efforts of staff involved in the support of those systems;

corrupting or destroying other users' data;

violating the privacy of others;

disrupting the work of others;

using JANET in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment;

continuing to use an item of networking software or hardware after UKERNA has requested that use to cease because it is causing disruption to the correct functioning of JANET;

other misuse of JANET or networked resources, such as the introduction of 'viruses'.

Internet service providers also have their policies and a collection of these is available online. (See list for URL of Acceptable Use Policies site). The policy of America Online (AOL) sets out its principles with helpful explanations of the various elements it covers, such as email, Usenet and chat. (See list for URL) The problem is obviously that whilst providers of access in the public sector (schools, universities, libraries, government departments) might be able to enforce their policies with members and employees, it is a more delicate matter for commercial providers to limit the activities of paying customers.

6.1.3 Industry codes of practice

There is also work in progress to draw up industry-wide codes, which define more fully the obligations of the various types of provider. An organization called the Internet Content Register has, with cooperation from the UK Consumers Association, drawn up an Internet Code of Practice (ICOP). (Internet Code, 1997) This covers:

1. Audience, and ways of ensuring information is suitable for it;
2. Advertising, and the standards that should apply;
3. Contracts;
4. Copyright and information ownership;
5. Information, and its quality (including decency);
6. Applets, browser scripts and CGI usage;
7. Mail and news, particularly unsolicited communications;

The organization offers certification for service providers who undertake to operate under ICOP. This is to be backed up by monitoring and the investigation of complaints. An agreement is offered between Internet Content Register and service providers, which has clearly-stated mutual responsibilities. Whether this initiative proves to be successful or not, it offers ideas as to what shape industry self-regulation through codes of practice might take.

6.2 Library Policies

One regular theme that occurs in documents about self regulation of the Internet is tribute to the usefulness of library policies in addressing the whole issue. For example, Computers and Academic Freedom makes available an article which discusses how principles developed in the library world can be applied to public and academic use of computers. (Kadie, 1994) The principles discussed in this chiefly come from documents prepared by individual libraries, and by the American Library Association (ALA). Other important library organizations do not have such clearly articulated positions. The International Federation of Library Associations (IFLA) passed a resolution accepting the report of a Committee on Freedom of Access to Information and Freedom of Expression (CAIFE) at its meeting in Copenhagen in September 1997. However the recommendations in this document were of the most general kind and said nothing specific about networks. Subsequently, however, a permanent Committee of IFLA was established as an ongoing mechanism to address this issue. The Library Association (UK), whose members and secretariat do monitor and discuss freedom of expression on networks, also has only the most general policy documents, such as a Statement on Censorship (last revised in 1989).

The ALA, in contrast, has consistently taken a strong stand in favour of freedom of expression and accepts that it must therefore show how freedom can be used safely and responsibly. The basic position of the ALA is set out in its 'Library Bill of Rights', as revised in 1980, taken in conjunction with resolutions on 'Access to Electronic Information' of 1996, and 'Use of Filtering Software in Libraries' of July 1997. (See ALA Web site, URL in list) These documents show a firm stand on US constitutional freedoms, which are held to apply to all, regardless of their age (subject only to parental guidance for children). The Internet is treated as analogous to a library, and therefore the principles operating in libraries are argued to extend naturally to Internet access on library premises. (Markkula Center, 1997)

Filtering is accepted by some librarians, who draw a further analogy with book selection and the mediated access to parts of library collections which is normal for one reason or another. The crudity of the filters available has, however, created real difficulties for many librarians in reconciling their fundamental faith in freedom of information with the use of any filters. (Mason, 1997)In holding to policies favouring unhindered freedom of access, libraries are subject to pressure from organizations such as Enough is Enough. This organization provides a kit of questions and arguments for use by those wishing to encourage libraries to use filters to shelter children from offensive content. (Safeguards, 1997)

6.3 Personal and parental responsibility

Finally, there are organizations which point out that ultimately individuals must accept personal responsibility for what they choose to view on the Internet. Furthermore, they must accept that they have responsibility for what their children view. This line of argument turns attention towards rules for personal and family responsibility, and towards ways of making positive selection of high quality material. This is the implication of the policies of an organization called The Children's Partnership, which in turn cooperates with other US organizations, the National PTA and The National Urban League. The Children's Partnership focuses on parental involvement, the quality of information literacy skills teaching in schools, and equality of access in the information society, rather than on negative aspects of Internet use. (Parents, 1996)

As far as parental involvement is concerned, there are sets of suggested rules both for parents and children. The National Center for Missing and Exploited Children (see URL for Child Safety on the Information Highway) suggests the following seven guidelines for parents:

> never give out identifying information;
>
> get to know the services your child uses;
>
> never allow a child to arrange a face-to-face meeting with another user;
>
> never respond to offensive items;
>
> remember that people online may not be who they seem;
>
> remember that things read online may not be true;
>
> set reasonable rules and guidelines for your child.

A similar set of rules which parents can encourage children to follow is offered by Pippin (see URL), an organization promoting positive use of the Internet:

> don't give out your last name, address or phone number;
>
> don't lie about your age;
>
> remember that people may not be who they say they are;
>
> don't open attachments from people you don't know;
>
> if you're afraid, tell your parents;
>
> if you feel uncomfortable, save the message and leave;
>
> don't go alone to meet someone in person who you've met online.

The ALA, similarly, advises parents that the best way to ensure their child's safety on the Internet is to be there with them and to agree rules. (Librarian's Guide, 1997) Like several other organizations, it complements this by actively recommending sites which it feels will entertain and inform children. An original list of 50 has been expanded to more than 700, selected according to criteria that are displayed on the site. (Great Sites, 1997)

7. Conclusions to Part One

There are genuine causes for concern arising from the nature of some material available over the Internet. However, these differ from concerns over print and broadcast material only because of the comparatively unregulated way in which networked information enters the home, library and educational environment. Public and official anxiety has expressed itself in three main approaches to the issue: legislative solutions, filtering and blocking, and self-regulation of the Internet and its use.

Solutions based upon new legislation are generally inappropriate for various reasons:

> they tend to infringe the basic principle of free expression;
>
> they are difficult to enforce because the Internet operates under too many jurisdictions;
>
> the nature of the network provides technical means to avoid control, such as mirror-sites;
>
> the networked environment changes too fast for legislation to keep up with it.

Filtering and blocking is not a fully accepted solution on grounds both of principle and practicality. Objections in principle are more or less insurmountable, but some minor element of filtering could be used by parents, and those with parental responsibility, without deviating from the social norms which limit access by children to material in other forms. Use of filtering and blocking must be by choice and, if possible, consent. Their imposition without consent or the scope for challenge is surely just as unacceptable as any form of censorship. This is a compromise, but compromises are a normal part of the fabric of life.

At present, compromises on filtering and blocking are difficult because the filtering process is crude in its effects, and there is a lack of transparency as to what is blocked, and why. Any acceptance of filtering and blocking, by those who favour freedom of expression, will require much improved technology, and high quality systems for the rating and labelling of content. An acceptable platform for ratings metadata is already available in the form of PICS which, despite hostility to it from advocates of complete freedom of expression, is not, in itself, automatically an instrument of censorship.

It is the systems of rating which PICS would support which are more capable of being a means of censorship. Ratings systems require good sets of standards, and existing ratings standards, mainly designed to deal with recreational materials, are inadequately specific. To attach ratings metadata to content is ideally the work of content providers themselves, but good systems of third party provision are also acceptable. Properly funded ratings agencies, which enjoy the confidence of the Internet industry and users, would be needed if this alternative is to be pursued seriously.

Self-regulation of networks and their content through codes of practice for content and service providers and users is, in principle, and for technical reasons, the best means of ensuring confidence in networks as communication media. The improvement and promotion of such codes of practice will be required if they are to capable of effective application by the groups at which their provisions are directed. Self-regulation should not mean self-policing, so the relative spheres of law enforcement agencies and regulatory bodies need to be clearly delineated. Finally, self-regulation needs to be supported by programmes to encourage responsible and informed use of networks, along the lines of those provided by the ALA and other organizations.

Part Two:
Implementation of Freedom of Expression in Public Access Points

1. Introduction

Access to communications networks, particularly the Internet, is an issue for the individual and for governments, but it is also an issue for those who have managerial responsibility for public access points. It is clearly the responsibility of individuals to make decisions on their own behalf about what they look at and read. At the same time, democratic governments have a responsibility to ensure that the information available conforms to the requirements of the law, particularly on matters such as national security, the prevention of disorder and crime, and the protection of health and morals. But at a public access point, the essential responsibility of those in charge is to give individuals the fullest possible freedom to seek for knowledge. This is a difficult role for two reasons. One is the availability via networks of content which is illegal in the jurisdiction where it is accessed (though not necessarily illegal where it was originated) and other material which, whilst it is not illegal, is widely believed to be harmful. The second is that networks are extensively used by young people for whom their parents still have legal responsibility. Popular opinion is that these young people are in danger of harm from certain kinds of content. The manager of a public access point must find ways to cope with this confrontation between the basic principle on which public access is provided, and the anxieties about access that the nature of some content creates in the public mind.

