EUROPEAN MASTER DEGREE IN HUMAN RIGHTS AND DEMOCRATISATION 2000-2001
RAOUL WALLENBERG INSTITUTE

Internet and Freedom of expression

Rikke Frank Jørgensen
rfj@digitalrights.dk

Supervisor:
Gregor Noll

Abstract

Internet challenges the right to freedom of expression. On the one hand, Internet empowers freedom of expression by providing individuals with new means of expressions. On the other hand, the free flow of information has raised the call for content regulation, not least to restrict minors' access to potentially harmful information. This schism has led to legal attempts to regulate content and to new self-regulatory schemes implemented by private parties. The attempts to regulate content raise the question of how to define Internet in terms of "public sphere" and accordingly protect online rights of expression. The dissertation will argue that Internet has strong public sphere elements, and should receive the same level of protection, which has been given to rights of expression in the physical world. Regarding the tendency towards self-regulation, the dissertation will point to the problem of having private parties manage a public sphere, hence regulate according to commercial codes of consumer demand rather than the principles inherent in the rights of expressions, such as the right of every minority to voice her opinion. The dissertation will conclude, that the time has come for states to take on their responsibility and strengthen the protection of freedom of expression on Internet.

29.600 words

Table of Contents

1. Introduction

1.1. Point of departure

In his 1998 report to the U.N. Commission on Human Rights, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression outlined the case against government regulation of Internet access and content as follows: "The new technologies and, in particular, the Internet, are inherently democratic, provide the public and individuals with access to information and sources and enable all to participate actively in the communication process. The Special Rapporteur also believes that action by States to impose excessive regulations on the use of these technologies and, again particularly the Internet, on the grounds that control, regulation and denial of access are necessary to preserve the moral fabric and cultural identity of societies is paternalistic. These regulations presume to protect people from themselves and as such, are inherently incompatible with the principles of the worth and dignity of each individual" (E/CN.4//1998/40:IIC4).

In 1999 a consortium of executives from the main media and information technology industries established “The Global Business Dialogue”. The consortium points to the inconsistent international regulation in cyberspace and argues that parliaments are challenging them to develop effective self-regulatory mechanisms. One of the areas, which the consortium addresses, is content regulation, led by Walt Disney.

In December 2000 the United States Congress passed the Children’s Internet Protection Act, which requires schools and libraries to install "technology protection measures" to shield minors from adult content. Two coalitions of US civil liberties groups, library associations, websites and individual library patrons will now challenge the federal law that mandates the use of filtering software in schools and libraries receiving federal grants for computers or Internet access.

In January 2001 a Danish public library announced that it had made filtering mandatory on its public computers, in order to block access to pornography and other indecent material for both adults and minors. The library announced that pornography is not information according to the library’s definition of information and therefore is not protected as such.

In January 2000 an executive from the Danish web portal Jubii.dk described how Jubii automatically, and without notifying their users, changes indecent expressions in their chat rooms in order to facilitate a more decent online environment.

*

Internet challenges the right to freedom of expression safeguarded in the international human rights treaties. On the one hand, Internet empowers freedom of expression by providing individuals with new means of imparting and seeking information. On the other hand, the free flow of information has raised the call for content regulation, not least to restrict minors' access to potentially harmful information.

In the US the call for state intervention has so far led to the US Communication Decency Act in 1996, the Children's Online Protection Act in 1998, and the Children's Internet Protection Act in 2000. On the European level, governments have not sought to the same degree to regulate potentially harmful content by legislation, but are increasingly encouraging private parties, such as Internet Service Providers, to self-regulate.

The legal attempts to regulate content on Internet raises the question of how to define Internet in terms of public sphere and accordingly balance the online rights of expression against the restrictions necessary in a democratic society. In other words, *which level of protection should be provided for the communicative sphere of cyberspace*?

Also, the tendency towards private parties' self-regulation raises some interesting issues from a human rights perspective. Freedom of expression is a protection of individuals' right to voice opinions and to receive information without state interference. This freedom builds on the presumption that the public sphere is managed, or at least supervised, by the state. However, on Internet, the public sphere is neither managed nor supervised by the state, but by private parties whom increasingly self-regulate in order to secure a "safe" online environment. This raises the question of positive state obligations; specifically *how to secure freedom of expression in a public sphere managed by private parties?*

1.2. Aim of dissertation

The dissertation will try to give an answer to these two questions, thereby making a contribution to the political and legal zone of ambiguity, which currently characterises the protection of online freedom of expression. In doing so, the dissertation will explore:

- How the communicative sphere of Internet can be understood in terms of public versus private sphere.
- How the characteristic features of Internet differ from other media types.
- Which level of protection the right to freedom of expression provides for.
- The legal and political space so far defined for regulating online expressions and information retrieval, including self-regulatory tendencies.
- The need for further legal or political action.

For the theoretical basis, the dissertation will draw on Habermas' description of modernity as consisting of system and lifeworld. The theory will be used as a framework for discussing the evolution of Internet from the first lifeworld oriented vision to today's reality, which is a penetrated sphere of private entities, regulation and commercialisation.

In assessing Internet as a new communicative sphere, the focus will be on Internet's functional characteristics and how it resembles and differs from other media. The concept of system and lifeworld will further be used to discuss Internet in terms of public versus private sphere.

As a legal basis, the dissertation will use Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the related case law of the European Court. The level of protection provided for by the right to freedom of expression will be discussed by examining the scope of application of Article 10. The legal assessment will include some current policy tendencies in the field of freedom of expression and Internet.

In order to define the legal and political space so far defined for online content regulation, some recent cases will be examined. The cases will primarily deal with two types of content regulation, namely state legislative measures and self-regulatory schemes.

The final part of the dissertation will discuss the level of protection that should be provided for online expressions, including the issue of positive state obligations in order to protect freedom of expression in a communicative sphere managed by private parties.

2. System, lifeworld and Internet

The chapter will introduce Habermas' theory of modernity, and use the concepts of *system* and *lifeworld* as a theoretical framework for discussing the evolution of Internet from the first lifeworld oriented vision to today's reality of system penetration.

2.1. The concepts of system and lifeworld

The concepts of *system* and *lifeworld* are central in Habermas' analysis of modernity, where they represent two different forms of action spheres: a lifeworld with communicative actions oriented to reaching understanding; and a system with instrumental/strategic actions oriented to success (Habermas 1991:258).

Lifeworld represents individuals' natural worldview and functions as the basis for their communicative actions. The lifeworld consists of three components: culture, society and personality, which represent a coherent resource that functions as a background for individuals' adjustment to the surrounding society. The cultural aspect is referring to the cultural heritage and language. The society aspect is referring to the social norms and rules for how to behave in society and is, as such, helping to ensure that social integration can pass relatively unproblematic. The personality aspect is referring to the individual capacities learned during the socialisation process (Habermas 1992:138).

An important function for the lifeworld is to serve as "home" for communicative actions. As the lifeworld represents the cultural and linguistic horizon of meaning, it gets a context creating as well as a constitutive function. As context, the lifeworld functions as an implicit horizon, which individuals' draw upon when communicating. Its constitutive function is related to the fact that individuals are captured in the structure and worldview of their language, which accordingly constitute how they perceive the world. According to Habermas, it is through communicative actions that individuals reproduce the lifeworld, specifically maintain and develop culture and language.

Closely connected to communicative actions is the concept of public sphere and public opinion. According to Habermas, events and occasions are public when they, in contrast to closed or exclusive affairs, are open to all, in the same sense as we speak of public places or public houses (Habermas 1989:1). The public sphere appears as a specific domain, the public domain versus the private, where communicative action can flourish and form public opinion (Ibid:2). It is through communicative actions in the public sphere that lifeworld gains its potential for opposing the system, by fostering the public's role as a critical judge (Ibid).

Whereas lifeworld is symbolic in its nature, the system is material. The system represents societies economic-administrative apparatus, which is not reproduced through communicative action but through money and power. The system is a norm free social sphere, where subsystems (economic and political) are regulated by anonymous and language free media[1]. Since these media are not based on communicative actions (where you need to present arguments) they allow for much faster and more effective interactions.

