COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 16.10.1996
COM(96) 487 final

COMMUNICATION FROM THE COMMISSION

TO THE COUNCIL, THE EUROPEAN PARLIAMENT,
THE ECONOMIC AND SOCIAL COMMITTEE
AND THE COMMITTEE OF THE REGIONS

Illegal and harmful content on the Internet

TABLE OF CONTENTS

INTRODUCTION

The symbol of the convergence between telecommunications, computer and content industries, and one of its main drivers, the Internet has established itself as one of the ***main building blocks of the Global Information Infrastructure*** and as an ***essential enabler of the Information Society in Europe.*** Characterised by a growth rate unprecedented in the history of communication technologies, the Internet now reaches some 60 million users in 160 countries, doubling each year. Its most popular application, the World-Wide-Web, based on protocols developed in Europe, is fast becoming a standard vehicle for information publication and electronic commerce, with an estimated 10 million sites world-wide in 1995, up 1600% over the previous year. Driven by its meteoric growth, and its rapid evolution from a government/academic network to a broad-based communication and trading platform, the Internet is currently revolutionising a number of ***economic sectors***, with the emergence of a ***vibrant and fast-growing "Internet Economy".*** Simultaneously, the Internet has also become a ***powerful influence in the social, educational and cultural fields*** – empowering citizens and educators, lowering the barriers to the creation and distribution of content, offering universal access to ever richer sources of digital information.

Reflecting these opportunities, the vast majority of Internet content is for purposes of information for totally legitimate (and often highly productive) business or private usage. However, like any other communication technologies, particularly in the initial stages of their development, the Internet carries an amount of potentially harmful or illegal contents or can be misused as a vehicle for criminal activities. Although statistically a limited phenomenon, a wide range of distinct areas are concerned. These are covered by different legal regimes and instruments at the national and international level, e.g.:

- *national security* (instructions on bomb-making, illegal drug production, terrorist activities);
- *protection of minors* (abusive forms of marketing, violence, pornography);
- *protection of human dignity* (incitement to racial hatred or racial discrimination);
- *economic security* (fraud, instructions on pirating credit cards);
- *information security* (malicious hacking);
- *protection of privacy* (unauthorised communication of personal data, electronic harassment);
- *protection of reputation* (libel, unlawful comparative advertising);
- *intellectual property* (unauthorised distribution of copyrighted works, e.g. software or music)

While the benefits of the Internet far outweigh its negative aspects, these aspects cannot be ignored. They are pressing issues of public, political, commercial and legal interest. Reflecting these concerns, recent political discussions in the European Union have stressed the need for urgent action and concrete solutions.

Therefore, most recently, on 27 September 1996 the Telecommunications Council adopted a resolution on preventing the dissemination of illegal content on the Internet, in particular child pornography. The Council took note that the Commission would publish a Communication on this issue, and welcomed that initiative. Stressing the need for rapid response, the Council urged the Commission to carry its ongoing work and to present practical measures in time for the next Telecommunications Council on 28 November 1996.

The Commission is fully aware of the importance of these issues, and of the need to strike the ***right balance between ensuring the free flow of information and guaranteeing protection of the public interest*** so as to meet justified concerns.

Already, at the informal Council meeting held in Bologna on 24 April 1996, European Telecommunications and Culture ministers had identified the issue of illegal and harmful content on the Internet as an urgent priority. It was considered that, while existing national laws apply to the Internet, agreement should be reached in a wider context to address the specific challenges raised by this "network of networks". The Commission was therefore requested to produce a summary of problems posed by the rapid development of Internet, and to assess, in particular, the desirability of European or international regulation.

As regards the distribution of ***illegal content*** on the Internet, it is clearly the ***responsibility of Member States to ensure the application of existing laws. What is illegal offline remains illegal online***, and it is up to Member States to enforce these laws. Nevertheless, given the highly decentralised and transnational nature of the Internet, concrete measures to reinforce co-operation between Member States should be launched in the context of Justice and Home Affairs.

At another level, the presence of illegal and harmful content on the Internet has ***direct repercussions on the workings of the Internal Market.*** In particular, the adoption by Member States of regulations of new Internet services intended to protect the public interest may also create risks of distortions of competition (for example, through widely divergent responses to the question of potential liability of Internet service providers), hamper the free circulation of these services, and lead to a re-fragmentation of the Internal Market. If unsolved, such problems may justify Community intervention. Like in any new and fast-growing industry, legal and regulatory certainty is the *conditio sine qua*

non to foster investments, guarantee the development of a competitive Internet services sector, and ensure the growth of a wider Internet-based economy in Europe.

It is widely recognised that the international nature of the Internet and its unique characteristics (extremely decentralised structure, resistance to tampering, high degree of automation, global reach, wide usage) clearly pose novel, and specific, problems. These problems need innovative, and specific, solutions which should be put in place rapidly, anda co-ordinated response at EU and international level.

Complementary to the present initiative, issues of protection of minors *stricto sensu* - themselves a subset of wider issues of illegal and harmful content - will be addressed in the *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services.* That Green Paper takes a horizontal approach, and will initiate a long term reflection on this issue across all electronic media.

This Communication assesses the opportunities offered by the Internet, identifies different variations of illegal and harmful content, describes the technical environment of the Internet and gives policy options for immediate action on a technology and/or legal base to fight against such content on the Internet.

1. THE OPPORTUNITIES OF THE INTERNET

The potential of the Internet to inform, educate, entertain and conduct business on a global scale is considerable. At a relatively modest cost, vast quantities of information can be sent around the world in new multi-media communications. A number of countries in the world, and in particular in the European Union, have already seized on these radical new opportunities.