That there is genuinely felt concern, rather than something created by the news media to increase interest in their publications and broadcasts, can easily be illustrated from some recent surveys of opinion in Britain. In the first Which? Online survey by the research agency MORI (Annual Internet Survey, 1998), 58% of respondents agreed with the suggestion that the Internet undermines the morality of the nation by making pornography and other illegal materials freely available, and only 13% said they would feel comfortable letting their children use the Internet unsupervised. At the same time, another MORI survey of children's attitudes suggested that parents might be right if they felt their children were potentially beyond their control in this area, since 30% of children were confident that they knew more than their teachers about the Internet (*Children's attitudes*, 1998). Finally, a slightly earlier survey of teachers' perceptions of what were termed 'the new entertainment technologies' revealed that teachers were seething with anxieties. Approximately 75% were confident that there was a cause and effect relationship between frequent use of computerised entertainment and various aspects of impaired learning (Miller, 1994). These concerns may, or may not, have a basis in reality, but they do create a particular environment of opinion in which public access points must be managed.

This report uses the same methods as those which were employed in Part one of this document. It presents an argument relating specifically to network public access points, based partially on the material presented in part one, but also on a fresh sampling of news and opinion from the first six months of 1998. The intention is to contribute to the preparation of Recommendations by the Council of Europe, which will be of assistance to governments contemplating legislation or other actions which will have implications for the management of public access points, and also for those who are directly responsible for the day-to-day management of such points.

2. Network Public Access Points

Although many families in Europe have a computer in the home (38% in Britain, with a higher percentage for homes where there are school age children) (Nation divided, 1997), this still leaves a large majority of the population dependent on public access points if they wish to make use of networked communication and information resources. Provision of public access is not at all evenly distributed between nations, nor it is it evenly distributed within nations. The highest levels of public access are available in educational establishments. Libraries and other information institutions, cultural institutions, and information kiosks, also give access. The extent of public access outside the educational sector varies considerably between individual institutions and types of institution. The importance of public access of this kind is that it is the source of any claim which networks might have to be a universally available phenomenon. Therefore the policies and administration of the hosting institutions are crucial to making freedom of expression and freedom of access to networked content matters of fact as well as principle.

2.1 Educational establishments

Access to networks in universities and other institutions of higher education is more or less universal in European countries, and schools increasingly also offer access to both their staff and students. More than 85% of British secondary schools have Internet access, although the same is true of only 5% of primary schools (Blamire, 1998). As a range of government initiatives are in place to spread school access more widely in Britain, it is reasonable to expect something like universal access will be achieved early in the new millennium, and other European countries are also moving swiftly in this direction. Universities generally seek to have a networked computer in every staff office, and many are also beginning to offer network connections in the rooms of student residences. However, more commonly, access is obtained in a computer room, laboratory or library. Such facilities vary from a single networked machine in some schools through to literally hundreds in the learning centres of well-equipped universities. This has the implication that, for the most part, networked material which is accessed by teachers in schools, and by students at all levels of education, is viewed in public areas of their institution.

2.2 Libraries and other information institutions

Internet access in libraries and information centres is an increasingly important form of public access. For the purposes of this report, access in academic and school libraries can be considered as an aspect of public access in educational institutions generally, rather than as part of library access. Research and other special libraries do, however, fit under this heading. Because of their closely defined and limited clientele, they differ from public libraries in matters of network public access. They, and access points provided in information offices specialising in tourism, education, employment, and other topics of importance to the citizen, have a defining clarity and singularity of purpose. The case in public libraries is clearly different, and it is public libraries in which the truly public access is beginning to be more common. Large numbers of British and Danish public libraries are substantially automated, and many offer Internet access. Universal connection of public libraries to the network is promised in Britain in the near future (*New library*, 1997). However, only 20% of German and Portuguese public libraries were considered as automated in 1996 (Thorhauge, 1997). Only 20 German public

libraries had their own Website in 1997, but progress since has been swift with quite small public libraries, such as that of Zadar, Croatia, having put up professionally presented Websites in 1998.

Archive services also have public workstations, firstly to provide access to their own networked finding and retrieval systems. Internet connection is appropriate at such points as a means to provide remote access to electronic archives and the Webpages of other archive services. Certain types of restriction on access to archive content are already a normal aspect of archival practice. They generally arise from the protection of official and institutional secrecy and of the privacy of individuals (Council of Europe, 1998). However, a strong principle of archival work is concerned with maximising access to documentation of the past in whatever form it occurs, so the provision of network public access points fits into the archive ethos very naturally.

2.3 Cultural institutions

It is now a common experience to visit a museum and find some form of multi-media presentation relating to the exhibitions and collections, but many museums also give access to networked cultural resources from outside their own walls. There is also a wealth of access provided by cultural institutions such as medialabs, community arts centres, and small arts-related companies of various kinds. This type of access varies greatly from example to example, but it tends to have in common the fact that it offers more than just the facilities to use content created by others, it provides opportunities to create new cultural or educational content. A few of the large and growing number of such centres are Artec, London; Society for Old and New Media, Amsterdam; Public Netbase, Vienna; Terravista, Lisbon; Mikro, Berlin (examples from an unpublished paper by Marleen Stikker, Society for Old and New Media). Any kind of restriction of access would be wholly alien to the philosophy of such centres, and would seriously inhibit that freedom to innovate with new media which is the centres' *raison d'etre*.

2.4 Kiosks and cafes

Finally, there is access which is public, in the sense that it is available at low cost to anyone who wishes to use it. This is at the same time often private, in the sense that it is provided by private organisations or on private premises. Internet cafes, or cyber cafes, are becoming ubiquitous in big and medium-sized cities. They offer cafe facilities with the possibility of time on networked computers (at a small cost), rather in the way that newspapers and magazines are still offered (free) for the use of customers of cafes in some European countries. There are also public information terminals, or kiosks, in the foyers of public buildings, shopping malls, transport centres, and also in the streets. Most of these offer dedicated access to some network providing local government, consumer, travel, or other similar information. Touchpoint in the UK is an example of such services. However, the Dutch national telecommunications service KPN Telecom now provides street terminals at which Internet access is available using a normal Dutch phonecard. This system is being expanded from 25 initial sites in Amsterdam, and there is interest from other parts of the world. In many ways these are the true public access points, unconstrained by the types of policy and administrative concern which come when an institution physically hosts a service.

3. The Issues

Although many of the issues which concern those responsible for public access points have been touched on in Part one of this report, it is necessary to draw together the main areas of concern at this point. These fall into two groups. First there are matters concerning the responsibility of public access points for the content which is available through them, and for the content actually accessed by users. These include:

- liability for illegal content;
- responsibility for harmful content;
- welfare of minors;
- avoidance of offence.

Then there are issues raised if the option of filtering and blocking content were to be adopted. These are essentially:

- the ethical rationale for filtering
- costs and consequences of filtering.

3.1 Liability for illegal content

Legal liability for what is used at the public access points for which they are responsible is a source of anxiety for managers. However, the tendency is for legal systems to place liability firmly with content providers. Information access providers, unless they have an editorial function in relation to the content which they make available, are also broadly exempt from liability. This did not prevent a judgement in the Bavarian courts in May 1998 that Felix Somm, former head of CompuServe in Germany, was guilty of aiding and abetting child pornography. The verdict did, however, seem to fly in the face of the recent German multi media legislation which exempted information access providers from liability for content placed there by their customers, unless they were aware of the content and had failed to take means to remove it (Child porn, 1998). It is clear from this that there is no real legal threat to managers of public access points on account of content which might possibly be accessed from workstations they have provided. If indeed such material is accessed, the liability falls chiefly on the user. There have been cases, for instance, of teachers suspended or dismissed for accessing pornography on screens which might be visible to young people in their care.

3.2 Responsibility for harmful content

The issue of so-called harmful, but not actually illegal, content is a more difficult one. The distaste of vocal and well-organised people for some Internet content which presents sexual, drug-related, political and other controversial matters, but which clearly enjoys the protection of the law in most democratic countries, has led to discussion of this category of material being rolled up into the discussion of illegal material. This is a dangerous confusion because it threatens to undermine the central purpose of public access points, and the institutions which provide them. If material is not illegal then the citizen has a clear right to choose to use it. The manager of a public access point is not essentially responsible for the content itself, but has a clear responsibility for providing free access to that content.

Much of the debate over this has concentrated on libraries, but it affects all types of information institution. Archive services, for instance, have a commitment to free access similar to that of libraries. An important issue that has so far been very little addressed in professional debate is the archiving of Internet content. A publicly accessible digital archive should seek to represent Internet content for posterity, and in doing so should concentrate on content which has not been paralleled on paper. If this principle is followed logically, the kinds of controversial material which present problems at other public access points will also be there to present the same problems for archival services.

It is important that the principle of free access is clearly understood across the information professions. At the conference on 'The Twenty First Century Information Society: the Role of Library Associations' held in Budapest, 11-13 May 1998, the centrality of freedom was strongly restated, for instance by Barbara Ford, President of the American Library Association: 'intellectual freedom is the core value of the library profession' or Bendik Rugaas, National Librarian of Norway: 'freedom is the whole rationale of librarianship'. Such principles can also be applied very strongly to other professional information activities in the educational and cultural spheres.