Habermas uses the concepts of system and lifeworld to characterise modern societies with two main tendencies. On the one hand, a growing complexity where still more interactions are mediated by the system's media (money and power) and where still more subsystems are created to deal with this complexity. On the other hand, an increasing uncoupling of system and lifeworld – that is social integration and system integration. Habermas is concerned about this development because the system increasingly gets disconnected from norms and values, in which it should be anchored (Habermas 1992:154). But he is also optimistic in the sense that he believes the rationality inherent in communicative actions can re-establish the coupling between system and lifeworld.

This distinction between social and system integration is one of the main differences between Habermas and a system thinker such as Luhmann. For Luhmann, there is no distinction between system and lifeworld, but only between different subsystems. Accordingly, different system perspectives replace lifeworld as a common linguistic and cultural background and the normative base, which it implies. Modern societies consist merely of media-mediated subsystems, which has as their main task to reduce

[1] Media simulate some of the features of language, for instance the structure of raising and redeeming claims, whereas the structure of mutual understanding is not reproduced (Habermas 1992:263).

complexity. Through this process of reducing complexity, the systems constructs an inner complexity according to its media, such as money, power or love. The inner complexity represents the level of (outer) complexity, which the system is able to deal with (Luhmann 1993: Chapter 1:II). Despite these differences between Habermas and Luhmann, there are several common lines in their drawing of the modern society; such as increased complexity, increased contingency (the imperative of choice), and system differentiation. Another similarity is that both Habermas and Luhmann stress the importance of communication, whether to reduce complexity (Luhmann) or to establish a coupling between system and lifeworld (Habermas).

In the following section I will explore how Habermas' concepts of system and lifeworld can be used to describe the modern information society – especially the gradual transformation of Internet from an early anarchy stage to an increasingly system controlled agenda.

2.2. Internet as lifeworld

Cyberspace[2] as a new phenomenon appeared in Western Europe in the early1990s. First in universities and research centres, then within society generally, cyberspace became the new target of libertarian utopianism (Lessig 1999:4). Cyberspace arose from the displacement of certain architectures of control. The single-purpose network of telephones was replaced by a multipurpose network of data. The one-to-many architecture of mass media was supplemented by an architecture, where every individual could participate. "The space promised a kind of society that real space could never allow – freedom without anarchy, control without government, consensus without power" (Ibid).

Using Habermas' terminology we would say that Internet in the early stage held promises for an empowered lifeworld, by providing conditions for a communicative sphere free from system interference. In cyberspace, society could regain the critical public sphere, which was lost in the complexity of modern societies, where "town square meetings" where replaced by mass media. In cyberspace, everyone could make an

[2] The term cyberspace originates from the American author William Gibson. "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding" (Gibson 1984:51).

appearance, since no editors or power structures would prevent the individual from voicing her opinion. And appearance *is* important for participating in the public sphere. If individuals do not appear, that is are neither seen nor heard, they do not exist as a public voice. "Only in the light of the public sphere did that which existed become revealed, did everything become visible to all. In the discussion among citizens issues were made topical and took on shape" (Habermas 1989:4).

If we look at Habermas' description of public opinion, we see why the first perception of cyberspace held such promise for a stronger public sphere. Drawing on C.W. Mills, Habermas characterises the formation of public opinion by: (1) virtually as many people express opinions as receive them. (2) Public communications are so organised that there is a chance immediately and effectively to reply to any opinion expressed in public. Opinions formed by such discussion (3) readily find an outlet in effective action, even against – if necessary – the prevailing system of authority, and (4) authoritative institutions do not penetrate the public, which is thus more or less autonomous in its operation (Habermas 1989:249). Some of these characteristics, particularly the equal possibility of receiving and expressing opinions, are precisely some of the features, which distinguish Internet from traditional mass media, as we shall see in the following chapter.

Habermas stresses that opinions cease to be public opinions when they are entangled in the communicative structure of "mass". This is due to the characteristics of mass media such as (1) far fewer people express opinions than receive them, thus the community of publics become an abstract collection of individuals who receive impressions from the mass media. (2) The communications that prevail are so organised that it is difficult or impossible for the individual to answer back immediately or with any effect. (3) The realisation of opinion in action is controlled by authorities who organise and control the channels of such action, and (4) the mass has no autonomy from institutions; on the contrary, agents of authorised institutions penetrate this mass, reducing any autonomy it may have in the formation of opinion by discussion (Ibid). Accordingly, the public sphere of the modern world dominated by mass media has lost part of its pre-modern potential for forming public opinions.

Another point made by Habermas when discussing the evolution of communication in the public sphere is the change in the "opinion power structure", thus the need to protect the diversity of the public dialogue from the public itself. Whereas the threat to public

opinion used to be authoritative powers such as the king or state, the threat is increasingly the public itself. "Wherever the apparently no less arbitrary power of the public itself had taken the place of princely power, the accusation of intolerance was now leveled against the public opinion that had become prevalent. The demand for tolerance was addressed to it and not to the censors who had once suppressed it. The right to the free expression of opinion was no longer called on to protect the public's rational-critical debate against the reach of the police but to protect the nonconformists from the grip of the public itself (Habermas 1989:134).

The early vision of cyberspace held the potential for a revitalised public sphere, a sphere free from traditional power structures; built on consensus-oriented communication from the bottom-up by the participants. In this way, Internet represented a potential for strengthening communicative actions. It could be a new means for opposing the systems colonisation of lifeworld.

And Internet does bear promising features for strengthening pluralism and empowering civil society. Here are a few practical examples to illustrate:

- *Easier to get your message out*: Through e-mail and websites, human rights organisations in Egypt and the Palestinian territories can disseminate information more effectively than before, despite modest resources and limited access to local media (HRW 1999:17).
- *New means for suppressed media*: When Radio B92 in Belgrade was closed by the authorities, the station put its programming on the Internet using a Dutch Service Provider. Radio Free Europe, Voice of America and Deutche Welle picked up the station and broadcasted it back into Serbia. In response to this, the government allowed the station back on the air (GILC 1998:C).
- *Easier to "meet and discuss":* Citizens of Arab countries have been able to debate with Israelis in chat rooms at a time when it was difficult for them to have face-to-face contact, telephone conversations, and postal correspondence, due to travel restrictions and the absence of phone or mail links between many Arab countries and Israel (HRW 1999:18).
- *Harder for governments to censor information*: The China News Digest (www.cnd.org) makes available news from non-official sources. While the

Chinese government sometimes blocks the site, users in China have found ways to access it (GILC 1998:B).

- *Easier to find information, for instance from a specific minority group*: An Arab Gay and Lesbian website (www.glas.org) caters to people who, in many Arab countries, have few places to obtain information pertaining to their sexual orientation (HRW 1999:19).
- *Easier access to public information, for instance new laws, decision making and so on:* Through the European Unions website (europa.eu.int) the public can gain access to all EU publications in several languages.
- *Easier access to global information:* For Indian children in the Chiapas region in Mexico, a few computers with Internet access have meant access to a "global library" of information[3].
- *Mobilising civil society*: The McSpotlight site (www.mcspotlight.org) is created to provide information on the "McLibel" trial, against MacDonald and other multinational corporations. The site is a new way of mobilising consumers worldwide and has received some of the most extensive press coverage ever given to a website (Liberty 1998:263).

However, promising these new possibilities were, and presently are, the development of cyberspace over the last five years has led to a situation where Internet is a mixture of liberal potential and the reality of strong system influence. Before we take a look on the tendencies of system colonisation, let me try to sum up the essential features of the (modern) public sphere before and after Internet's entrance onto the scene.