In ***social terms***, the Internet represents significant potential benefits. It offers unprecedented opportunities for empowering citizens, and for connecting them to ever richer sources of digital information. The Internet has been used by great effect in a number of Member States to connect administrations and citizens. Lowering the barriers of entry to the dissemination of information on the local, as well as on the global scale, the Internet allows individuals or associations to publish information about their activities to a wide audience at modest cost. In the ***field of culture***, the Internet already contributes significantly to the creation and dissemination of European digital multimedia content, fostering linguistic diversity, and the *rayonnement* of European cultures in the world. As exemplified by a number of innovative projects linking ***libraries, schools and universities*** in Europe, the Internet is similarly the key to a ***new "electronic literacy"***, and, as such, the cornerstone of the new and far-reaching European Union initiative, the Action Plan ***"Learning in the Information Society"***.

Currently revolutionising ***electronic commerce***, the "network of networks" is likely to play a ***crucial role for the European economy***. This is directly linked to the liberalisation of Europe's telecommunications market, which should translate into lower operating costs for Internet users and service providers[1]. As the US market already demonstrates, the Internet is ***directly fostering a new and fast-growing Internet economy***[2], creating new categories of businesses and new jobs (Internet infrastructure and software, Internet access providers, consumer and business content distribution, online retail and financial services). Beyond this "core Internet economy" of businesses which create revenues directly from the Internet, the Internet is having an ***indirect impact on a much wider "Internet sphere of influence"***. The Internet is thus radically transforming a number of existing economic sectors (travel services, insurance, direct retailing, electronic publishing), creating new markets, reducing costs and improving customer service. It is, in particular, generating ***new opportunities for European SMEs***, a growing number of which are now eagerly capitalising on unprecedented access to global markets offered by the World Wide Web. Similarly, large economic sectors, such as the direct marketing industry in Europe (which represented a total income of ECU 37 billion in 1994[3]), and in particular the traditional catalogue business, are actively integrating the Internet in their marketing and fulfilment strategies, and planning gradually to migrate a substantial part of their activities to the Internet.

In the field of ***advertising and marketing***, the Internet presents a number of significant and well documented advantages. Because of its interactive nature, and the immediacy and ease of communication, advertising messages can be targeted at audiences much more precisely than has been possible until now, and feedback obtained from current or potential customers. Similarly, when used for executing transactions or even delivering content on line, the Internet offers considerable cost savings for both businesses and customers.

---

1 One of the key factors in the development of the Internet market in the US has been the lower cost of telecommunications (lower costs of leased lines for professional users; of local calls for individual customers).

2 An estimate by Forrester Research concludes that the Internet "core economy" will generate in the US alone some $2.2 billion in 1996. By the year 2000, some $45.5 billion will be directly attributable to Internet activity - a twenty-fold increase in five years. According to Forrester Research, the Internet's most intense economic activity will center on Internet infrastructure ($ 14.2 billion), consumer content ($2.8 billion, including Internet advertising and rights purchases), business content ($ 6..9 billion, including business intelligence now supplied on proprietary networks), online trade ($ 21.9 billion, including $ 6.9 billion from new electronic retail activities and $ 15 billion from the migration of traditional EDI systems), and financial services (management through the Internet of an estimated $ 46.2 billion in assets and savings)

3 Source: *Study on the Extent of Direct Marketing in the European Union*, interim report by FEDIM for the European Commission.

Enlarging the scope of ***electronic commerce*** to the general public on global markets, the Internet is, at the same time, bringing radical changes in business-to-business transactions, as companies migrate from proprietary networks and closed protocols (such as traditional EDI) to the Internet and to corporate "Intranets". This ***business-to-business sector is currently the fastest growth area*** in the global Internet economy. It is a sector of crucial strategic importance for European companies competing on world-wide markets.

As any other sector of activities, the Internet may be used for legitimate purposes or misused by some elements of the society. The framework for the Internet should, therefore, ***foster economic development***, while taking account of ***justified social and societal concerns***. Consumers and businesses must be reassured that the Internet is a safe and secure place to work, learn and play.

This Communication, therefore, aims

- ***firstly to describe briefly the different types of illegal and harmful content,***
- ***secondly to examine the technical context in which action can be taken to deal with illegal and harmful content, and***
- ***finally to suggest a number of practical measures designed to be rapidly implemented***

In the following sections, *section 2* describes the different Internet applications, *section 3* defines what is meant by "illegal and harmful content", *section 4* deals with ways in which to combat illegal content, *section 5* explains issues related to harmful content and *section 6* presents a number of proposals.

2. HOW DOES THE INTERNET WORK?

The Internet is the most visible example of an international computer network. Although it is neither the first nor the only such network, it is distinguished by the fact that nobody "owns" it and by the fact that over the past few years "ordinary" users, private individuals and businesses, and not just the scientific or academic community, have started to use it widely, causing a dramatic increase in the number of computers linked to the Internet[4].

The increase in the numbers of servers providing Web content and in the number of users connected to the network is startling. In Europe alone, the number of servers increased by 60% over the period January 1995 - January 1996. See also statistics referred to in IPSO newsletter July issue (http://www.ispo.cec.be/ispo/newsletter/ISPOJULY/ISPOJULY04.html - 5 million new servers in the last 12 months).

Unlike other traditional networks such as broadcasting, the Internet is essentially user-driven, with users themselves, rather than established publishers, generating a substantial part of the "content".

A unique characteristic of the Internet is that it ***functions simultaneously as a medium for publishing and for communication***. Unlike in the case of traditional media, the Internet supports a variety of communication modes: one-to-one, one-to-many, many-to-many. An Internet user may "speak" or "listen" interchangeably. At any given time, a receiver can and does become content provider, of his own accord, or through "re-posting" of content by a third party. The Internet therefore is ***radically different from traditional broadcasting***. It also ***differs radically from a traditional telecommunication service***. This constant shift from "publishing mode" to "private communication mode" – two modes governed traditionally by very different legal regimes – constitutes one of the main challenges of Internet regulation.