The principle of freedom is particularly important when looking at institutions like public libraries, which have the widest possible remit in subject terms. Their broad cultural function naturally allows the user to follow lines of investigation which can lead to material on areas of intellectual, political and artistic controversy. Whilst some people would argue that publicly-funded institutions should not permit access to material which can be seen as harmful, preventing this would be a clear violation of rights of free access to information.

3.3 The welfare of minors

In all of the debate, the issue is most difficult when it is applied to young people for whom parents still have legal responsibility. Schools and other institutions take on some of this responsibility *in loco parentis*, and must try to act in the same spirit as parents would. However, although parents and their surrogates may have the legal right to restrict the access of the young people in their care, it is debatable whether they have a full moral right to do so. It could be argued that a public access point which made information about safe sex or dealing with drug problems available to young people would have acted more in their interests than a parent who tried to keep this information away from them.

Be this as it may, the tendency has been for institutions not to provide full access to information for children, Sometimes this is because they cannot: many systems of schooling rely wholly on material generated by the teacher, and on textbooks. Indeed, school libraries with any real range of content are the exception rather than the rule throughout most of Europe. Even in the USA, where large and well-stocked libraries are the norm, there has been a tradition of quite strict control of the material available (Doyle, 1997). As a recent writer puts it:

> There seems to be plenty of legal and historical precedent for censorship of any medium that is used in tax-supported public schools (Lamont Johnson, 1996).

Thus, whilst limiting young people's access to networks would destroy some of that valuable freedom to explore and learn through exploring which networks offer, it has to be recognised that it would not be unusual in terms of existing practice in school systems.

3.4 Avoidance of offence to other users

At one level, recreational use of networked content in public areas can potentially distract the attention of 'serious users'. The playing of noisy or brightly-flashing games might fall into this category. In certain types of information institution (special libraries etc), access to networks is provided with either public or private funding for purposes which, although they might on occasion include aspects of recreation, have a specifically defined informational, educational or cultural purpose. It is arguable that the network user at access points provided in such institutions has no particular right to access material other than that which is relevant to the defined purposes of the institution. This would mean that blocking access to irrelevant content would not be a significant violation of basic rights.

At another level, if access is to content which is illegal or harmful, and pornography is most commonly mentioned in this context, then offence, moral disturbance and, allegedly, harassment can be seen to take place. It is frequently argued that the user accessing distasteful text, images, and even sound, at a public terminal should be prevented from causing offence to other users. There are anecdotes about users masturbating whilst viewing pornography at public access points, and women have brought successful sexual harassment cases against bosses and fellow employees who have left downloaded pornographic material in files which they have then accessed. However, the same type of argument has always applied, and still applies (just as weakly as ever) to people with open books and magazines in front of them at some public point such as a library desk. There is a difference between discreetly accessing distasteful material, for whatever reason, and deliberately or carelessly offending others with it. The latter can be dealt with by the manager without necessarily preventing use, but to interfere with the former is to accept that one person's moral or temperamental preferences override those of another.

3.5 Ethical rationale for filtering content

The question is, if a public access point filters content and blocks certain categories, is it actually practising censorship. Filtering has been described on the one hand as 'the privatizing of censorship' (Lasica, 1997) and on the other as 'a real alternative to Internet censorship' (Internet censorship, 1997). There is truth in both of these positions, but it varies according to the circumstances. For the individual or family strongly wishing to restrict their own exposure to certain types of content, filtering might indeed seem an acceptable alternative to censorship. The wording of what the Bonn Declaration has to say on filtering and rating should be noted. It says that the important thing is:

> To enable users to select categories of content they do or do not wish to receive, so as to deal with information overload and undesired or harmful content (Ministerial Conference, 1997).

It speaks of users, rather than those acting on their behalf. It mentions filtering for what users do want, before mentioning what they do not want. It refers to the problem of tracing resources in a situation of information overload before it refers to undesired content. All this is about the individual exercising choice.

However, for the individual using a public access point, the use of filtering software by the host institution would definitely seem to be the application of censorship. It would also, in most countries, go beyond the requirements of the law. Since it is the public access point which is the concern of this report, it is the latter case which needs to be looked at further. As suggested in Section 3.3, the use of filtering in a school system would not be incompatible with tradition in a type of institution where the concept of *in loco parentis* is very important. It might also be justifiable in institutions where public access was necessarily constrained by the aims and objectives of those institutions (see Section 3.4) for reasons not connected with moral judgements on the content that might be accessed.

Where filtering is surely inappropriate is in information providing institutions with a broad remit, and of public libraries in particular. The strongest defender of this viewpoint is, as noted in Part one, the American Library Association (ALA). In doing so it cites the First Amendment to the American Constitution, which was the inspiration for the Library Bill of Rights. This was adopted by the ALA on 16th June 1948 and has been reaffirmed since, most recently on 23rd January 1996 (*Library Bill*, 1996). It states unequivocally that:

> Libraries should provide materials and information presenting all points of view on current and historical issues. Materials should not be proscribed or removed because of partisan or doctrinal disapproval.

It is sometimes argued that since librarians have always exercised selection in what they have purchased and made available to the public, the use of filtering is a logical extension of that practice. Whilst it is probably true that some librarians used the need to select as a convenient method for avoiding the acquisition of controversial material, the Bill of Rights clearly calls for all viewpoints to be reflected. With the Internet, there is no reason to select because of lack of money or storage space, so all viewpoints can now be reflected by the full range of available material. Indeed a US federal district judge directly rejected the selection/filtering analogy, pointing out that since Internet resources do not require shelf space or physical maintenance, it actually costs a library more to restrict content than it does to allow unrestricted access (Censorship ruling, 1998). The logic of this is that despite the passionate defences which are offered for it (Burt, 1997), filtering is not an acceptable practice for genuine public access points.

3.6 Costs and consequences of filtering

To filter content involves direct costs at virtually every point along the information chain. The cost of purchasing and installing filtering and blocking software is probably the smallest element involved, and falls directly on the owner, even if the software is supplied along with the rest of the system. In the city of Boston, Massachusetts, where 200 public access terminals were filtered, the cost was estimated at $10 per networked computer, and $40 per computer with direct dial-in access. Most of the rest of the costs are almost impossible to quantify, and they are distributed amongst the various players. Only their scale is obvious.

The creation of a metadata platform, such as PICS, involves costs right across the system. Likewise the creation of ratings systems is not cost free, although the direct cost may be borne by some interested body such as a trade association (the Recreational Software Association, for example), lobbying organisation, or religious body. The cost of actually applying ratings to particular Websites or items of content by some third party such as an agency specifically set up to provide ratings would be enormous, if only because there are millions of items that would need rating. Even self rating has costs. These include small ones arising from the time and trouble the content provider has to put into the task, but also larger ones from any monitoring and enforcement of the system by an official or non-governmental agency (similar to the Internet Watch Foundation in Britain). Excluding minors from using sites with ratings that indicated legal 'adult' content through systems of user-authentication also has a cost. This is a visible cost because, at present, authentication agencies recoup their own costs through fees to their clients. Even if filtering and blocking was to be universally applied, the costs of policing and the legal costs of prosecutions would not be eliminated. They would also not necessarily be reduced, since a higher level of content regulation could actually result in the identification of more instances that seemed to call for the attention of law enforcement agencies and the legal system.

The issue of costs is not simply one concerning aspects to which money values can be assigned: there are also what the economist calls the *opportunity costs* of gains which are lost or foregone. Placing restrictions on use can deny the benefits that occur from comparatively unfocused surfing of the Internet as a means of developing information skills and experience. Restrictions on navigation through the Internet can also seriously restrict the creative potential that is offered by accidental discoveries and the unexpected juxtaposition of images and ideas. The Internet is too chaotic for its use to be easily channelled into totally predictable directions, and there might well be losses to the individual or organisation if this were to be attempted.

On the other side of the argument, it can be suggested that there are costs arising from not filtering. For instance, a reason for restricting access to networks in an institutional context is that a good proportion of Internet use within organisations is recreational. It is quite simply the case that such usage will not only take up an employee or student's time for purposes which are not directly relevant to an organisation's aims and objectives, but that it can easily test the bandwidth and memory of an institution's systems and therefore be to the detriment of more relevant use. Managers have little difficulty in believing that the interests of the organisation require policies restricting non-relevant access, and that this can best be administered by blocking access to certain aspects of content.

There is also the cost of alleged damage to those exposed to harmful material. Those who wish to restrict or exclude certain kinds of content argue that it encourages behaviour which has social costs, some of which can be quantified. Thus, if drug-taking were encouraged by networked content, this could have consequences for crime rates and the need for certain kinds of psychological and medical provision. The trauma of accidental exposure to distasteful content has already been alleged in sexual harassment cases, and the consequences can be measured in the compensation awarded to victims and the punishments to perpetrators.

Most aspects of these issues have been the subject of impassioned debate within the information professions in the USA. The listserv operated by ALA's Office for Intellectual Freedom saw debate deteriorate to a level of personal abuse that led to calls for the list to be moderated (Berry, 1998). David Burt, perhaps the library community's chief advocate for filtering, withdrew from the list as a consequence, and refused to contribute unless moderation was introduced. Although Burt's views seem to be those of a minority in the ALA, they are strongly represented in the broader community (see Part I, Section 5.6). As a response to this, the ALA issues documents to assist librarians cope with community challenges to library materials (*Coping with challenge*s, 1996; *Questions and answers*, 1997). Whilst the debate also exists in Europe, it has not been conducted with anything like the same intensity.