The public sphere before Internet was characterised by mass media as the main mediator of public opinion. With mass media, public dialogue is channelled through a filter where editors choose, which information to present. Using Luhmann's system terminology, we could say that the system of mass media acts according to a communicative code, that determines, which information is selected for publishing or broadcasting, and which information is not (Qvortrup 2001:237). The media cannot present all information, or voice every public opinion, thus system selection is necessary. The public act as information providers to the degree that they provide "saleable stories", but their primary role is as more or less passive information receivers. From an individual point of view,

[3] Internet access is part of "El Mono Pintado" - a project to empower Indian children in Chiapas, Mexico. For further information see http://www.pangea.org/ropalimpia/enotbre2.htm (in Spanish).

the possibility of appearance, for expressing an opinion on radio or television, is very limited. The press has the role of public watchdog or caretaker of the public sphere, but since the press is also enrolled in the system of money (information has to be saleable) and power (the information selection process is part of an institutional power structure), the press is representing both lifeworld and system interests.

With Internet, the public sphere gains a communication means, where every individual can appear and express opinions. On Internet, the filtered mass media communication is supplemented by a communication where the individual can be both information provider and receiver. Cyberspace therefore holds potential for a stronger diversity of opinions and expressions, as they actually exist in society, thus strengthening the public discourse and sphere. An interactive public sphere, where consensus-oriented communicative actions can flourish, supplements the rationale of mass media. The precondition for this empowered public sphere is, however, both cyber-access and cyber-listeners, since public appearance is no good if no one is listening. I will return to these preconditions in the following chapter, after first examining recent Internet development.

2.3. Internet as system

Over the past five years, Internet has moved from the free anarchistic vision to the reality of commercial interests, tools and power. The private sector has realised the potential in the new information market and the increasingly commercial focus is changing some of the initial "rules" of cyberspace, for instance the initial separation between access and content providers and the vision of a free public sphere with unlimited access to information. Private entities, the system sphere, are taking over an increasingly large part of cyberspace, with the result that still more interactions are mediated by the systems media (money and power) and still more subsystems are created to deal with this complexity. To give a few illustrations:

From openness to (system) security

Internet was originally built for research[4], and the architectures were aimed at openness, whereas security in the early Internet stage was provided for by security schemes such as the PGP (Pretty Good Privacy) web-of-trust model. When e-commerce entered the scene, the call for more secure transactions started. The security infrastructure is now developing with commercial applications with built-in encryption, digital signatures and

[4] Until 1991 the National Science Foundation forbade its use for commerce (Lessig 1999:39).

"certificate authorities" to provide for digital certificates. Also the issue of regulation of encryption, that is government's access to secured communication through "recovery keys", has been subject to political debate and regulation for the last five years[5]. This transformation from openness to secureness is one example of new system regulations, in this case the commercial sector and governments redefining the rules of cyberspace.

Commercialisation – new actors and gatekeepers

Another aspect of e-commerce is the increasing focus on the control of cyberspace infrastructure and content, in order for private enterprises to gain market shares from the cyber market. This is changing the media picture and introduces new coalitions of actors. Traditional players in media – publishers and broadcasters – are being joined by partners from the telecommunication sector, from the IT industry and from the financial service sector. New alliances form new trans-national corporations. "As Information becomes the most tradable commodity in the world, many of the major industry players will be global corporations richer than many medium sized-countries. They will have enormous power" (CoE 1998:162).

Some of the new alliances bring together information carriers and content providers, which give these enterprises increasing power to combine control of access with control of content[6]. This can be a step in the direction of access providers as "gatekeepers" that filter access and content due to corporate interests, thus system imperatives of power and money. The development potentially moves a still larger part of cyberspace from the public sphere to a system sphere mediated by power and money and potentially endangers individuals' right to uncensored and non-discriminatory access to the public sphere[7]. So far the media market has argued for self-regulation, but at the European level there is political pressure for a new regime of national and international rules to limit concentration of media resources and to safeguard pluralism (Ibid:163)[8].

[5] "Companies that were once bastions of unregulability are now becoming producers of technologies that facilitate regulation. For example, Network Associates, interior of the encryption program PGP, was originally a strong opponent of regulation of encryption; now it offers products that facilitate corporate control of encryption and recovery of keys" (Lessig 1999:52).

[6] " Free access to a diversity of information sources and creative products is under pressure as a result of the strong trend towards consolidation on the global online market. In all the essential domains of this market one finds a strong degree of concentration among key players" (Hamelink 2000:146).

[7] The creation of one of the worlds largest companies to exploit the new technologies; the merging of British Telecom and the United States telephone conglomerate MCI is one example of a new multi-billion-scale actor. It is also an example of infrastructure and content merging, since MCI have partnership with Rupert Murdochs large media company News Corporation (CoE 1998:162).

[8] The most recent EU initiative in this field is the Green Paper on the convergence of the telecommunications, media and information technology sector, and the implications for regulation (COM 97, 623). The Green Paper states that competition rules are not enough to safeguard media

Barriers to information freedom - search engines

Since no "content directory" of Internet exists, search engines are crucial both as user tools of finding information, and for published information to be easily found. Information that cannot be found on Internet is in principle non-existent to the potential reader. Today there exists a variety of commercial search engines, such as Yahoo, Lycos, Altavista, and Webcrawler, most of them connected to content providers. These are commercial services, where users need to register their content to secure their appearance in cyberspace, and where keyword technique influences the information's position in the searching hierarchy, that is the position on the search result list. A website, which is not connected to a search engine, cannot be found unless the user knows the specific address of the site. Thus, commercial search engines work as both tools and potential barriers to information retrieval.

Search engines have up till now primarily been perceived as neutral information retrieval tools[9], but with the Media Industry's increasing focus on ownership of web portals and the connected search engines, the picture might be changing. For instance did Walt Disney in 1998 announce the purchase of 43 percent of the stock in the search engine Infoseek. Also Time-Warner and News Corp. began the development of their own web portals, and MCI concluded a deal with Yahoo!, whereby its clients will be guided to the search engine of Yahoo! (Hamelink 2000:147). Since the existence of "neutral" search engines is crucial to realising the communicative potential of cyberspace, a development where "information retrieval" becomes a custody would essentially change the rules of Internet, and move information retrieval from a public cyber sphere of communicative actions, to a system sphere of money and power.

Towards Internet regulation

With Internet being "an American invention", the US has more or less privileged access to the "road" level of cyberspace regulation, such as the domain name system (Mayer 2000:149). However, on the "substantive" level there have been a broad variety of

pluralism and access.

[9] For instance did the search engine Altavista in the spring of 1999 start to sell the first two positions in the "search results list", but was so strongly criticized by their users that they stopped the attempt to commercialize the search results. For further information see http://www.joyzone.dk/soegemaskiner/a11_altavista.asp (in Danish).

attempts to regulate cyberspace[10]. It is important to note, that Internet regulation does not depart from a legal vacuum, but that most of the legal issues, for example child pornography, copyright or trans-national commerce, are already subject to regulation or can be resolved by deduction from existing rules (Ibid:151)[11].

Seen from the perspective of human rights, the two major areas of Internet regulation have been privacy and freedom of expression. The privacy issues at stake so far have been (1) how to ensure the privacy of personal data and (2) how to balance the privacy of communication against law enforcement's need for interception and access to online communications. The content issues have been (1) how to control illegal content and (2) how to control legal but potentially harmful content without unduly infringing on the right to freedom of expression (Liberty 1998:146). Since the main topic of this thesis is legal content regulation, I will concentrate on the tendencies in this field and not go further into the area of regulating on-line privacy.

In understanding the regulatory dilemmas of content, it is crucial to distinguish between illegal content such as child pornography and content, which is legal, but might be harmful when accessed by minors, for example adult pornography. Often the two discussions are mixed, thereby confusing the criminal law agenda of combating for instance child pornography with the moral agenda of combating legal content, which might be harmful to minors.