The many different ways of distributing Internet content reflect the structural and historical idiosyncrasies of this network. The extent to which technical measures can be used to detect, track down or intercept illegal and harmful content also significantly differs from application to application.

Most individual users will not have permanent direct access to the Internet. They will go through an access provider. This includes:

- ***Internet access providers***, specialised in offering access to the Internet ;
- ***Internet service providers***, who offer additional services such as hosting content produced by themselves, or by users or by third parties (those who produce content are referred to here as content providers);
- ***On-line service providers***, who provide proprietary content[5] for subscribers on their closed systems, and now also offer them Internet access.

The term "Internet service provider" is often used generically, without a clear distinction being made between the *service of providing access to the Internet* and the *service of hosting content*. The terms "access provider" and "host service provider" will be used here to differentiate. The same organisation can of course fall within both categories.

---

[5] Such "proprietary content" may be produced by the online service provider itself, or produced contractually for that provider by a third party (entertainment company, financial services institution, airline, etc.). The online service operator generally assumes editorial responsibility for such content, like a traditional publisher.

Both ***"access provider"*** and ***"host service provider"*** will connect to the Internet via a leased line, a telecommunications connection made available by the ***"network operator"***, such as British Telecom.

The ***World Wide Web*** (WWW or Web) is the area where pages with text, graphics and even sound and video clips may be viewed. Pages are linked to each other by a series of "hyper-links" offering a congenial and highly interactive way of navigating through Web content. These pages may be published by anyone who has access to storage space on a "host" computer connected to the Internet running the appropriate software (a "Web server" or "site"). This possibility to become a "content publisher" is often given at low cost as an additional service by Internet access providers, and individuals in this way have the same potential to distribute information as large corporations. The pages published in this way are available to any Internet user who chooses to consult them, and are identifiable by an address which is used in order to consult them directly, or to reach the page through hyperlinks.

Electronic mail allows communication between individuals. It is also easy to send out the same message to multiple addresses using mailing lists. Although in general the author of the correspondence will be identified by his e-mail address, "anonymous remailer" systems have been set up where the sender's identity is not passed to the recipient. Messages sent to an Internet address are stored in the recipient's mailbox on the mail server maintained by the access provider until the recipient reads them.

In some 15,000 ***newsgroups***, the content is provided by individuals who send messages (which may be simple text, but can include graphics encoded so that they can be transferred). These messages are not stored in a single place, but copied from one newsgroup server to another. Because of the enormous storage requirements, host service providers will often only keep such messages on their newsgroup servers for a limited period and may well not carry all newsgroups. There are also sites on the World Wide Web where archives of newsgroup contents are stored and can be searched.

Additionally, ***Internet Relay Chat*** (IRC) allows direct communication in real time between Internet subscribers, and may be used to organise face to face meetings and the exchange of content. IRC can now support low resolution video technologies such as CUSeeMe.

All of these means can be used to distribute illegal and harmful content, and the extent to which they can be controlled will be pointed out in the following sections.

3. ILLEGAL AND HARMFUL CONTENT ON INTERNET

The Internet is a new form of distribution and communication. Like any other communication technologies, particularly in the initial stages of their development, the Internet carries an amount of potentially harmful or illegal contents or is misused as a vehicle for criminal activities. Like any other communication technology, such as the telephone or GSM, the Internet can be used by criminals to facilitate their activities.

All these activities fall under the existing legal framework. Therefore, the Internet does not exist in a legal vacuum, since all those involved (authors, content providers, host service providers who actually store the documents and make them available, network operators, access providers and end users) are subject to the respective laws of the Member States.

In terms of illegal and harmful content, it is crucial to differentiate between content which is illegal and other harmful content. ***These different categories of content pose radically different issues of principle, and call for very different legal and technological responses.*** It would be dangerous to amalgamate ***separate issues such as children accessing pornographic content for adults, and adults accessing pornography about children***. Priorities should clearly be set and resources mobilised to tackle the most important issues, that is the fight against criminal content - such as clamping down on child pornography, or use of the Internet as an new technology for criminals.

a. Illegal Content

There exists a whole range of rules which limit for different reasons the use and distribution of a certain content. The infringement of these rules lead to the illegality of the content.

Certain issues do not involve protection of public order, but rather the protection of the rights of individuals (protection of privacy and reputation) and of an environment allowing creation of content to flourish (intellectual property). Content such as breach of copyright, libel, invasion of privacy or unlawful comparative advertising will usually be dealt with at the initiative of the person whose rights are infringed by a civil action for damages or an injunction, although there may also be remedies under the criminal law or administrative law (data protection). Host service providers may also be drawn into disputes over such content, because they may be accused of having facilitated its distribution.

Certain content is - in addition - ***considered as criminal*** by the laws of Member States.

This is the case for example with child pornography, trafficking in human beings, dissemination of racist material or incitement to racial hatred, terrorism or all forms of fraud (e.g. credit-card fraud).

The exact definition of offences varies from country to country. Within the EU, even child pornography, for example, where a high degree of consensus exists, is covered by specific legislation in some Member States and by more general rules relating to obscenity in others.[6]

Where certain acts are punishable under the criminal law of one Member State, but not in another[7], practical difficulties of enforcing the law may arise.

b. Harmful content

Various types of material may offend the values and feelings of other persons: content expressing political opinions, religious beliefs or views on racial matters etc.