4. Filtering: Legislation and Implementation

The debate, as far as it affects public access points, centres on filtering and the blocking of certain content as a result of this process. The content of the debate touches on all or most of the issues outlined in the previous section. It tends to focus on two main areas: attempts to legislate, and the struggles that occur when particular communities attempt to introduce filtering in their libraries and schools.

4.1 European Law

Since the Part One of this report was completed (December 1997) the most significant European development in the political debate on filtering is the Recommendation on the Protection of Minors and Human Dignity in the Audiovisual and Information Services (European Commission, 1998). This was passed by the European Parliament on 14th May 1998 by a majority of 513 to 1 and adopted on 28th May by the Council. It recognises that illegal content and harmful content are two distinct issues, requiring different approaches and solutions. The document stresses self-regulation and responsibility, and, in particular, in its Recommendation 5, it calls for measures to 'facilitate identification of, and access to, quality content and services for minors, including through the provision of means of access in educational establishments and public places'. This emphasis on facilitating access to quality content, as opposed to preventing access to harmful content, is an important assertion that policy should be based on positive principles rather than those governed by fears.

The document goes on to suggest that self-regulation should be through a code, or codes, of conduct. So that a code can offer protection to minors, it suggests that information service providers should indicate potentially harmful conduct by a warning page, descriptive labelling, and systems to check the age of users. It also suggests that parental control should be assisted by filter software activated by the user, and filter options activated by operators at a higher level (presumably referring to options for the settings that the user can choose to apply). None of this refers explicitly to filtering at public access points. This is important, because if such principles were to be applied to public access points, particularly those used by people of all ages, they would produce effects which it is important to examine closely.

At public access points intended solely for young people (schools, or children's libraries) the recommendations would permit the use of a filtering system in a way that could grant the maximum access, whilst offering parents the assurance that access takes place in a safe environment. The providers would ensure that content which might be considered unsuitable for young people could not be easily accessed inadvertently. A warning page would offer the user the opportunity to choose not to access material. Descriptive labelling would reinforce this and permit filtering that is precise because it can be based on considered assessments of content. The age checking systems would oblige young users to draw back from access to sites when this is prohibited by the content provider (or to take responsibility for access by cheating the system in some way). The manager of a public access point for young people would then have the ability to advise and assist users on the basis of the information these warnings and blockings provide. At this stage, it would be possible to disable or adjust filtering by negotiation, if material were seen to be blocked unnecessarily.

At a public access point provided for people of all ages (in a public library, for instance) the case would alter. An adult might well wish to take advantage of warnings so as to avoid content that might be distasteful. At the same time, that same adult might wish to access legally available, but distasteful, content for any one of a number of perfectly legitimate reasons. The warnings might be irrelevant and the age check no problem, but filtering, on the basis of what parents might not wish children to see, would produce a clear interference with the adult user's right of free access to information. Thus, admirable though the Recommendation might be in many ways, any code of conduct for network public access points which might be derived from it needs to ensure that concern with the protection of minors is not allowed to compromise fundamental rights.

At the national level, there has been fairly recent legislation in Germany. An amendment to the Act on the Dissemination of Publications Morally Harmful to Youth was implemented in August 1997, as part of a group of measures responding to EC Directives (Federal Republic of Germany, 1997). It refers to 'technical measures... to ensure that the offer or dissemination [of morally harmful publications by means of electronic information and communication services] within Germany is restricted to users of legal age.' This has generally been interpreted to require that filtering software should be installed on public access point workstations available to those under the age of 18, although the wording (in translation) seems obscure. The Act would seem to be the firmest enactment on filtering in Europe.

4.2 The law in the USA after CDA

Since the Communications Decency Act was defeated in the courts in 1997, the political debate has shifted. The Internet summit held in Washington, 1-3 December 1997, produced little consensus. In a contribution perhaps significant for what it did not say, Vice President Gore strongly endorsed parental use of filtering, but he, and the Summit as a whole, did not concern themselves with public access points to any great extent. Since popular indignation and distress over Internet content was not dispelled by the Summit, or other initiatives, further bills have been tabled in the US legislature.

The most significant of these has been Senator John McCain's Internet Schools Filtering Bill (St. Lifer, 1998). This limits discounted telecommunications services, otherwise available to schools and libraries, to those which agree to apply filtering restrictions to their Internet access. This bill has passed its initial stages, despite the suspicion that President Clinton and Vice President Gore would prefer an amendment limiting subsidies to access points which have a strategy in place to protect minors. The ALA has opposed the bill on grounds of principle, saying that it would prevent libraries from meeting the information needs of the whole community. It has also been pointed out that many libraries would refuse to apply for the telecoms subsidies if these were tied to the imposition of filtering. McCain's own defence of his bill is that

> The prevention lies not in censoring what goes into the Internet, but rather in filtering what comes out of it onto the computers our children use outside the

home (Flagg, 1998).

Whilst this is true as far as it goes, the prevention would effectively apply to adults as well as children, and makes no distinction between young people of different ages. Material, on safe sex for instance, which might be unsuitable for a 6 year old, might be very appropriate for a 16 year old.

At state level there is also considerable legislative activity. This varies in focus, but is usually concerned with protection of minors from harmful materials (Oder, 1998). In various states, such as New Mexico and Ohio there have been legislative attempts to regulate the content of Internet providers. These have not made much progress, and their fate seems likely to be similar to that of a 1996 New York State law which was ruled invalid in the courts. More significant have been measures to mandate the filtering of sexually explicit materials at public access points used by minors. During 1998 in Arizona, California, Indiana, Kansas, Missouri, Oklahoma, Tennessee, Virginia and Washington bills have been introduced which, although varying in the details of their approach, are all at least partially directed at public access points. Several resemble the McCain bill in tying funding to filtering in some way. In most of these cases the American Library Association has mounted effective campaigns of information and lobbying to modify or defeat the proposed measures. This is clearly an ongoing struggle that will continue into the immediate future.

4.3 Implementation of filtering

A number of communities, the most prominent examples being in the USA, have sought to introduce filtering at public access points within their jurisdiction. These cases have produced the clearest expression of the divisions of opinion over filtering. Some of the American cases have become minor *causes celebres*. Two important ones (Austin, Texas, and Loudoun, Virginia) will be discussed in some detail here.

4.3.1 Austin, Texas

Austin Public Libraries have been filtering since 1997 (Branch and Conable, 1997). This was precipitated by two incidents that disturbed staff: a user was found printing out pictures of paedophile sex, and an adult was found showing children how to access pornography. Filtering with the Cyber Patrol software was begun as an interim measure, and Austin has continued to examine its position on the issue ever since. Three reasons for filtering were cited: to shield children from harmful content; to protect staff from what some regarded as sexual harassment; to avoid legal liability for users accessing illegal content. The Austin librarians acknowledge that the system blocks some legal and useful material, but they have unblocked about 300 sites in response to public demand. To try to avoid liability for interference with users' First Amendment rights they post a warning that content is filtered at each Internet workstation. They do not use the full range of possibilities offered by the software, originally choosing only to block 'partial and full nudity', 'gross depictions' and 'sexual acts'.

The interesting thing about the Austin case is that filtering was adopted only tentatively and the process has been closely monitored since (Cyber Patrol, 1998). The data-systems programming manager has adjusted the settings in Cyber Patrol to meet the perceived need, and the types of material blocked have been reduced to just the sexual acts category. They have examined the possibility of designating some machines for children and other (unfiltered) machines for adults. This was originally felt to be impractical at branches where there were only two machines and more than half of usage was by adults. Discomfort for users where differential access has subsequently been tried has indeed been a problem. Experiments have been carried out with screening some terminals to ensure privacy, and this has not proved entirely satisfactory (Schuyler, 1997). Because of all this, Austin has some claim to be a laboratory for filtering in public libraries. The results from the laboratory have provided some useful messages about the administration of filtering in practice. The significant thing is that since it was introduced in Austin, there has been a considerable reduction of the level of filtering first adopted. This is as a result of consideration of the day-to-day experience of librarians and users with the effects of filtering. It represents a process of attempting to reconcile the concerns which originally led to filtering with provision of information service which meets the requirements of users.

4.3.2 Loudoun, Virginia

The case of Loudoun is important because of the public scrutiny to which it has been subjected, and the way it has been tested in the courts. The court actions, initiated by a citizen's group calling itself Mainstream Loudoun in December 1997, challenged the installation of filters on all the library's terminals (St. Lifer and Rogers, 1998a). Filtering had been introduced for reasons similar to those cited by Austin. These were to protect minors, but also to stop use of offensive material by adults, because this would create a 'hostile environment' in which claims of sexual harassment might be made. It was also to avoid the danger of the library, or its employees being held liable for illegal material accessed by users. The software chosen by Loudoun is X-Stop, which, like many other filtering products, has been alleged to block sites considerably beyond the range originally intended. A number of highly respectable sites such as the Zero Population Growth site, the Safer Sex Education site, and the American Association of University Women's site, have been mentioned. Loudoun's response to this is that users can request the unblocking of sites, and this will be done at the discretion of the librarians.