On the European level, the EU Commission has for the last five years encouraged greater cooperation between member states both to enforce criminal law on Internet and for the definition of minimum European standards on criminal content[12]. Regarding legal but potentially harmful content, the Commission encourages the IT industry to form a platform enabling the use of filtering systems based on common standards community-wide[13]. It also encourages content providers to cooperate by adopting their own codes of conduct including systematic self-rating. The *Action Plan on Promoting Safer use of the Internet* is the most recent follow-up on EU's Internet policy. The action

[10] At EU level the most coherent legal framework is contained in the *Directive on electronic commerce* (Directive 2000/31/EC).
[11] For an account of the contesting views on states ability to regulate cyberspace see Goldsmith 1998.
[12] See for instance the *Communication on Illegal and Harmful Content on the Internet* (COM 96, 487).
[13] The Commission identifies two basic technical means of protecting children for accessing harmful and illegal content: "upstream control" which means preventing illegal content from being published and "downstream control" which means preventing harmful content from reaching minors, for example through a filter device (Ibid).

plan has a large range of projects directed at making Internet a safer place, not least for children. The projects are divided into three main areas: establishment of Hotlines, development of rating and filtering systems and awareness building – amounting to a total of 25 Million ECU (Decision no. /98/EC).

A last aspect of Internet regulation to be mentioned here is the issue of Internet Service Providers (ISPs) liability. Some countries, such as Tunisia, have tried to regulate ISPs through Internet specific legislation, which holds ISPs liable for content they host or carry (HRW 1999:35). Other countries such as Singapore regulate ISPs through licensing terms demanding that they block access to foreign websites and newsgroups deemed harmful to national morals (GILC 1998:II). In Europe the issue has been debated since 1995[14]. The Commission in the *Communication on Illegal and Harmful Content on the Internet* stressed that Internet access 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. ISPs should not be targeted by the individual governments and law enforcement bodies where the ISPs have no control of the Internet content" (COM 1996, 487:4b). Also, the most recent European Directive on electronic commerce seeks to establish legal certainty through an exemption from liability for intermediaries who act only as a "mere conduit" for access to information (Directive 2000/31/EC).

New self-regulatory schemes

As illustrated above, the EU increasingly appeals to private parties' ability to self-regulate, not least in the field of potentially harmful content. In 1999 some of the worlds most powerful business players[15] established the Global Business Dialogue on electronic commerce (GBDe) with the aim to establish standards for electronic commerce thereby promoting self-regulatory systems instead of legislation. In the field of content, the working group is lead by the Walt Disney Company, with the aim to: "continue the development of and promote adherence to online codes of conduct and other self-regulatory mechanisms, in order to discourage the distribution of harmful and

[14] In 1998 Germany made headline with *the CompuServe trial*, where the managing director was held responsible for making available prohibited content (child pornography in newsgroups) to users and passed a suspended sentence for two years (Mayer 1998:151). In 1996 the French government proposed legislation by which ISPs should monitor and censor content on their servers. The French Constitutional Court struck down the proposal for being imprecise (Liberty 1999:184).

[15] The forum is made up of executives from e.g. Hewlett Packard, Microsoft, AOL, Bertelsmann, France Telecom, Walt Disney Co., Deutche Bank, DaimlerChrystler, Toshiba Corp, NEC Corp.

illegal content and to protect the interests of all users of electronic commerce, particularly minors" (GBDe Paris Recommendations:3). GBDe is one example of private parties taking on the task of self-regulation.

Another example is PICS (Platform for Internet Content Selection), a technical standard being developed by the World Wide Web consortium in order to supports parents' ability to filter material, which their children access on the web. PICS will provide for third parties, as well as individual content providers, to rate content on the web. The participants in the PICS working group include most of the major service providers, IT industry, content providers and consumer organisations[16]. I will return to the discussion of PICS and filter software in chapter six.

A third example is the ongoing debate on whether Internet Service Providers should self-regulate potentially harmful content on their servers, for instance by following common codes of conduct[17]. In June 2000 the Danish Internet Service Provider Get2Net announced that they would remove websites with "filthy" content from their servers (Berlingske Tidende, 8 June 2000) The announcement started a public debate on the issue of ISP self-regulation in Denmark, and other major Danish service providers such as Cybercity and Scandinavia Online opposed the idea of ISPs in the role as moral regulators (Computerworld Online, 9 June 2000c). The debate was followed by a conference in January 2001, where Get2Net announced that they would opt for voluntarily filter solutions based on user choice instead of removing content[18].

The issue of Internet content self-regulation has been debated under the headline of *INFOEthics* at annual UNESCO conferences for the last four years. It was also the theme of an OECD forum in 1998. Up till now no common agreement has been reached on the issue.

The increasing focus on Internet regulation, whether it be by applying existing laws, developing Internet-specific laws, applying content-based license terms to ISPs, or governments' encouragement of self-regulation by private parties, are all examples of

[16] For further information see http://www.w3.org/PICS/.
[17] It should be noted, that the issue of ISP self-regulation differs essentially from the traditional use of the term. Normally self-regulation is when a profession, for example journalists, doctors or a company decide how to regulate their *own* behavior by setting ethical standards for the profession. However, with ISPs the issue is not regulation of their own behavior but instead regulation of the behavior of their customers, specifically the moral character of their communication.
[18] For further information on the case see http://www.get2net.dk or http://www.digitalrights.dk.

system gaining control over still more areas of the initially free public sphere of cyberspace. The tendency of increasing commercialisation of Internet combined with the concentration of access and content providers indicate a commercial cyber sphere, in which the initial lifeworld potential for civil society is under strong pressure. If the current trend continues, governance of – and access to – cyberspace will, within a few years, be controlled by a concentrated group of media/IT/telecom market leaders, leaving little space for free information access and content diversity. Of course one could argue that for "cyber techies" there will always be a way to steer clear of system regulation. However, for the majority of Internet users; the "mainstreamers", the system regulated and commercialised sphere of Internet is increasingly setting the agenda.

Hence, the initial potential for a stronger civil society through a revitalised and interactive public sphere is currently being challenged by system colonisation. States in non-democratic regimes seek to suppress the free flow of information by for instance ISP control, whereas states in democratic regimes encourage self-regulation by private parties in order to regulate potentially harmful content. Commercial players are increasingly in control of access to information in cyberspace, potentially endangering individuals' right to freely impart and receive information, thus gaining the benefit of an empowered lifeworld. The process of system colonisation is still under way, but it is difficult to contest that Internet today contains a legal and commercial sphere representing strong system influence.

3. Internet as a new communicative sphere

This chapter will examine the essence of Internet as a new communicative sphere, that is, describe how it resembles and differs from other media, including the role of public and private parties in regulating the sphere. The chapter does not intend to give a description of the technical features of Internet, but rather outline the functional characteristics.

3.1. Functional characteristics of Internet

Should one term be used to describe Internet; it is *network*. Internet is a global network of computer hosts, telecommunication paths and gateways linking those hosts. The result is a decentralised, global medium of communication - a "cyberspace" - that links people, institutions, corporations and governments around the world. "The Internet is not a physical or tangible entity, but rather a giant network, which interconnects innumerable

smaller groups of linked computer networks. It is thus a network of network" (District Court on CDA:4).

Internet is open in the sense that no single entity; academic, corporate, governmental or non-profit administers it. There is no centralised storage location, control point, or communication channel and it would not be technically feasible for a single entity to control Internet (Ibid:5). Internet allows any person with access to computer and modem to exchange communication. These communications can occur almost instantaneously, and can be directed either to specific individuals, to a group of people or to the world as a whole. Internet facilitates bi-directional communication, where users are both speakers and listeners and allows for a variety of different communication methods. The most common functions can be grouped into six categories (Ibid:7-11, modified).

- One-to-one communication (such as e-mail or chat)
- One-to-many communication (such as listserv or chat)
- Many-to-many communication (such as newsgroups or chat)
- Real time remote computer utilization (such as telnet)
- Information retrieval (such as ftp, gopher and world wide web)
- Publishing information (world wide web)

One-to-one communication is provided for by e-mail, which allows users to address and transmit a message to one or more people. E-mail is in principle comparable to sending a letter, but unlike postal mail it is generally not "sealed" and can be accessed or viewed on intermediate computers between sender and recipient, unless the message is encrypted.

One-to-many communication is provided for by listserv, which is automatic mailing list services, allowing for communication about particular subjects of interest to a group of people. Listserv can be open, in the sense that users can add or remove their names from the mailing list, or closed in the sense that "membership" is controlled by an administrator.

Many-to-many communication is possible through distributed message databases; so-called newsgroups. Newsgroups are open discussions on particular topics, where

users do not subscribe to a mailing list (as with listserv), but can access the database at any time. Newsgroups can be both open and moderated.