What is considered to be harmful depends on cultural differences. Each country may reach its own conclusion in defining the borderline between what is permissible and not permissible. It is therefore indispensable that international initiatives take into account different ethical standards in different countries in order to explore appropriate rules to protect people against offensive material whilst ensuring freedom of expression.

In this context it is understood that the fundamental rights, especially the right of freedom of expression have to be fully respected (limitations in the Member States see Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, Annexe III)

4. IDENTIFYING AND COMBATING ILLEGAL CONTENT ON INTERNET

It is a matter for Member States to define what is illegal by law and to enforce it by detecting illegal activity and punishing offenders. However the special characteristics of the Internet mean that law-enforcement is more complicated than where more traditional means are used.

---

[6] See Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services

[7] For example publication of *Mein Kampf* by Adolf Hitler or "revisionism" i.e. denying the reality of the Holocaust. These are forbidden in some Member States, e.g. Germany, but not in others.

While detecting breaches of the law in public applications of Internet (World Wide Web) is straightforward, detection is not easy in private applications (e-mail, for instance). Similarly, while enforcement of the law is relatively easy within national boundaries, it is much more difficult in an international context.

a. Technical limits to law-enforcement

The technical features of the Internet make certain types of control ineffective. Because of the way in which Internet messages can be re-routed, control can really only occur at the entry and exit points to the Network (the server through which the user gains access or on the terminal used to read or download the information and the server on which the document is published).

Even if a published document is removed from one server as a result of intervention by the authorities, it can easily and quickly be copied to other servers in other jurisdictions, so that it continues to be available unless and until such sites are also blocked. Thus ***additional international co-operation is required to avoid "safe havens" for documents contrary to general rules of criminal law.***

b. The role of Internet access providers and host service providers

Internet access providers and host service providers play a key role in giving users access to Internet content. It should not however be forgotten that the prime responsibility for content lies with authors and content providers. It is therefore essential to identify accurately the chain of responsibilities in order to place the liability for illegal content on those who create it.

i) Legal responsibilities of Internet access providers and host service providers

The general regime for legal responsibility, which could also be applicable to Internet access providers and host service providers for illegal content (of whatever form, be it child pornography, copyright infringements, fraudulent offers, libel etc.) takes, according to the circumstances a number of different forms: under the criminal law, under civil law (an action for damages for breach of copyright or libel, or a dispute arising under their contracts with users or with network operators) or under administrative law (the system of regulation in place in the country where the access providers and host service providers operate). Although ***access providers*** do not directly control the content available on the Internet, or what part of it their customers choose to consult, in some cases they have been investigated by the authorities because of the existence of illegal and harmful content which users can access through the providers' technical facilities. 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, to steer a path between accusations of censorship and exposure to liability.

Where ***host service providers*** themselves provide content on the World Wide Web or on newsgroups, they are of course liable for this in the same way as any author or content provider. Where the content is provided by third parties, host service providers' liability needs to be clear.

In a number of Member States[8], legislation has been adopted or proposed defining the legal responsibilities of host service providers in such a way that they are only liable for an item of content hosted on their server where they can reasonably be expected to be aware that it is *prima facie* illegal or fail to take reasonable measures to remove such content once the content in question has been clearly drawn to their attention.

Some rules go further and appear to require access providers to restrict access to other sites which contain illegal content.

Network operators, on the other hand, are not normally exposed to liability in criminal or civil law for the content carried over their networks, although they may be required by the terms of the relevant legislation or licenses to take steps in relation to their customers (access providers) if the latter use facilities to carry illegal content.

The degree of liability for content such as unlawful comparative advertising and breach of copyright must also be considered in the light of the detailed examination by the Commission of the effects on the internal market of the different national rules relating in particular to commercial communications and copyright [9].

ii) Self-regulation on a national, European and international level

In a number of Member States, Internet access providers and host service providers have already set up systems of self-regulation. In the United Kingdom, ***at the initiative of the Industry***, a Code of Conduct has been agreed. An independent body, the Safety Net Foundation has been set up to provide a rating service for newsgroups and a hot-line to which members of the public can report content they consider illegal. Similar steps have been taken in Germany and in the Netherlands[10].

---

[8] Austria, Germany, France, UK.(Defamation Bill).

[9] Proposal for a directive on commercial communications, draft communication on the Follow-up to the Green Paper on Copyright and Related Rights in the Information Society.

[10] In France, a Code of Conduct has similarly been proposed in the *Rapport de la Mission Interministérielle sur l'Internet.* Text avaliable at http://www.telecom.gouv.fr/english/sommaire.htm

The Commission welcomes this general move towards self-regulation and has encouraged the setting-up of a European network of associations of Internet Access Providers. This co-operation could further be extended to the wider international level. Facing common problems, industry self regulating bodies could usefully co-ordinate their approach, in particular regarding technical solutions. Similarly, in the highly decentralised Internet environment, ***Internet Users have a very important role to play*** in contributing to industry self-regulation.

iii) Removal of files from the servers

Once a host service provider becomes aware of the *prima facie* illegality of content hosted on his server, in principle the legislation in the Member States foresee that he must clearly take steps to remove the content in question. This information might be received from the national self-regulatory body set up to identify illegal content or from an equivalent body in another country. Since content can easily be copied to other servers, this approach needs to be followed by other host service providers not just in the country involved, but world-wide. An international network of self-regulatory bodies would greatly assist this process, although it will no doubt take time for such a network to be put into place .

iv) Blocking access at the level of access providers

If the illegal content cannot be removed from the host server, for instance because the server is situated in a country where the authorities are not willing to co-operate, or because the content is not illegal in that country, an alternative might be to block access at the level of access providers.