The defence to the lawsuit which was offered by Loudoun was that filtering is analogous to various accepted library practices. In taking this line, Loudoun went somewhat beyond the usual equation of filtering with libraries' selection of the books and other materials they acquire, in preference to other materials which they reject. It was argued that libraries were free to select some items and not others, and that they were not compelled to acquire the rejected materials on request, just as they were not compelled to use inter library loan to borrow books they had chosen not to buy. This argument was countered by Mainstream Loudoun, who argued that the Internet was actually all one acquisition, and that refusing to let a user have something from the Internet was the equivalent of removing a book from the shelves, or cutting articles out of an encyclopedia. As reported in Section 3.5 the judge rejected Loudoun's argument (St. Lifer and Rogers, 1998b) on 7th April 1998, on the grounds that their policy was not analogous to a selection decision, but to refusing a user access to material already within a library collection.

The Loudoun case illustrates what a vigorous defence of filtering might involve, but it is interesting to contrast it with the neighbouring Prince William County, Virginia, which has chosen a rather different policy. The Library Board there voted against filtering, preferring to allow most terminals in the library to be used for unrestricted Internet access. The exception to this were to be the terminals in the children's room, where young people were to be directed to sites preselected for quality, and mediated through software called the Library Channel. This software system has been criticised for not presenting a representative subset of Internet content, and for blocking some sites in effectively the same way as the filters used elsewhere. However, since Prince William does not intend to prevent young people's access to terminals outside the children's room, their ability to search widely will be retained. Surveys of local opinion seem broadly to support this approach, and the divisions experienced in Loudoun have so far been avoided by its neighbour.

5. Management of Freedom of Expression

Although the Internet represents a new generation of media which is in the process of transforming communication throughout the globe, it should be remembered that not everything about it is unfamiliar. It does have an enormous amount in common with other communications media. It requires senders, such as creators of Websites and other content providers, or email correspondents and contributors to chat facilities. It has channels in the form of computers and telecommunication links. There are receivers in the form of Internet users who, with a pleasing circularity, are also senders when they themselves contribute content, however fragmentary that might be. The content which the Internet carries is fundamentally no different from other human communication, it is merely richer, more varied in form and more easily available than with most previous modes of communication. It is because of the richness and apparent unfamiliarity of the Internet that it is a source of anxiety amounting to fear. This fear is the reason why calls are made for it to be managed for the protection of users, particular of young people as users.

Such calls have a considerable impact on the managers of public access points. They are obliged to devise strategies which will address the anxieties and fears of the public, their representatives, and the news media which comment on the situation. In doing this, they can call on principles and interpretations which have been developed to deal with past and present forms of media and content. The validity of existing principles is not seriously compromised in the new circumstances, but it has become necessary to decide how they should be interpreted in relation to new technologies. It will be argued here that three main approaches offer themselves to the managers of network public access points. These can be identified as:

- regulatory approach, with the role of the manager reduced to that of administrator of laws and regulations strictly interpreted;
- automated implementation, through delegation of managerial decisions to a system which will filter and block information on the basis of pre-set standards;
- self-responsibility, through acceptance of the need to develop principled strategies and to take responsibility for decisions case by case.

5.1 Implementation driven by regulation

This amounts to an acceptance that the role of the manager is merely to understand the law and apply its requirements strictly and literally. The extension of this position is usually to avoid acting with any freedom in areas where the law is silent or unspecific. The implications of this approach vary according to the nature of the laws which apply in a particular jurisdiction. Thus in the USA and some other democracies the constitution and the law derived from it provide for broad freedoms so that it is then naturally the responsibility of the manager to protect and enhance these freedoms. The principled struggle of the American Library Association against the Communications Decency Act, and its continuing campaign against filtering, show a commitment to the protection of constitutional freedoms, rather than a passive wait for legislative guidance. In more restrictive systems, such as that of the former Soviet Union, and the authoritarian regimes prevalent in many other parts of the world, the role of the manager can essentially deteriorate to that of an administrator of restrictions on access to information and freedom of expression imposed from above.

Whilst this might suggest the superiority of an ethos based in constitutional freedoms, such a position does not always produce simple solutions to problems. The ethical position of modern librarianship is, for instance, not as straightforward as it is usually presented. In the first half of this century, librarianship was dominated by an activist philosophy which encouraged the librarian 'to shape the reading and through it the thought of the whole community' (Harris, 1976). Only in the last fifty or so years has this been gradually replaced by a philosophy which focuses on freedom of expression and access to information. The fight against censorship has replaced the concern with the quality and appropriateness of information as the main driving principle. A major impetus for this seems to have been the involvement of American librarians in the struggle against the injustices of the McCarthy era. It was paralleled in Britain by the development of a neutral stance expressed in the so-called creed of the librarian: 'no politics, no religion, no morals' (Foskett, 1962). The problem with this is that, at its extreme, it effectively exempts the librarian from ethical decision-making.

The practical effects of an uncritical reliance on freedom of access to information are easy to illustrate. In 1976 Robert Hauptman conducted a simple experiment (Hauptman, 1976). He visited 13 libraries and asked for information on the chemical properties of the explosive cordite, strongly implying that he intended to blow up a suburban house. Each librarian he consulted complied with his request without question, and he concluded that they showed no obvious sign of awareness that they were making an ethical decision. Hauptman's conclusions were disputed by some who argued, for instance, that the librarians 'were indeed demonstrating an ethical commitment not abjuring one' (Swan, 1982). Despite this, it is clear that too literal a reliance on external guidance can reduce the role of the manager of public access to information to that of a passive administrator of the decisions of others. It is important to remember that, depending on the nature of the external influence, this position can expose managers to the moral ambiguities of freedom just as easily as it can turn them into the agents of a system of censorship.

In one or two countries, Britain and the Netherlands for example, bodies have been set up to act as middlemen between law enforcement and the providers of information. Their existence also potentially allows the manager of public access points to withdraw from both policy- and decision-making in favour of a specific external agency. The Internet Watch Foundation (IWF) in Britain operates a 'hotline' for members of the public to report Internet content to which they object. It its first year of existence it received 781 reports, dealing with over 4300 items, usually containing child pornography (Internet Watch Foundation, 1998a). In about half of these cases, it felt able to approach the relevant Internet Service Provider, so as to get the offending material removed. The IWF has also turned its attention to questions of access, and recommends filtering and rating as a system which 'allows free speech on the Net and free choice to consumers' (Internet Watch Foundation, 1998b). As is pointed out in the next section, filtering may indeed be of benefit to individual consumers. The same is not, however, the case for the user of a filtered public access point.

5.2 Automated management

Automated filtering and blocking of Internet content offer a superficially attractive means of resolving problems with access. As stressed in Vol I, filters are not necessarily objectionable in principle. The idea of filtering the chaotic resources of the Internet both for content that one positively wishes to use and for content which one wishes to avoid, is a valid reaction to information overload. To apply filtering systems on behalf of another, as a librarian might do for a user, is also perfectly reasonable, if the wants of the other are fully known and mutually agreed. To apply filtering systems on behalf of a whole community, containing as it must, individuals with a range of interests, tastes and sensibilities, clearly risks constraining the freedom of all or some members of that community.

The manager of a public access point is clearly in need of good guidance on the question of filtering. The cases discussed in 4.3 illustrate the issues that filtering raises and the difficulty of using experience with more familiar media like print to produce helpful interpretations. Perhaps the more interesting example from the practical point of view is that of Austin, Texas. It has been in progress long enough to illustrate the dialogue between principle and practice very amply. It also illustrates how much work there is to be done if the manager seeks to use the filter as more than just a means for keeping the problem of Internet content at arms' length. If there is a serious intent to allow the maximum legal access on behalf of both adults and children, then a filtering system must be fully understood and the ability to manipulate its operation must be obtained. The ways in which filters work are not completely transparent to the purchaser, and adjusting the way they operate is not an easy matter.

Schneider (1997) provides a thorough guide to filters, and her advice is that a filter is not a single solution and that its adoption will call for a great deal of work. The first aspect of this work is testing any filtering product that is being considered for purchase. This testing should take place in the environment in which it is intended to use it, and should assess its performance in real life situations. Like most software products, the filters which are on the market were shown by Schneider's research to behave both worse and better than expected, and they generally tended to behave differently from expectations. What emerges from her case studies of filter use in a number of libraries is that if libraries developed an overall Internet strategy, they could incorporate filtering in this to the level they wanted. This might mean using filtering system-wide, using filters to limit access on some computers only, incorporating aspects of filtering in a programme to promote Internet use by children, or using some arrangement such as privacy screens on some computers in preference to filtering. Her advice, and the detail she provides, dispels the idea that filters are an easy substitute for taking full responsibility for access decisions.

5.3 Self responsibility

This is the acceptance of the full responsibility for managing public access to networks. It rejects both dependence on a rigid interpretation of laws and externally-imposed regulations on the one hand, and the aid of devices which remove the need to make decisions on cases on the other. It is the most demanding course to adopt, and requires both preparedness and continuing vigilance. Preparedness is expressed through the development of policies for access. Vigilance is needed so as to offer a continuing interpretation of policy as cases present themselves to the manager. The principles which guide this approach are present in the philosophy of modern information work and librarianship, and are also implicit in modern educational philosophy.