One-to-one, one-to-many or many-to-many communication can also take place through Internet relay chat, which allows two or more users to engage in a real time dialogue by typing messages that appear immediately on the other participant's computer screen. Some chat conversations are moderated or include channel operators.

Telnet provides for *real time remote computer utilization*, as a method to access and control remote computers in real time. Telnet can for instance be used to connect to and access a remote library's online catalogue.

Information retrieval can be done by different methods. Ftp (file transfer protocol) and Gopher are both simple methods to list the names of computer files available on a remote computer, and to transfer the files to a local computer. The most well-known and widespread approach however is World Wide Web (WWW). WWW is a series of documents stored on different computers all over Internet; a platform through which people and organisations can communicate through shared information. The web uses a "hypertext" formatting language (HTML) and programs that browse the web. Hyperlinks allow information to be organized and accessed in flexible ways, and allow users to locate and view related information although information is stored on numerous computers all over the world. "These links from one computer to another, from one document to another across the Internet, are what unify the Web into a single body of knowledge, and what makes the Web unique" (Ibid:10).

World Wide Web also provides for *publishing information;* making information available on WWW. Publishing requires that the publisher have a computer with W3C server software connected to Internet, and that the information is formatted according to the rules of the web standard. Web publishing is simple enough that individual users and small organisations can use WWW to publish "home pages", equivalent to individualised newsletters. Web publishers can either make their websites open to all Internet users or make information accessible only to those with advance authorisation. Most publishers choose to keep their sites open to all in order to give their information the widest possible audience. In order to search for particular information among the public sites, search engines are used.

The open, decentralised nature of WWW differs essentially from previous information systems, for instance database systems such as Lexis, PolInfo and Dialog, which were closed both in the sense that they required varying access software (as opposed to the common standard of the web browser) and in the lack of a possibility for inter-linkage of information.

Following on from this brief outline of the functional characteristics of Internet, I will now examine how Internet differs from other types of media.

3.2. Internet and other types of media

In 1996, the European Commission noted: "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, and 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" (COM 96, 487:7).

Let me illustrate by comparing the functionality of Internet with those of telephone, mass media and common-interest assemblies.

Telephone (one to one): Similar to a telephone, Internet allows for interactive communication between users or small groups in real time, regardless of location. However, unlike the telephone, Internet also allows single users to communicate instantly with large groups of people, thereby greatly extending the reach of the message. Furthermore, the cost of communication is significantly smaller on Internet when compared to long distance telephone calls, thereby lowering the access barriers.

Mass Media (one to many): Similar to mass media (radio, television, print media), Internet allows the broadcaster to reach a large audience. But, unlike mass media, Internet enables any user to be a publisher or broadcaster since editorial control is shifted from a small elite; editors and producers, to every user. Where mass media represent a closed, edited, communication system, Internet holds an open, interactive communication

sphere where everyone can be both speaker and listener[19]. Recalling Habermas' preconditions for the formation of public opinion, we can argue that Internet's interactive nature provides the public with a communicative sphere that is essentially different from mass media, because the distance entailed in the closed, one-way communication structure of mass media is replaced by an open, two-way communicative structure, where every user can speak, listen and disagree. "The programs sent by the new media curtail the reactions of their recipients in a peculiar way. They draw the eyes and ears of the public under their spell but at the same time, by taking away its distance, place it under "tutelage", which is to say they deprive it of the opportunity to say something and to disagree" (Habermas 1989:171). Whereas mass media is a *representation* of lifeworld; an instrument for the public sphere, Internet to a stronger degree *is* public sphere with new means for the public to participate.

Also the cost factor differs. Where mass media have large production and distribution costs, the marginal cost of Internet communication is very low[20]. The marginal cost of adding another website, sending another e-mail message, or posting to a newsgroup is essentially zero (GILC 1998:IIA). It is a forum for expression in which the traditional access and cost barriers are effectively lower; hence exclusion is in principle not possible[21]. In relation to growth rate, the speed of Internet penetration is significantly faster than previous media, making Internet the fastest growing tool of communication ever. Whereas radio took 38 years to gain widespread acceptance[22] and television took 13 years, WWW has taken 4 years (UNDP 1999:58).

Common-interest communities (many to many): Similar to physical world assemblies, Internet has common-interest communities, which can be created and shared by a number of individuals. However, on Internet these communities are independent of the users' physical location and are more accessible in the sense that individuals have stronger means of seeking and finding common-interest groups from all over the world. Also, the cost factor to participate in global online-communities is considerable lower than the physical world's travel expenses.

[19] "It follows that unlike traditional media, the barriers to entry as a speaker on the Internet do not differ significantly from the barriers to entry as a listener. Once one has entered cyberspace, one may engage in the dialogue that occurs there" (District Court on CDA:16).
[20] In the pre-modern stage of the print media also the press was characterized by low production cost and many small publishers (Habermas 1989:168).
[21] The low cost factor preconditions the presence of basic telecom infrastructure in the country, thus it might be significantly higher in developing countries.
[22] UNDP define widespread acceptance as years from inception to 50 million users (UNDP 1999:58).

Besides the functional characteristics inherent in existing media, Internet also provides for fundamentally new means of *Information retrieval*. The easy and low cost access to seek information globally is something that goes beyond the functionality of existing media. Individuals' ability to actively seek and respond to information is perhaps the single most unique feature of Internet communication. Contrary to the communicative actions of mass media, which is based on one-way, saleable information, Internet provide the individual with means for consensus-oriented communicative actions in a public cyber sphere, which is in principle accessible for all.

3.3. Internet as public sphere

By combining the different functional elements of Internet, we see a mixture both of existing media and of private and public communication. The communicative sphere of Internet is open and public in the sense that everyone in principle can access WWW or newsgroups, but it also provides for more closed and private communication, via e-mail[23] or chat rooms dedicated to a particular topic.

World Wide Web is a public sphere, in principle accessible for everyone like a public park or building, but it is also a commercial sphere *managed* by private entities. Even though WWW is often named the "information superhighway" it paradoxically contains no public street but only public locations in the form of websites or cyber assemblies. The websites can be commercial sites selling products or advertisement, they can represent non-profit entities such as NGOs, or they can be individuals' means for communicating a message. Regarding information retrieval, this is a private action *in* a public sphere comparable to seeking information in the physical world, but with essentially different means due to the digital form of the information. Individuals who wish to search for, or receive, certain material can find information on a global scale by using search engines. This differs essentially from going to a local library, bookstore or travel agency, where the information retrieval is bound to physical limits. A Danish citizen who wishes to access the various exhibitions of the Museum of Modern Art in New York has no comparable means of doing so except to enter the museum's website

[23] E-mail communication as the most clear-cut personal communication in cyberspace has not to the same degree as WWW been subject to the discussion of content regulation, but rather to privacy related issues such as users right to use strong cryptography (technical means to secure the privacy of correspondence) and users right to privacy in relation to surveillance, for instance at the workplace or related to cyber crime.

and look at the pictures in digital form. Similarly, a Danish homosexual who wishes to find information on the gay community in San Francisco, can, by the use of keywords, find information on Internet, thereby foregoing the alternatives of travel and phone calls, both implying a much higher cost level. Let us take a closer look at the public and semi-public sphere of cyberspace and compare it to the physical world[24].

The physical public sphere features among others the following characteristics:

- Individuals *interact physically* with other people while in the public sphere.
- Communication is mostly linked to *physical presence* of at least two persons.
- Communication is *influenced by our look, physical capabilities, voice, and age*.
- Individuals can *only to a certain extent avoid information* when moving around in the physical sphere, since information such as signs, posters, pictures and sound (mass media) forces itself on us to a strong degree.

Whereas the World Wide Web features among others the following characteristics:

- Individuals *interact virtually* not physically with other people.
- Individuals can *access the public room in private* thus impart or receive information while being alone.
- Individuals can *avoid limitations connected to space, look, physical capabilities, voice, and age.*
- Individuals can *choose which information to encounter* – to a higher degree.
- Individuals can *choose which information to avoid* – to a higher degree.