It is as yet unclear how far it is technically possible to block access to content once it is identified as illegal. This is a problem which also affects the degree of liability of the access providers. The lack of clarity on the technical feasibility has not prevented this approach being implemented in certain countries because access providers are a relatively small and identifiable group.

Some third countries have introduced wide-ranging legislation to block all direct access to Internet via access providers by introducing a requirement for "proxy servers" similar to those used by large organisations for security reasons, ***combined with centralised blacklisting*** of documents, for reasons which go far beyond the limited category of illegal content as defined in this communication. ***Such a restrictive regime is inconceivable for***

Europe as it would severely interfere with the freedom of the individual and its political traditions. Due to Europe's complex and open communication infrastructure the practical feasibility of such an approach also remains open to question.

A second approach which involves requiring access providers to block their subscribers' access to illegal content on a case-by-case basis has been followed recently by law enforcement authorities in Germany.

In the CompuServe case the public prosecutors considered that certain items available on newsgroups were illegal, and requested CompuServe[11] to block access to these newsgroups. Since CompuServe's software did not initially make it possible to differentiate between German subscribers and others for access to newsgroups, CompuServe suspended access to a number of newsgroups to all its subscribers world-wide, which created wide-spread protests that German standards of morality were being exported. Subsequently, CompuServe restored access to most of these newsgroups except to its German subscribers. No action was apparently taken against other access providers based in Germany, so their subscribers could continue to consult this content, if the access provider chose to carry the newsgroup in question.

In a recent case, the German public prosecutors threatened to prosecute the German Internet access providers unless they blocked access to a magazine published on a Web site on a server in the Netherlands which allegedly promoted terrorist violence. Under protest, the access providers did so. However, this meant blocking access to all content on the Dutch server, including harmless content, while the document continues to be available to Internet users outside Germany. A number of anti-blocking tactics were also immediately put in place.[12] It is not clear whether the content is contrary to Dutch law - at all events the Dutch authorities have not intervened. The Dutch host service provider has complained that the action of the German authorities constitutes an interference with the free movement of services within the EU.

Upstream blocking of sites may therefore present a number of significant shortcomings. It may not prevent, in particular, criminal users from "hopping" from one Internet mode to the other, i.e. from a Web page, to a Usenet newsgroup, to standard e-mail.

---

[11] A large US-based international commercial online service provider which also provides Internet access, and has a substantial number of subscribers in Germany

[12] At the latest count, the document is mirrored on 43 WWW sites and 2 newsgroups and is available from an e-mail listserver.

This demonstrates that there is a ***need for co-operation between the authorities and Internet access providers in order to ensure that measures are effective and do not exceed what is required.***

c. Anonymous use of Internet

Users of the Internet are normally identified, by stating the author of a World Wide Web home page or by the identifying address of the page ("URL") or in the mention of an e-mail address for electronic mail or a newsgroup message. This is desirable in accordance with the democratic principle that individuals, while free to express their thoughts and beliefs, should nevertheless be accountable for their actions.[13] The principle of legal traceability should, therefore, be incorporated into national or European Codes of Conduct for remailing activities.

Law enforcement authorities have expressed concern at various techniques which allow anonymous use of the Internet. This may facilitate sending illegal content by making it difficult or impossible to identify the offender.

This problem does not concern the World-Wide Web, where a host service provider knows, or at least has the means of knowing, the content provider. However anonymity allows users to send electronic mail or a message to a Usenet newsgroup without the recipient knowing their name or their e-mail address, because an intermediary (the anonymous remailer) has removed this information

There are legitimate reasons why a user might wish to remain anonymous[14] (including fear of retaliation for views expressed or lack of confidence in the use to which his personal details might be put by the recipient).[15]

---

[13] In the proposed Distance Selling Directive a requirement is made that those offering goods and services at a distance (including electronically) should identify themselves.

[14] Moreover, the European Convention on Human Rights contains relevant provisions affirming the right to privacy and to the secrecy and to the secrecy of the correspondance. The same principle is enshrined in the constitutions or in the constitutional traditions of all Member States. Subject to exceptions necesssary in a democratic society, they have been respected in the postal and telecommunications sector.

In the decision granting a preliminary injunction against the US Computer Decency Act, the judges affirmed the importance of anonymity on the Internet: "*Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR).*"

[15] See paras 29 and 30 of the UK "R^3 Safety-Net" proposals <http://www.ispa.org.uk>

However, the legitimate need for anonymity should be reconciled with the principles of legal traceability. The recent Safety Net proposals[16] in the United Kingdom address this double concern. They take the view that use of truly anonymous accounts is a danger, while use of pseudonyms which are traceable is not. They propose measures to close known loopholes and improve traceability and that anonymous remailers record details of identity. These details would be subject to data protection legislation and therefore made available to the police under appropriate legal safeguards.

The question of legal traceability needs work both on technical issues and on global co-operation in order for measures to be effective.

d. Judicial and police co-operation at EU and international level

As mentioned above, the definition of offences varies from country to country. Due to the international nature of Internet, even if the legislation of the concerned country forbids such contents and require criminal prosecution, it may also occur the author, content provider, and the host service provider, may all be beyond the reach of national law enforcers. Criminal law only operates within national frontiers. In order to avoid loopholes for criminal activities, it would be therefore important, that Member States would define certain minimum common standards in their penal legislation.

Furthermore, penal judicial co-operation and police co-operation should be reinforced among EU Member States and international co-operation with our main third country partners should be envisaged, for instance on the basis of conventions or new international legal instruments.

In this context it would be useful to extend the co-operation also to the prevention of criminal practices using the Internet as a new vehicle for their activities.

Technical expert sand criminal law experts could also meet in order to look at the most appropriate ways to reach some common penal standards. An improved co-operation at EU level between industry and law enforcement authorities should equally be encouraged.