To deal with the latter first, the ideas which have driven educational change and development in the second half of the century, have been rooted in a concept of the individual child as the centre of the learning process. This child-centred approach sees the schoolchild's development as beginning from very different levels of experience which create unique learning needs. Ultimately the child has responsibility for satisfying these needs, and this means that the teacher must withdraw from the position of arbiter of the learning process. The role of the teacher becomes that of advisor, facilitator and counsellor. Although this position has been consistently opposed by supporters of a more traditional pedagogy, respect for the child as an individual learner is present throughout the school systems of Europe and North America. Thus even a teachers' organisation with a traditional approach phrases its professional code in terms of the child's individuality:

> The professional teacher recognises the individuality of every student, respects his or her personality, fosters a healthy environment for education and learning, exercises authority with compassion and ensures that disciplinary or other corrective action is constructive and refrains from words or actions which are destructive or negative and respects the dignity of all concerned (Professional Association of Teachers, 1988).

The recognition of the autonomy of the individual learner has obvious implications for provision for children with special learning needs, for members of minority groups, and for those isolated from centres of education. It also leads naturally into the concept of lifelong learning, or continuing education, and it has obvious implications for access to an individual learning resource such as the Internet. It is radically different from the generalised view of the learner which informs the arguments of those who wish to control Internet access. Their view regards children as the object of a learning process directed by teachers, with the support and guidance of parents, in which knowledge is passed on at levels and speeds determined on the child's behalf by the system. Educational systems now generally recognise that individuals learn in different ways, have different requirements as to the subjects they study, progress at different speeds, and have different levels of emotional maturity. It therefore follows that those who manage a resource for individual learning, such as the Internet, should seek to maximise the learner's freedom to use it in ways that meet individual needs.

Library and information professionals also recognise the centrality of the information user in ways which they did not always do in the past. The philosophy of neutrality outlined in 5.1, whilst it can result in a passive acceptance of external control, does also seek to grant individuals the maximum scope to discover for themselves. Progressive library and information systems accept that they must not only seek to understand the evolving needs and preferences of their community, through user research, community profiling and performance monitoring, but they must also use this knowledge to create systems which will facilitate the autonomy of the 'end user'. This can be an uncomfortable position for a professional whose role has always been that of an intermediary, trained to find and select content on behalf of others. It does not necessarily, however, reduce the importance of the information professional, whose intervention is still required to help the user search effectively and obtain maximum benefit from the content discovered.

Both the child-centred view of education, and the user-centred view of librarianship point towards the position classically adopted in the professions - that the professional's first duty is to the client. As Hill (1997) points out, in the work of what he refers to as the modern information professional (MIP), it is sometimes unclear as to who actually is the client: the schoolchild or the parent, or the school board; the library user or the librarian's employer. However, the principled position is that the client is the individual whose specific needs are served. It is usual for professionals in all spheres (medical, legal, financial, etc.) to see the client as entitled to expect a degree of confidentiality in the relationship, and to expect to be treated equally with other clients. This has implications if the information professional regards a young person as the client, since it raises the question as to when the parent's views are the most significant and when its the child's. There is a clear sense that in many cases the child's expressed preferences would be the professional's concern, with all which that might conceivably imply in terms of Internet use.

Hill's discussion of information ethics includes the suggestion of two principles that are central to the debate over Internet public access points. They are:

- an MIP shall at all times defend and promote the right of the freedom of information in the context of access to information and that of communicating information to third parties;
- an MIP shall not attempt to censor or hide information unless required to do so by the law of the land and even then not if to do so is contrary to universally accepted human rights.

Although the phrasing of these suggested principles is not of the clearest, their broad intention is obvious and likely to be widely endorsed by those who work with information. These principles make it imperative for the manager to take full responsibility for the public access point, without delegating either policy to some external form of regulation, or day-to-day administration to an electronic device.

6. Conclusion to Part Two

The question that Part Two sets out to deal with is how public access points should be managed so as to provide genuinely broad and full access to networked information. The problem that is addressed is that of the illegal and harmful content that is seen as an inhibition to granting complete access. Important problems such as how governments can meet the costs of democratic access, or how content can be provided that will meet the needs of all types of citizen, regardless of gender, disadvantaged status, language and culture are not specifically addressed here. The one exception to this is that the question of illegal and harmful content is inextricably linked with the question of young people's access.

The direct implication of the discussion in the foregoing sections of Part Two, and much of what is contained in Part One is that:

1. the manager must accept responsibility for how public access to networks is provided;
2. national and international law and regulation provide structures within which to work, but they do not remove the need for management decisions;
3. filtering is not a substitute for informed and closely-involved management of facilities;
4. professional principles provide broad guidance as to how the manager should act, but they need interpretation if they are to be of use in specific cases;
5. a policy on Internet access is needed, so as to guide the manager and to indicate to users the parameters within which access is provided.

The need for a policy is listed last here, but it is the most important element in effective management of public access points. When a fully agreed and clearly stated policy exists, the manager can address specific problems in the confidence that there is a strong source of guidance for decision-making. To develop a policy on Internet access it is possible to turn for help in a number of directions. These include the law of the land, the aims and objectives of the parent institution, and professional codes of practice. It is also vital to begin with a thorough awareness of community standards, needs and preferences, of the kind that can be obtained from surveys specially undertaken as part of the process, and from sources already published or otherwise available.

The policy formulation exercise should not be done in isolation. There are rich resources of policy documentation available which will indicate what other institutions have chosen to include in their own policies (see Collections of Internet Policies at the end of this report). There is also a certain amount written about the process of creating a policy (Fishman and Pea, 1994; Campbell, 1998). Partnerships with parents groups, professional associations, non-governmental organisations concerned with education and child welfare, and other relevant bodies, are all an important element in creating widely-acceptable policy. A number of such organisations are mentioned in Part One, Section 6.3, and relevant Websites are included in the list at the end of this report.

The chief elements which policy formation needs to address are: the identification of the community to be served, its particular characteristics and needs, factors which influence its attitudes to information provision, and the way in which law and regulation impact on this. There needs to be clear understanding of where responsibility for content accessed is felt to lie: with content providers, information service providers, the users themselves, or with the managers of the public access point. The policy should address the extent to which the public access point will express its own responsibility through such measures as registering and training users, posting warning notices, creating warning screens, requiring users to sign statements of responsibility for their use of the system, the physical organisation of workstations in respect to privacy, the supervision of the public access area, or the use of filtering. Policy should also address matters like the actions to be taken in the case of misuse, and response to challenges directed at material accessed by users. Any institution which includes young people amongst its user body should ensure that relevant issues, such as the extent to which it operates *in loco parentis*, are fully addressed.

The policy can be seen as a public document in its own right, or it can be used to develop guidelines for public use. Since two different audiences are addressed (funders, colleagues, law enforcement bodies, pressure groups, etc. on the one hand, and users on the other) it is probably better to create two related documents. The internal document can provide context and supporting argument, but the one for public use will concentrate on short, clear statements that indicate what is offered by the public access point and what is expected of the user. A tabulation of the main elements of 72 Internet access policy documents issued for public use shows that certain types of statement are to be found in a majority, or substantial number, of them (Lake Oswego Public Library, 1996). These are not necessarily the most appropriate points to stress, but the tabulation at least gives an indication of tendencies in existing presentations of policy to the user.

Most commonly there are disclaimers and warnings: warnings of the possibility of finding objectionable or offensive material (57%); disclaimers of responsibility for the material users may find (79%); and statements of parental responsibility for what children may find (58%). A large number of documents contain general warnings of sanctions for misuse of the system (43%), or draw attention to specific forbidden behaviour, which includes infringement of intellectual property (32%), violation of system security (35%), and other kinds of illegal activities (35%). A range of other topics is mentioned, but less frequently than the above. They include time limits on use of workstations, the need to sign an acceptable use agreement, prohibition of user's own software, prohibition of harassment of other users, etc.

Despite the amount of work that has been done to develop policy by institutions which provide public access points, and the number of policy documents which have been issued for public use, there is still enormous scope for work on the policy area. Strong policies are crucial to the defence of freedom of expression and of the freedom of access to information from censorship controls or the cruder effects of filtering systems. Policies should take a positive approach to the provision of public network access, rather than merely seek to defend it against external pressures. Provision of public access needs to be based on a clear understanding of why it is offered. That understanding, expressed in a strongly argued document, is the best defence that can be adopted.

Policy formation is the area in which the Council of Europe can most usefully intervene, through the development of policy guidelines rooted in the principles which it exists to promote. Such policy guidelines will be of assistance to governments considering legislation or regulation of public Internet access. They will also assist those responsible for the management of public access points in the formulation of documents relating to their own specific circumstances.

Bibliography for Part One

ACLU (1997) Fahrenheit 451.2: Is cyberspace burning? www.aclu.org/issues/cyber/burning.html

ALA (1986) Intellectual Freedom Committee. *Books/materials challenge terminology*. Chicago: ALA.

Ang, P.H. and Nadarajan, B. (1996) Censorship and the Internet: a Singapore perspective. *Communications of the ACM* 39, 6. pp.72-78.

Arthur, C. (1997) Ratings plan for Internet sparks censorship fears. *Independent* (UK) Oct. 6th.

Atton, C. (1996) Anarchy on the Internet. *Anarchist Studies* 4. pp.115-132.