As illustrated above, *being* in the public cyber sphere is *a more private act* than being in the physical sphere, since you can hide your identity and be in the public sphere while at home. But it is also *a more public act*, since your expressions are searchable and accessible for a world community, thus giving the expressions a much larger reach and potential audience. These unique features of cyberspace are an important part of its defining characteristics.

[24] At this point, I will not elaborate on the commercial part of Internet but refer to chapter two, where the increasing commercialization of cyberspace is described.

When imparting information the individual has less control over the effect of the expressions, since there is no means of controlling the potential audience as opposed to the physical world where you would, to a stronger degree, know who you were speaking to. The opposite feature characterizes the information retrieval process. Individuals in cyberspace have stronger control over which information they receive, since they to a higher degree affirmatively seek information. We could therefore argue that the need to protect individuals from receiving "harmful" content is less pressing in cyberspace than in the physical world, where individuals are more likely to be confronted by unsolicited signs, posters, noise, pictures and sound. "If the cyberspace in which the information superhighway operates is regarded as analogous to public space, then First Amendment principles evident outside of the electronic media suggest that the burden may be on users of the information superhighway to avoid unwanted messages by electronically averting their eyes. In other words, accessing the information superhighway may be like walking onto a city street, and users should be expected to cope with the wide array of entertainment, annoyance, and offence that normally takes place there" (Harward Law Review quoted in Lessig 1999:38).

When comparing cyberspace with public space, Lessig points to the burden on the users to "electronically avert their eyes", thus cope with the variety of potentially offensive information in the same way as they would do when walking in a street. Yet, in contrast to the physical world, cyberspace is not zoned in districts, such as red light districts or family neighbourhoods, and therefore individuals do not have the same means of recognising "safe" and "less safe" areas. They do on the other hand have *new means of avoiding information* due to the characteristics of affirmative information retrieval outlined above. However, since the access to information is easier in cyberspace, also the access to provoking or disturbing expressions is easier. In the physical world people only encounter a minimum of the existing information, whereas the diversity of expressions is more accessible in cyberspace. We could argue that cyberspace gives freedom of expression a reality check as to how much diversity a society can actually cope with.

Recalling Habermas' definition of public sphere[25], let us finally examine the semi-public sphere of cyberspace that contains chat, listsserv and newsgroups. These cyber assemblies are public in the sense that they are accessible by all, but unlike physical

[25] "Arrangements are public when they (in contrast to closed or exclusive affairs) are open to all, in the same sense as we speak of public places or public houses (Habermas 1989:1).

public assemblies private parties manage them. Cyber assemblies are typically organised according to a topic, and can have moderators or "electronic door men", who monitor discussions and censor expressions, which fall outside the ambit of the discussion forum. Thus the defined topic, potential audience or moral/ethical criteria of the service or content provider define the permitted expressions. Unlike the physical world cyberspace do not have publicly managed space, such as street or parks. "Much of free speech law is devoted to preserving spaces where dissent can occur – spaces that can be noticed and must be confronted by non dissenting citizens. People have a right to the sidewalks, public streets, and other traditional forums. They may go there and talk about issues of public import or otherwise say, whatever they want. Constitutional law in real space protects the right of the passionate and the weird to get in the face of the rest" (Lessig 1999:69). Since cyberspace do not have public space, comparable to streets in the physical world, the role of cyber assemblies is crucial as public meeting places. However, given that cyber assemblies are anchored in the commercial sphere, the codes of system (consumer demand) prevail over the codes of lifeworld (rights of expression), as we shall further explore in chapter five and six.

From the fact that the communicative sphere of Internet is characterised by being open, participatory and with content pluralism as strong as the minds of human beings[26], it follows that Internet is essentially different from mass media. Using Habermas' terminology, we would say that Internet is anchored in lifeworld, and though it is increasingly colonised by the system, the features of its communicative sphere holds some of the characteristics of the pre-modern public sphere: A sphere where communication can flourish from the bottom-up, a sphere which is in principle accessible for all.

Mass media, though they represent lifeworld, are operating within systems power structure and money imperative. The mass media concept is therefore not transferable to cyberspace, but needs to be replaced by a concept that takes into account the complexity of content and functionality on Internet, not least the twilight zone between public and private. Since freedom of expression is a protection of public sphere communication, it is essential that Internet is clearly defined in terms of private and public communication

[26] "It is no exaggeration to conclude that the content on the Internet is as diverse as human thoughts" (District Court on CDA:15).

sphere[27]. As illustrated in chapter two, Internet represents system regulation and commercialisation, but it also represents a lifeworld-anchored sphere. Internet thus represents communicative actions, which are an essential part of being human: the freedom to speak, to listen, to seek information and to disagree. Merely treating Internet as a new media system does not take into account the complexity of its features, nor its unique characteristics of being both system and lifeworld. Internet is more than a new media system; it represents a new way for individuals to live and communicate in the modern world.

3.4. Access to Internet

When discussing Internet's communicative potential, it needs to be stressed that it draws on some preconditions. One precondition is cyber-access - another is cyber-listeners. Regarding cyber-access, the 1999 UNDP Human Development Report shows that access is still not available to most of the world's population, though the fastest rates of growth are in less developed countries[28]. In consequence non-connectivity of the majority of the world's population mitigates against the potential benefits of Internet as a new communicative sphere. In his millennium report UN Secretary Kofi Annan states: "At present, a yawning digital divide still exists in the world. There are more computers in the United States of America than in the rest of the world combined. There are as many telephones in Tokyo as in all of Africa" (UN 2000b:8). The problem of a "digital divide" between those who have cyber-access and those who do not is a political issue, which has been discussed at various international meetings, most recently the G8 meeting in Japan in 2000.

Concerning cyber-listeners, it needs to be stressed that the effect of WWW publishing or common-interest assemblies is relative to the number of cyber-listeners, that is the number of people who actually visit the website or newsgroup, in the same way that the effect of mass media broadcasting must be seen as relative to the number of listeners. Appearance in the public sphere of WWW has no practical effect if the information does not reach the intended audience. The importance of securing individuals with

[27] Mass media, especially print media, have developed borderlines between the public and private sphere for many years, whereas the borderlines in cyberspace are still being negotiated.

[28] See UNDP Human Development Report 1999 (p. 63) for a figure over Internet users worldwide.

cyber-access, and to secure non-discriminatory access to information, is thus crucial to realising the potentials, which Internet holds as a new communicative sphere[29].

A last Internet feature to be mentioned here is related to the level of protection assigned to online communication, thus securing individuals freedom of expression on Internet.

3.5. State protection

Human rights traditionally regulate a power relationship between state and individual, hence protecting individuals' freedom from arbitrary interference by public authorities. In relation to freedom of expression, the protection concerns individuals' right to hold and express opinions, hence oppose the system. With telecom, print or mass media, the protection of freedom of expression is subject to state-regulation through media or telecom law. For instance, almost all countries have established systems for regulating the broadcast media. Issues in relation to these systems include the fairness of licensing procedures and the independence of regulatory bodies from government and commercial pressures (Article 19, The Virtual Freedom of Expression Handbook on broadcast and print regulation). States around the world also regulate the print media and other printed works in a variety of ways, including rights of reply, the impartiality of subsidy systems, and the independence of any regulatory bodies (Ibid). Regarding telecom regulation, this typically includes the protection of non-discriminatory access for citizens to telecommunication lines. In this sense mass media, print media, and telecom are government-supervised, and governments even have some rights to supervise content as a results. As we shall see in chapter five, the US Supreme Court has refused to perceive Internet as a mass media justifying content regulation since the "scarcity doctrine", which justifies content regulation of mass media, does not apply to Internet.

However, if we shift focus from the negative obligation on governments *not to interfere*, to the positive obligation *to protect*, we might argue that states increasingly need to secure that freedom of expression is protected in cyberspace. Thus provide for Internet the same level of protection, which is provided for the physical public sphere.

In cyberspace the control of Internet access and the protection of freedom of expression to a large degree are in the hands of commercial parties, specifically Internet Service

[29] In a 1999 report Article 19 argues for access to information technology as a basic human need (Article 19 1999).