The agreement by Justice and Home Affairs ministers in Dublin to reinforce police co-operation, within the framework of EUROPOL, against paedophilia and trafficking in children and women, and to endeavour to set common minimum standards for the law

---

[16] *"R3 Safety-Net: Rating, Reporting, Responsibility For Child Pornography and Illegal Material on the Internet"*, September 1996

against sexual abuse of minors, should be seen as an encouraging first step in this direction.

Similarly, the declaration of the World Congress Against the Sexual Exploitation of Children recently held in Stockholm should form a basis for common action.

5. DEALING WITH HARMFUL CONTENT ON INTERNET

The main weapon for dealing with harmful content is in ensuring that practical means are available to limit access by the vulnerable to such content.

a. The principle of freedom of expression.

The European Convention on Human Rights, signed by all Member States and part of the general principles of Community law, contains relevant provisions affirming the right to freedom of expression. These rights can be subject to some conditions, are not absolute and are subject to important qualifications, for instance permitting licensing of broadcasting, television or cinema enterprises. The same principle is enshrined in the constitutions or the constitutional tradition of all Member States.

The borderline between what is protected by free speech and what can be restricted may not be easy to draw by the Member States.

In France, the Constitutional Council recently annulled the provisions of the Telecommunications Law which set out the conditions under which access providers (including Internet access providers) were to be free of criminal liability for content to which they gave access. The law gave power to the Conseil Supérieur de la Télématique to make recommendations on what types of content was permissible. The Constitutional Council took the view that this provision needed to be drafted more carefully, since questions of individual liberty were involved.[17]

One general conclusion is that ***any regulatory action intended to protect minors should not take the form of an unconditional prohibition of using the Internet to distribute certain content that is available freely in other media.*** Another conclusion is that

---

[17] Le Conseil Constitutionnel a décidé de supprimer les articles 43-2 et 43-3 de la loi sur la réglementation des télécommunications au *motif «que la loi a confié au Conseil Supérieur de la Télématique le soin d'élaborer et de proposer à l'adoption du Conseil Supérieur de l'Audiovisuel, auprès duquel il est placé, des recommandations propres à assurer le respect par certains services de communication de règles déontologiques, sans fixer à la détermination de ces recommandations, au regard desquelles des avis susceptibles d'avoir des incidences pénales pourront être émis, d'autres limites que celles, de caractère très général, résultant de l'article 1 de la loi susvisée du 30 septembre 1986».*

existing rules on content regulation need to be examined to see whether they can be applied by analogy, and that the most restrictive rules should not be applied simply because of Internet's wide potential reach.

Reflecting similar concerns elsewhere in the World, in the United States, a District Court ruled the key provisions of the Communications Decency Act intended to protect minors to be unconstitutional, relying on the principle of free speech in the First Amendment to the US Constitution.[18] The Act was held to have been drafted too widely, because although it was legitimate to protect minors, host service providers could not identify whether a user was a minor, so that in practice "adult" content could not safely be published at all, thus interfering with constitutionally protected free speech.

b. The legal framework of the Internal Market

As the circulation of information on networks covering more than one country is cross-border by nature, it is ***governed by the legal framework of the Internal Market and competition rules***. In particular, it is ***protected by the principle of the free provision of services***. National authorities can take measures limiting this fundamental freedom for example for the protection of minors, but only if the measure is proportional. In other words, the measure must be appropriate to achieve the pursued objective and may not exceed what is necessary to achieve this aim.

In this perspective, the Commission has recently adopted[19] a proposal for a Directive on the establishment of an information and a co-operation procedure between Member States and the Commission on new regulatory issues concerning Information Services. By providing regulatory transparency and preventing a re-fragmentation of the Internal Market, this proposal aims to ensure a more effective protection of the general interest in this field, and a more focused reply to emerging regulatory needs. In addition, the proposed administrative co-operation system between the Member States and the Commission would enable the European Union to deliver a more coherent message on these issues on the international level.

c. Parental control software: empowering parents to protect minors

Fortunately, technical means exist which will allow differences in moral standards, not only between national legal systems but also between the subjective judgments of users,

---

[18] US District Court for Eastern Pennsylvania ACLU v. Reno, 11 June 1996. Full text available at <http://aclu.org/>

[19] COM(96) 392 final, 30.8.1996

to be taken into account. This will allow the aims of free flow of information and respect for individual preferences to be pursued simultaneously.

In response to public demands, ***a number of technologies have been developed over the past two years to enable parents to control Internet content coming into their homes.*** Contrasting with "upstream censorship" by official agencies (preventing illegal content *from being published* at all), filtering provides for "downstream control" by parents (preventing harmful content *from reaching minors).* The filtering model - which stresses ***parental responsibility rather than government intervention*** - is strongly advocated by the industry and by civil liberties groups as the most effective way of solving the specific challenges of the Internet and of taking into account the differences in standards of taste and decency between countries, communities and families. It is a pragmatic, not a legal, response to the presence of harmful content on the Internet - although the provision of filtering devices could have in some cases a legal impact (exoneration of liability for access providers who offer such devices).

Useful as a "line of defence" at the end-user level, filtering software can also be applied at various stages in the transmission process, for example by host service providers or access providers.

Filtering software follows three main models: *"blacklisting"* (where access to listed sites is blocked), *"whitelisting"* (where access is only possible to listed sites) and *"neutral labelling" (*where sites are labelled or rated, but it is up to the user to decide how to use the label or rating).