Barme, G. and Ye, S. (1997) The great firewall of China. *Wired* 5.06 www.wired.com/wired/5.06/china.html

Bennahum, D.S. (1997) The Internet revolution. *Wired* 5.04

http://www.wired.com/wired/5.04/internet.revolution.html

Borger, J. (1997) Hamas accused of using Internet as terror tool. *Guardian* (UK) Sept. 27th.

Branch, B. and Conable, G. (1997) To filter or not to filter. *American Libraries* Aug. pp.100-102.

Burt, D. (1997) In defense of filtering. *American Libraries* Aug. pp.46-48.

Capitanchik, D. and Whine, M. (1996) *The governance of cyberspace: racism on the Internet*. London: Institute for Jewish Policy Research.

Carol, A, (1996) A feminist argument against censorship. www.fiawol.demon.co.uk/FAC

Cavazos, E.A. and Morin, G. (1994) *Cyberspace and the law*. Cambridge, Mass: MIT Press.

Censorware Search Engine (1997) *Netly News*. www.pathfinder.com/time/index.html

Cormack, A. (1997) Web security. www.niss.ac.uk/education/jisc/acn/authent /cormack.html

Cyber-Rights (1997) and Cyber-Liberties (UK) Who watches the watchmen: Internet content rating systems and privatized censorship. www.leeds.ac.uk/law/pgs/yaman /watchmen.html

Dempsey, L. and Heery, R. (1998) Metadata: a current review of practice and issues. *Journal of Documentation* forthcoming.

Diamond, E. and Bates, S. (1995) Law and order comes to cyberspace. *MIT Technology Review* 98. Oct. pp.22-33.

Dority, B. (1997) Ratings and the V-chip. *The Humanist* May/June pp.16-19.

Elliott, C. (1995) Paedophiles on the Internet use codes to avoid detection. *Guardian* (UK) Nov. 21st.

Elmer-DeWitt, P. (1995) On a screen near you. Its popular, pervasive and surprisingly perverse. *Time International* July 3rd. p.38.

European Commission (1996). Illegal and harmful content on the Internet. www2.echo.lu/legal/en/Internet/content/communic.html

European Commission (1997) Action plan on promoting safe use of the Internet. www2,echo.lu/legal/en/internet/actpl-cp.html

Family Research Council (1997). Press release. June 26th. www.ciec.org/SC-appeal /970626-FRC.html

Faucette, J.E. (1995) The freedom of speech at risk in cyberspace. *Duke Law Journal* 44.

pp.1155-1182.

First Report (1997) on UK Encryption Policy. Cyber-Rights and Cyber-Liberties (UK). www.leeds.ac.uk/law/pgs/yaman/ukdtirep/htm

Great Sites (1997). www.ala.org/parentspage/greatsites/amazing.html

Hoffman, D.L. and Novak, T.P. (1995) A detailed critique of the Time article 'On a screen near you'. www.hotwired.com/special/pornscare/hoffman.html

Internet censorship (1997) and freedom of expression. www.surfwatch.com/surfwatch /censorship.html

Jeffreys, D. (1997) Do we want our schools linked to a world that obeys no law? *Daily Mail* (UK) Oct 6th.

Jellinek, D. (1997) Beyond the bamboo cybercurtain. *Guardian* (UK) Nov. 27th.

Kadie, C.M. (1994) Applying library intellectual freedom principles to public and academic computers. www.eff.org/CAF/cfp94.kadie.html

Katz, I. (1997) Internet escapes censor's web. *Guardian* (UK) Nov. 7th.

Kleiner, K. But who guards the guards? *New Scientist* Mar. 29th. p.50.

Kuner, C, (1996) Federal law to regulate the conditions for information and communication services.

http://ourworld.compuserve.com/homepages/cjuner/multimed1.htm

Langford, D. (1995) Law and disorder in Netville. *New Scientist* June 17th. pp.52-53

Lappin, T. (1996) Cyber rights now. *Wired* 4.05 www.wired.com/wired /4.05/cyber.rights.html

Lasica, J.D. (1997) Censorship devices on the Internet. *American Journalism Review* July 19th. p.56.

Lessig, L. (1997) Tyranny in the infrastructure: the CDA was bad, but PICS may be worse. *Wired* 5.07. www.wired.com/5.07/cyber-rights.html

Librarians' Guide (1997) to cyberspace for parents and kids. www.ala.org/parentspage /greatsites/safe.html

McMurdo, G. (1997) Cyberporn and communication decency. *Journal of Information Science* 23, 1. pp.81-90.

Makkula Center (1997) for Applied Ethics. Access, Internet and public libraries. www.scu.edu/ethics/practicing/library access/homepage/shtml

Marshall, J.M. (1997) Internet ratings bureaus: how many will there be? *Internet Legal Practice Newsletter* 2. www.collegehill.com/ilp-news/

Mason, M.G. (1997) Sex, kids and the public library. *American Libraries* June/July. pp.104-106.

New FBI Draft (1997) encryption legislation. www.cdt.org/crypto/fbi_draft_text.html

Newey, A. Networking for God*. Index on Censorship* 4. pp.132-137.

Parents (1996) and the Information Superhighway: an action sheet for getting involved. www.childrenspartnership.org/bbar/pbpg.html

Pedlars (1996) of child abuse: we know who they are. *Observer* (UK) Aug. 25th.

Perkins, M. (1997) Barriers to technical solutions. *IFLA Journal* 23. pp.23-29.

Policing the Internet: (1997) *Conference Report*. London: Association of London Government.

Recommender systems. (1997) Special section. ed. Resnick, P. and Varian, H.R. *Communications of the ACM* 40. Mar. pp.56-89.

Resnick, P. and Miller, J. (1996) PICS: Internet access controls without censorship. *Communications of the ACM* 39. Oct. pp.87-93.

Resnick, P. (1997) Filtering information on the Internet. *Scientific American* Mar. pp.54-56.

Right turn (1995) in cyberspace. *Economist* Aug. 26th. pp.77-78.

Robot as censor (1997). *IBM Networked World*. http://ibm.park.org/censor2.html

Rodriguez, F. (1997) Bad thing: Policing the Internet. www.teleport.com/room101 /badthing/police.html

Safeguards (1997) library alert. www.enough.org/safeguards_lib.htm

Shea, V. (1994) *Netiquette*. San Francisco: Albion Books.

Smith, G. (1996) *Internet law and regulation*. London: FT Law and Tax.

Sterling, B. (1992) *The hacker crackdown*. New York: Bantam.

Usdin, S. (1997) The great firewall of China. *Computer Life* 23. Mar. pp.44-47.

UK JET Report Controversy. (1997) Cyber-Rights and Cyber-Liberties (UK). www.leeds.ac.uk/law/pgs/yaman/htm

Vitiello, G. (1997) Freedom of expression online. *Focus* 28.

Wallace, J. and Mangan, M. (1996) *Sex, laws and cyberspace*. New York: Henry Holt and Co.

Wallich, P. (1997) Parental discretion advised. *Scientific American* Aug. p.21.

Watson, D. (1997) Internet censorship: demands for content controls. *Library Association Record* 99, 12. p.638.

Winner, L. Electronically implanted values. *MIT Technology Review* 100. p.69.

Wolf, C.J. (1994) Developing a school or district 'Acceptable Use Policy' for student and staff access to the Internet. www2.msstate.edu/~fyh1/aup.html

Bibliography for Part Two

Annual Internet Survey (1998). *Which? Online*. www.which.net/nonsub/special /ispsurvey/foreword.html

Berry, J.N. (1998) Practising free expression. *Library Journal* 123, 7. p.6.

Blamire, R. (1998) The information rich and the information poor: avoiding a new divide in Britain. In: Carr, J. and Mullins, A. (eds.) *Children on the Internet: opportunities and hazards*. London: NCH Action for Children. pp.7-11.

Branch, B. and Conable, G. (1997) To filter or not to filter. *American Libraries* 28, 8. pp.100-102.

Burt, D. (1997) In defense of filtering. *American Libraries* 28, 8. pp.46-48.

Campbell, S. (1998) Guidelines for writing children's Internet policies. *American Libraries* 29, 1. pp.91-92.

Censorship ruling (1998). *Library Association Record* 100, 5. p.238.

Child porn (1998) verdict stuns Net lawyers. *Guardian* (UK) 29th May.

Children's attitudes (1998) *towards teachers and school environment: a research study among 11-16 year olds*. London: Association of Teachers and Lecturers.

Coping with challenges (1996). Chicago: American Library Association.

Council of Europe (1998) *Draft recommendation No. R (97) on a European policy on access to archives*. Strasbourg: Council of Europe.

Cyber Patrol (1998) in Austin Public Library. www.realtime.net/~bladex/apl/apl.htm

Federal Republic of Germany (1997). *Information and Communication Services Act*. Bonn: Federal Parliament. www.iid.de/rahmen/iukdgebt.html

Doyle, R.P. (1997) *Books challenged or banned 1997*. Chicago: American Library Association.

European Commission (1998). Recommendation on the Protection of Minors and Human Dignity in the Audiovisual and Information Services. http://europa.eu.int/en/comm /dg10/avpolicy/new_srv/comlv-en.htm

Fishman, B.J. and Pea, R.D. (1994) The Internetworked school: a policy for the future. *Technos: Quarterly for Education and Technology* 3, 1. pp.22-26.