Providers[30]. This gives Internet Service Providers a "state-like" power over both private and public sphere communication and challenges the freedoms, which human rights are meant to protect. It also raises the question of how far the state's positive obligation goes towards protecting individuals from interference by third parties. Private parties' self-regulation potentially involve privatised censorship, where Internet Service Providers restrict individuals' freedom of expression in cyberspace by limiting which communicative actions are allowed on their servers and/or by removing content, which they find offensive, as illustrated by the Danish example in chapter two. The fact that Internet is still a relatively new communicative sphere and currently not clearly defined in terms of public, commercial and private borderlines indicates that the rights of expression lack the level of state protection, which the physical world has developed over decades.

Freedom of expression: state protection in the physical world and in cyberspace

	Physical public space	
State	-> Protection through human rights and national legislation	Individuals
	Telecom system	
State	-> Protection through telecom regulation	Individuals
	Media system	
State	-> Protection through media regulation	Individuals
	Cyberspace	
State	-> Protection to a higher degree left to private parties self-regulation	Individuals

Summing up this chapter, I wish to stress two main issues. One is that Internet cannot merely be perceived as a new media, comparable to mass media, but must rather be seen as a new communicative sphere encompassing both system and lifeworld. The many commercial elements of Internet co-exist with both personal/private means of communication and a public sphere, which provide individuals with essentially new means of expressing themselves, seeking information, meeting, debating, and potentially opposing the system.

The other point relates to the level of state protection outlined above. If we accept Internet as a new communicative sphere with strong lifeworld elements, we need to

[30] As discussed in chapter two, Internet is not a legal vacuum and states do enforce existing law, and have made several attempts to regulate the ISP industry. However, the current trend in relation to legal but potentially harmful content is that the ISP industry is encouraged to self-regulate.

consider whether this public sphere calls for positive state obligations in order to protect individuals' right to express themselves and to seek information free from interference by third parties. These two issues will be explored further in the following chapters, after first analysing the right to freedom of expression.

4. Freedom of expression

This chapter will examine the right to freedom of expression provided for by article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, and outline some of the political statements made in relation to Internet and freedom of expression.

4.1. Legal point of departure

Freedom of expression is a fundamental human right[31], which draws on values of personal autonomy and democracy. Freedom of expression is closely connected to freedom of thought and is a precondition for individuals' self-expression and self-fulfilment. The right to express oneself enables an open debate about political, social and moral values, and encourages artistic and scholarly endeavour free of inhibitions (Jacobs and White 1996:223). Freedom of expression is not absolute, since open debate and personal autonomy can cause conflict between the values and rights respected by the system. Therefore, rights of expression can be limited by the system.

The right to freedom of expression is provided for in the Universal Declaration on Human Rights Article 19, the International Covenant on Civil and Political Rights Article 19, the American Convention on Human Rights Article 13, The African Charter on Human and Peoples Rights Article 9, and the European Convention for the Protection of Human Rights and Fundamental Freedoms Article 10. The point of departure of this chapter will be Article 10 of the European Convention (ECHR) and the related case law.

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

[31] In its very first session in 1946, the UN General Assembly stated, "Freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated" (A/RES/59(1): Para.1).

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary" (Article 10, ECHR).

The European Court (the Court) has described freedom of expression as one of the essential foundations of a democratic society, one of the basic conditions for its progress and for the development of every man (Handyside 1976:23). Paragraph one of Article 10 lays down the freedoms protected, whereas paragraph two sets conditions for legitimate restrictions on these freedoms. If the conditions laid down in the second paragraph are not fulfilled, a limitation on freedom of expression will amount to a violation of the European Convention.

Using Habermas' concepts of system and lifeworld, we would say that Article 10, paragraph one provides protection for the individuals' and press' right to exercise communicative actions in the public sphere, whereas paragraph two provides for legitimate system restrictions on this freedom[32]. The legitimate system restrictions are in principle only connected to the state, and not private parties, since the Convention regulates a relationship between the individual and the state. However, as we shall see later on, the question of positive state obligations might extend to protecting individuals from restrictions by third parties.

4.2. Freedoms protected

The freedoms protected in article 10, paragraph one are:

- *Freedom to hold opinions.* The freedom implies that the state must not try to indoctrinate its citizens nor make distinctions between those holding specific opinions and others. The freedom gives citizens the right to criticise the government and form opposition[33].

[32] "A set of basic rights concerned the sphere of the public engaged in rational-critical debate (freedom of opinion and speech, freedom of press, freedom of assembly and association, etc.)" (Habermas 1989:83).
[33] Certain positions have inherent limitations to the right to express opinions, for example civil servants and prisoners.

- *Freedom to impart information and ideas*, which give citizens the right to distribute information and ideas through all possible lawful sources.
- *Freedom to receive information*, which includes the right to gather information and to try to get information through all possible lawful sources[34].
- *Freedom of the press.* The freedom is not explicitly mentioned in paragraph one, but has been underlined by the Court in several cases, where the Court has put strong emphasis on the public's right to know[35].
- *Freedom of radio and TV broadcasting.* The freedom is applicable also for radio and television broadcasting, since the specific possibility to introduce a licensing procedure implies that the freedom as such must be applicable[36].

Since strong content diversity is one of the main features of Internet communication, it is interesting to see to which degree a potential diversity of expressions is protected under Article 10. In an important judgment from 1976 the Court stressed the *pluralism of expressions* protected under Article 10. "Subject to paragraph 2 of Article 10, it is applicable not only to information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the state or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no democratic society" (Handyside 1976:23)[37]. As illustrated by the judgment, the contents of the expressions seem to be irrelevant to the applicability of Article 10. The fact that the information concerned is of a commercial nature or that the freedom of expression is not exercised in a discussion of matters of public interest is also indifferent (Van Hoof 1998:559).

[34] UDHR Article 19 and ICCPR Article 19 refer also to the right to *seek* information.
[35] The Court has often stressed the public interest or public debate factor, for instance in the Sunday Times case 1979, the Lingens case 1986 and the Jersild case 1994.
[36] For a long time the Commission saw no incompatibility between state monopolies of radio and TV and the Convention. However, in 1993 the court gave judgment in the Austrian radio monopoly case (Informationsverein Lentia and others 1993), where the Commission had come to the conclusion that a violation of Article 10 existed. The issue is also mentioned in CCPR General Comment 10: "Effective measures are necessary to prevent such control of the media as would interfere with the right of everyone to Freedom of Expression" (UNHCHR 1983:1).
[37] In assessing the right to freedom of expression provided for in the International Covenant on Civil and Political Rights Article 19, also the Human Rights Committee has stressed that all forms of expressions are entitled to the same degree of protection. "Article 19, paragraph 2, must be interpreted as encompassing every form of subjective ideas and opinions capable of transmission to others, which are compatible with article 20 of the Covenant, of news and information, of commercial expression and advertising, of works, of art, etc; it should not be confined to means of political, cultural or artistic expression" (CCPR/C/47/D/359/1989).

Up to this point no cases concerning Internet content regulation and Article 10 have come before the European Court. However, cases have been raised before courts in the US, which I will examine in the following chapter. First, here is an outline of some of the key concepts concerning Article 10.

The fact that Article 10 protects the free expression of opinions implies that a rather strong emphasis is laid on the protection of the specific means by which the opinion is expressed[38]. Any restriction of the means will imply a restriction of the freedom to receive and impart information and ideas. However, the means by which a particular opinion is expressed are protected only insofar as they are means, which have an independent significance (exclusive means factor) for the expression of the opinion (Van Hoof 1998:559)[39]. Since there exists no comparable alternative for individuals to communicate in cyberspace, one could argue that the independent significance of Internet as a specific means for expressing opinions and receiving information is rather strong.

Another important concept in Article 10, not least in the light of Internet's borderless nature, is the term *regardless of frontiers.* The term indicates that the state must admit information from beyond the frontiers of the country, both to be imparted and received, subject to the possible restrictions laid down in the second paragraph[40]. The term is not applied very much in case law, but is interesting in the light of upcoming cases related to Internet.