"Blacklisting" technique has been widely used in the first generation of standalone filtering packages such as Cyber Patrol. Introduced in August 1995, Cyber Patrol works with both direct Internet access providers and commercial online services. Its *CyberNOT* list contains approximately 7000 sites in twelve categories (violence/profanity, nudity, sexual acts, gross depictions, racism/ethnic impropriety, satanic/cult, drugs, militant/extremist, gambling, questionable/illegal, alcohol/tobacco). Parents can selectively block access to any or all twelve categories by checking boxes in the programme manager.

"Whitelisting" works on the reverse principle. "Whitelisting" software blocks out all Internet content, except expressly authorised sites on a "whitelist". This technique is highly limitative, and runs contrary to the logic of the Internet. It is however very safe, and has been used, in particular in the school environment.

"Neutral labelling" Contrasting with early standalone filtering software, a new industry-wide standard, the Platform for Internet Content Selection (PICS) has recently emerged

to provide a standard infrastructure for "neutral labelling" and filtering Internet content. Separating the two functions of rating of sites and filtering of sites, and allowing a high degree of flexibility and security, PICS is undoubtedly the most comprehensive and innovative solution yet to tackle Internet contents issues.

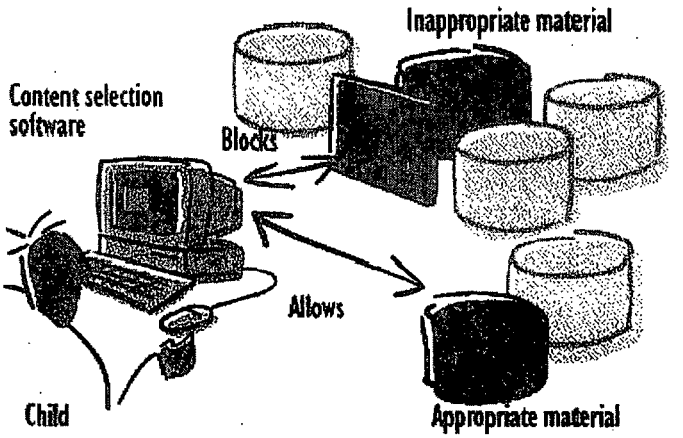

Figure 1: selection software automatically blocks access to some documents, but not others.[20]

d. PICS: a global industry standard

The Platform for Internet Content Selection (PICS) which was officially launched in May by the World Wide Web Consortium[21]***, is an industry-wide attempt to establish a global standard.*** Offering *"Internet access control without censorship"*, PICS is supported by a wide coalition of hardware and software manufacturers, access providers and online commercial services, publishers and content providers. It is now included as a standard feature in the latest generation of Internet browsers such as Microsoft Explorer 3.0 and Netscape 3.0, and is also supported by a number of filtering packages.

In contrast with the first generation of filtering software which relied on key words and *"black lists"*, PICS works on the ***principle of "neutral labelling" and filtering of all***

---

[20] These graphics, provided by Netscape are published on the WWW Consortium pages refering to PICS. This site provides extensive techical specification on the PICS standard. (http://www.w3.org/pub/www/PICS)

[21] The W3C is an industry consortium which seeks to promote standards for the evolution of the Web and interoperability between WWW products by producing specifications and reference software. The Consortium is international; jointly hosted by the MIT Laboratory for Computer Science in the United States and in Europe by INRIA who provide both local support and performing core development. The W3C was initially established in collaboration with CERN, where the Web originated, and with support from DARPA and the European Commission.

types of sites with an Internet "address" (URL) (Web pages, FTP, Usenet newsgroups). PICS effectively "tags" sites with "value-neutral labels". These labels can support different types of information: ratings (for instance, evaluating language, nudity, sexual content, violence), or pointers (identifying contents according to their relevance or interest for various constituencies of users). To be viewed, the site must (1) carry a PICS label, (2) be within the parameters set by parents on the home computer. Ratings can be established by content providers themselves (such as entertainment companies operating family-oriented web sites) or by third parties (such as religious groups or parents' associations). Each family decides which ratings systems it wishes to use and then, using the parameters, what is acceptable and what is not.

These ratings can be distributed and upgraded via a number of channels, online or off line (diskettes, CD ROMS).

Parents and educators can restrict access to sites that (1) carry a PICS label, (2) match the parameters set by the parents on the home computer. For the Recreational Software Advisory Council (RSAC), which provides the ratings for video games and Web content, parameters can be set by parents using cursors with values from 0 to 4 on four sets of criteria (language, nudity, sexual content, violence). Each family decides, using these parameters, what is acceptable and what is not.

Unlike the V-chip for television (which relies on hardware to provide blanket blocking of programmes), or most existing standalone software packages (which block indiscriminately through key words), ***PICS-compatible applications therefore provide an effective technology for the indexing and screening of content - and a flexible and inexpensive solution to the differences of sensibilities between various families and cultures***. Although the Internet ***may have created new risks, these techniques also offer new opportunities*** not available for other means of content delivery.

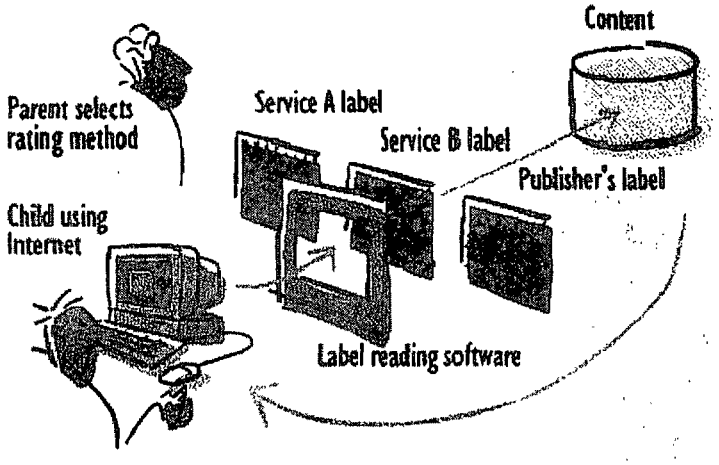

***Figure 2**: selection software blocks based on labels provided by publishers and third-party labelling services, and on selection criteria set by the parent.*