Flagg, G. (1998) Senate Committee approves Filtering Bill. *American Libraries* 29, 4. p.13.

Foskett, D.J. (1962) *The creed of a librarian*. London: Library Association.

Harris, M. (1976) Portrait in paradox: commitment and ambivalence. *Libri* 26, 4. pp.281-301.

Hauptman, R. (1976) Professionalism or culpability? An experiment in ethics. *Wilson Library Bulletin* 50, 8. pp.626-627.

Hill, M. (1997) Facing up to dilemmas: conflicting ethics and the modern information professional. *FID News Bulletin* 47, 4. pp.107-117.

Internet censorship (1997) and freedom of expression. www.surfwatch.com/surfwatch /censorship.html

Internet Watch Foundation (1998a) *First annual report December 1996-November 1997*. www.iwf.org.uk/about/annual97.htm

Internet Watch Foundation (1998b) *Rating and filtering Internet content: a United Kingdom perspective*. www.iwf.org.uk/label/index.htm

Lake Oswego Public Library (1996) *Internet policies: tables*. www.ci.oswego.or.us/library/politab.htm

Lamont Johnson, D. (1996) Finding the middle ground in the debate of Internet censorship in the public schools. *Computers in Schools* 12, pp.1-5.

Lasica, J.D. (1997) Censorship devices on the Internet. *American Journalism Review* 19th July. p.56.

Library Bill (1996) *of Rights*. www.ala.org

Miller, J. (1994) *The street of the pied piper*. Derby: Professional Association of Teachers.

Ministerial Conference (1997) on Global Information Networks. 6-7 July 1997. *The Bonn Declaration*.

Nation divided (1997) into IT haves and have-nots. *Guardian* (UK) 22nd October.

New Library: (1997) *the people's network*. London: Library and Information Commission.

Oder, N. (1998) Intellectual freedom legislation: the state of the States. *Library Journal* 123, 6. pp.54-57.

Professional Association of Teachers (1988) *Code of professional conduct*. Derby: Professional Association of Teachers.

Questions and answers (1997) *Access to electronic information, services and networks: an interpretation of the Library Bill of Rights*. Chicago: American Library Association.

St. Lifer, E. (1998) McCain Filtering Bill draws support despite misperceptions. *Library Journal* 123, 5. p.14.

St. Lifer, E. and Rogers, M. (1998a) Despite Federal filtering fight, PLs are handling it locally. *Library Journal* 123, 4. pp.12-13.

St. Lifer, E. and Rogers, M. (1998b) Judge: Loudoun challenge to filtering policy can proceed. *Library Journal* 123, 8. p.12.

Schuyler, M. (1997) When does filtering turn into censorship? *Computers in Libraries* 17, 5. pp.34-38.

Schneider, K.G. (1997) *A practical guide to Internet filters*. New York: Neal-Schuman.

Swan, J.C. (1982) Ethics at the reference desk: comfortable theories and tricky practices. *Reference Librarian* 4. pp.99-116.

Thorhauge, J. et al. (1997) *Public libraries and the information society*. Luxembourg:

European Commission DGXIII.

Selected Web sites

Acceptable Use Policies of Selected Internet Service Providers: www.jmls.edu/cyber/statutes

Very full list of the policies of the main ISPs.

American Civil Liberties Union: www.aclu.org

Led campaign against CDA. Site has documents.

American Library Association: http://www.ala.org

The best site for documents on library-related aspects.

America Online (AOL): http://www.aol.com/nethelp/news/newsnetiquette.html

Sets out AOL's policy on acceptable use.

Bluehighways: http://www.bluehighways.com

Has The Internet Filter Assessment Project (TIFAP) and other documents.

Campaign for Internet Freedom (UK): http://www.netfreedom.org

The site that was closed down for carrying 'dangerous' material.

Censorship and Intellectual Freedom Page: http://php.indiana.edu/~quinnjf/censor.html

Provides links to many other relevant sites and Usenet groups.

Censorware Search Engine: http://cgi.pathfinder.com

Reports on filtering products, but some doubts about reliability.

Center for Democracy and Technology: http://www.cdt.org

Advocates public policies advancing civil liberties in the networked environment.

Child Safety on the Information Highway: http://www.4j.lane.edu/InternetResources

/Safety/Safety.html

The National Center for Missing and Exploited Children's brochure, on the site of Eugene, Oregon, School District.

Citizens Internet Empowerment Coalition: http://www.ciec.org

Organization formed to campaign against the CDA.

Computer & Information Ethics Resources on WWW: http://www.ethics.ubc.ca/papers/computer.html

Canadian site with many links.

Computer Professionals for Social Responsibility: http://cpsr.org/dox/cpsr/about-cpsr.html

Presents the computer professional's approach.

Computers and Academic Freedom; http://www.eff.org/CAF

Has extensive archive relating to the academic community and the Internet.

CyberPatrol: http://www,microsys.com

Site for a leading filtering product.

Cyber-Rights & Cyber-Liberties (UK): http://www.leeds.ac.uk/law/pgs/yaman/yaman.html

Many links and documents, and a regular Cyber-Rights & Cyber-Liberties Newsletter.

CyberSpace Law Center: http://www.cybersquirrel.com/clc/expression.html

Has many links to other sites and documents on this and other law-related topics.

Electronic Frontier Foundation: http://www.eff.org

Many links and extensive archives on the site of the major libertarian campaigning body.

Electronic Privacy Information Center: http://epic.org

Site has many basic legislative documents.

Electronic Rights and Ethics: http://www.zip.com.au/~pete/ere.html

Developing an ethical standard for the Internet.

Enough is Enough: http://www.enough.org

Has materials for campaign to promote filtering in libraries.

Ethical Spectacle: http://www.spectacle.org

Online magazine covering ethical issues generally, and Internet censorship particularly.

Families Against Internet Censorship: http://shell.rmi.net/~fagin/faic

Accepts filtering as part of an anti-censorship programme.

Family Friendly Libraries http://www.fflibraries.org

Opposes social involvement of ALA (particularly on gay issues).

Filtering and Censorware in Libraries: http://www.geocities.com/Athens/Delphi/7382

Anti filtering site.

Filtering: http://www.filteringfacts.org

Site supporting filtering in libraries. Has links to other similar sites, articles and details of filtering products.

First Amendment Cyber-Tribune: http://w3.trib.com/FACT

Monitors freedom of expression issues worldwide.

Global Internet Liberties Campaign: http://www.gilc.org

International campaigning organization for human rights on the Internet.

Internet Content Register: http://www.internet.org.uk/icop.html

Promoters of the Internet Code of Practice (ICOP).

Internet Content Coalition: http://www.netcontent.org

Represents major media companies providing Internet content.

Internet Watch Foundation: http://www.iwf.org.uk

UK industry self-regulatory body.

Library Watch: [http://netwinds.com/library]

An online magazine opposing the ALA stand on censorship.

Markkula Center for Applied Ethics: http://www.scu.edu/ethics

Has the report on Access, Internet, and Public Libraries.

MIT SAFE: http://www.mit.edu/activities/safe

MIT student organization against censorship which links to sample newsgroups.

National Campaign to Combat Internet Pornography: http://www.nccip.org

Mostly about pornography, but discusses attitude to the Internet.

Netparents: http://www.netparents.org

Much information on filtering and rating.

Peacefire: http://www.peacefire.org

Student group's site, with links and documents.

People Against Pornography: http://earth.vol.com/~shark//pap.html

Christian site, mainly concerned with pornography as such.

PICS: http://www.w3.org/PICS

The official site describing and promoting PICS.

Pippin Central: http://www.pippin.com/English/InternetCenter/children.htm

Offers guidance on safe Internet use for children.

Recreational Software Advisory Council: http://www.rsac.org

Responsible for RSACi rating system.

Robbinsdale, Minnesota, School District: http://www.eta.K12.mn.us/~WMrdale /281.html

Very full list of school acceptable use policies, plus related documentation.

SurfWatch: www.surfwatch.com

(*Editorial note: January 2001: SurfWatch has recently been acquired by SurfControl and they have merged their Web sites: www.surfcontrol.com)*

Promotes the product as a means to fight Internet censorship.

VF-INFOethics: http://www.de3.emb.net/infoethics/start.html

Site based at the University of Constance, Germany, with links to many other sites.

WEBHITZ: http://www.infostar.com/

Links to sites related to parental control of Internet use.

Wired: http://www.wired.com

Journal with many relevant articles.

Collections of Internet Policies

Public Library Internet Access Policies: http://www.ci.oswego.or.us/library/poli.htm

Lake Oswego Public Library collection of policies from 126 libraries.

Rice University Collection of K-12 Policies

Contains policies and documents relating to creating policies.

Robinsdale, Minnesota, School District: http://www.eta.K12.mn.us/~WMrdale/281.html

Very full list of school acceptable use policies, plus related documentation.

Technology and WWW Policies: http://www.cc.colorado.edu/Library/Current/wwwpol.html

Collection of academic policies and links to other collections.

World-Wide Web Guidelines: http://cspmserver.gold.ac.uk/guidance.html

Mainly British academic policies.

Latest Revision: November 10, 2004