Work on labelling and rating systems in the computer environment is also showing great promise in other digital applications particularly in the field of digital television. These important developments are covered in the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services.

e. The extent to which filtering can be used

Since the early prototypes based on key words - which did not discriminate between pornographic and medical sites - ***filtering software has improved considerably***. However, although parental control software can now efficiently screen for suggestive words or for known sites, it cannot at this stage screen for explicit images unaccompanied by suggestive text, unless those who configure the software are aware of the particular site. Of course rating agencies can label sites on the basis of visual content, thus bringing them within the scope of PICS filtering.

Similarly, the opponents of filtering approach underline two main risks: that existing unacceptable content on the Internet could be always be accessed from an unprotected computer; and that in most homes computer-aware children may always disable their parents' best efforts. This concern has been addressed by PICS, which claim that the system is tamper-proof.

However, despite some limitations, currently available user-based software suggests that an ***effective method of empowering parents and protecting their children from inappropriate content is already widely and cheaply available.***

f. European rating systems

In order to ensure that users have access to rating systems suitable to their needs, and in order to avoid a situation whereby they have to rely on rating systems developed for the US where there may be a different approach on what is suitable content for minors, ***encouragement should be given to setting up European rating systems***. This should not however be a single monolithic system, since this would run counter to the principle of subsidiarity and be seen as an attempt to impose moral uniformity. Rather, ***European content providers, as well as European rating agencies, should be actively encouraged to set up their own rating systems.*** In any case, it should be ensured that rating, listing or self-control systems are based on open standards developed on a European or international basis rather than proprietary standards.

In parallel, development of European filtering and tracking software (in order to trace where illegal content comes from) should be encouraged in the framework of Community R&D programmes.

Reporting mechanisms ("hot lines") should be established, to encourage the public in detecting and reporting illegal and harmful sites. In the US, voluntary watchgroups are already playing a useful part in the updating of lists and verification of ratings.

g. Educating the public

Neither the strict application of laws, nor blind reliance on technology will entirely solve the issue of illegal and harmful content on the Internet. Public education will play a crucial role. ***Awareness activities should therefore be encouraged so that users understand the opportunities as well as the drawbacks of the Internet.*** Parents and educators, in particular, should be sufficiently informed so as to be able to take full advantage of parental control software and rating systems.

6. POLICY OPTIONS/CONCLUSIONS

The Commission considers that the following actions to reduce the flow of illegal and harmful content on the Internet should be taken. They aim to enhance the benefits which Citizens of the European Union will obtain from increased access to information through Internet and should be adopted - according their respective nature - under the provisions of the EC Treaty (free movement of services) or within the framework of Justice and Home Affairs.

This is a ***first set of measures for immediate action***. They do not prejudice further proposals as a result of discussions initiated by the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services.

1. Illegal content

a). Co-operation between Member States

Co-operation between Member States is vital to combat the sources from where criminal content comes and in restricting distribution of copies.

There is a need to reinforce co-operation in the context of Justice and Home Affairs with a view to:

- ***exchange information*** on those providing criminal content and enforce existing laws relating to criminal material

- encourage Member States to define ***minimum European standards*** on criminal content.

b) Liability of access providers and host service providers

The need for a common European framework to clarify the administrative rules and regulations which apply to access providers and host service providers should be assessed.

c. Encourage self-regulation

The Commission will continue to ***encourage co-operation between associations of Internet access providers to help the process of self-regulation***. This process should be put in motion in those Member States where it has not yet started. The Commission will ***encourage discussion and research into technical issues*** concerning access providers' and host service providers' role in limiting distribution of illegal content.

2. Harmful content

Community action to support use of filtering software and rating systems

- A Council recommendation could be envisaged setting out a clear political message ***encouraging the use of filtering software such as PICS***, and for one or more European rating systems. The Commission has already called upon the industry to form a common platform enabling the use of filtering systems Community-wide.

- European ***content producers*** should be encouraged to co-operate in this system by adopting their own ***Code of Conduct for content published on the Internet***, including systematic self-rating of content.

- A Commission initiative will ***support national awareness actions for parents and teachers***

3. International issues

a) An International Conference

At the Industry Council of 8 October 1996, the invitation by Germany to host an International Conference was accepted. This will involve representatives of law-enforcement authorities, together with representatives of access providers, host service providers and users. It will concentrate on:

- feasibility of ***immediate measures including a framework for international co-operation***, using the existing legal framework

- discussion on the ***possibility of an international convention on illegal and harmful content.***.

b) Extension of the dialogue

Since this dialogue must include the largest number of countries possible, it could be extended to a body with a larger membership such as the OECD, the World Trade Organisation, the United Nations, or one of the more specialised United Nations bodies.

4. Support actions

a) Transparency mechanism

Regulatory issues should be examined at Community level in a systematic and transparent manner, so as to elaborate coherent and effective legal solutions.

b) Information Web site

A site will be set up on the World Wide Web (hosted by a Commission server) containing original content and links to appropriate pages on other sites. This Web site will be part of a comprehensive set of Web pages dedicated to broad range of information and related topics, which will be established in the framework of the action plan *Learning in the Information Society* recently adopted by the Commission.

The type of content available could include a) information and guidance for parents, teachers and children b) parental control software c) information on activities of official bodies (EU institutions, Member States, third countries, international organisations and non-governmental organisations).