The Court has applied a strict supervision on preventive restraints on expressions reflected in those cases where the Court has held that the intended purpose of the ban on publication, the prevention of the disclosure of information, could no longer justify the prohibition because the information had already become public from another source. This was the case in The Observer and Guardian case from 1991, where the Court held that since the information (Spycatcher) was now in the public domain, and therefore no

[38] "Article 10 applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information" (Autronic AG 1990:23).
[39] Van Hoof states that since case law attributes to the first paragraph of Article 10 a broad protection, one may expect that Internet, as a new and increasingly important means to impart and receive information, will come within the ambit of Article 10, as far as it has an independent significance for the expressions of opinions (Van Hoof 1998:563).
[40] For judgments concerning the imparting and receiving of information from abroad see Groppera Radio AG and others 1990 or Autronic AG 1990.

longer confidential, "no further damage could be done to the public interest that had not already been done" (The Observer and Guardian 1991: Para.42). When discussing content regulation on Internet it is important to bear in mind, that regulatory means such as governments' bans on certain information, as carried out in Singapore or China, or mandatory filters on public computers, as carried out in Denmark or the US, are restricting access to information, which is already in the public World Wide Web domain[41]. Thus it is not a question of preventing the disclosure of the information, but rather a question of restricting individuals' access to information, which is already made public.

Regarding individuals' right to *receive information*, the term indicates that the collection of information from any source should in principle be free, unless legitimate restrictions under paragraph two can be raised (Van Hoof:562). In line with this interpretation the Court has ruled that the right to receive information "basically prohibits a government from restricting a person from receiving information that others wish or may be willing to impart to him"(Leander 1987:29).

It is still not clear to what extent the freedom to receive information entails an obligation on the part of the state to impart information (Van Hoof:565). According to Council of Europe's 1982 *Declaration on the Freedom of Expression and Information* the member states shall pursue an "open information policy in the public sector, including access to information, in order to enhance the individuals understanding of, and his ability to disseminate freely political, social, economic and cultural matters" (CoE 1982:1-2). Although the declaration is not a legal document is does give some direction as to the legal/political trend within the member states.

Regarding the level of protection provided for by Article 10, paragraph one is primarily a *negative obligation* on the state not to interfere in individuals' right to express opinions. It might however also entail *positive obligations* on the state to protect individuals from third party interference, thus raising the question of "Drittwirkung"[42]. The Court has held that, although the essential object of many provisions of the Convention is to protect the

[41] The US and Danish cases will be explored in the following chapter.
[42] Van Hoof speak of "a kind of indirect Drittwirkung" in cases where provisions of the Convention - notably Articles 3, 10 and 11 - imply state measures in order to make their exercise possible, i.e. the rights inferred for individuals imply a positive obligation on the part of the Contracting States to take measures vis-à-vis third private parties (Van Hoof 1998:23).

individual against arbitrary interference by public authorities, there may in addition be positive obligations inherent in an effective respect of the rights concerned (Ozgur Gundem 2000: Para.42). "Genuine, effective exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals" (Ibid: Para.43). Thus the state obligation not to interfere might extend to a positive obligation to interfere in order to protect the individual from third party restrictions. The concept of positive state obligations is still developing, and there is no clear legal interpretation on the issue so far.

Summing up on Article 10 paragraph one, it includes a rather broad guarantee of individuals' freedom of expression. Using Habermas' terminology we would say, that individuals' freedom to form and express opinions in the public sphere - whatever the subject be - is legally provided for in Article 10, and effectively implemented by the Court over the past years. Also, at first sight, the restrictions in paragraph two are formulated broadly. However, the Court has taken the position that the exceptions to freedom of expression must be narrowly interpreted and the necessity for any restrictions convincingly established (The Observer and Guardian 1991:30).

4.3. Admissible restrictions

The restrictions, which are admissible according to paragraph two, fall into three categories (CoE 1999:20):

- Protection of the public interest (national security, territorial integrity, public safety, prevention of disorder or crime, protection of health or morals).
- Protection of other individual rights (protection of the reputation or rights of others[43], prevention of the disclosure of information received in confidence).
- Necessity of maintaining the authority and impartiality of the judiciary.

Whereas the first and third point concern restrictions referring to the interest of the system, the second point concerns restrictions referring to lifeworld, that is the freedoms of other individuals.

[43] Politicians can use libel-statutes to curtail criticism in an effective manner. It is therefore important that politicians right to be protected against libel does not amount to outlawing criticism. In the Lingens case, the Court held that the penalty imposed on Mr Lingens (a journalist convicted for public defamation) amounted to a kind of censure, which could discourage him from making criticism of that kind in the future (Lingens 1986).

A key concept entailed in paragraph two is that of "*duties and responsibilities*". Duties and responsibilities play a particularly important part in three circumstances. Firstly, in cases regarding freedom of the press, secondly in cases where the person possesses a special status, and thirdly in cases where the protection of morals is involved (Van Hoof 1998:576).

The Court has often stressed that it is incumbent on *the press* to impart information and ideas on political issues as well as other areas of public interest. "Not only does the press have the task of imparting such information and ideas: the public also has a right to receive them" (Lingens 1986:26). Accordingly, restrictions on freedom of expression where the press is involved are interpreted narrowly by the Court (Ibid:571). Also, several cases have been raised concerning the issue of restrictions on *persons with special status*, such as soldiers, teachers, civil servants, and servicemen. Case law shows that the Court does not easily accept restrictions on freedom of expression due to special "duties and responsibilities" on these groups (Van Hoff 1998:578). We could argue that even though these persons act in a capacity as system representatives (for instance the school system), their right to freedom of expression (that is lifeworld communication) seems to prevail over their system relation when the Court balances the interest of system respectively lifeworld. Finally, duties and responsibilities play an important part in cases where the "*protection of morals*" is invoked to justify a restriction on freedom of expression[44]. Case law seems to indicate that if the concept of morals is involved on good grounds then this leads to a broad margin of appreciation, since state authorities are found to be in a better position to judge national morals[45]. Thus the system of state authorities can - to a relatively strong degree - invoke the protection of morals as a legitimate ground for restricting individuals' freedom of expression.

When assessing a restriction on freedom of expression, the Court applies a three-part test (1) The restriction must be *prescribed by law*[46] and meet the corresponding criteria of precision and accessibility, (2) it must have a *legitimate aim* as provided in Article 10

[44] See Handyside 1976, Müller and others 1988, Otto-Preminger-Institut 1994.

[45] "It is not possible to find in the domestic law of the various Contracting States a uniform European conception of morals. The view taken by their respective laws of the requirements of morals varies from time to time and from place to place, especially in our era, which is characterised by a rapid and far-reaching evolution of opinions on the subject. By reason of their direct and continuous contact with the vital forces of their countries, State authorities are in principle in a better position than the international judge to give an opinion on the exact content of these requirements as well as on the "necessity" of a "restriction" or "penalty" intended to meet them (Handyside 1976: Para.48).

[46] From this follows, that it is in principle the national parliament, who must decide whether or not a restriction should be possible.

paragraph two, and (3) it must be "*necessary in a democratic society.* The term "necessary in a democratic society" implies that there must be a pressing social need for the limitation and that it must be proportionate to the legitimate aim pursued (Guardian and Observer 1991: Para.40). The necessity test is the ultimate and decisive criterion for the Court[47]. When assessing the proportionality of the restriction in question, the Court examines whether the formalities, conditions, restrictions or penalties imposed on the exercise of freedom of expression are proportionate to the legitimate aim pursued, that is the restriction should not be overbroad nor be permitted if a less restrictive alternative would serve the same goal.

Article 10 paragraph two leaves to the contracting states a *margin of appreciation*[48]. The margin is given both to the domestic legislator and to the bodies that interpret and apply the laws in force. "The Contracting States enjoy a certain margin of appreciation in assessing the need for interference, but this margin goes hand in hand with European supervision, whose extent will vary according to the case. Where there has been an interference with the exercise of the rights and freedoms guaranteed in paragraph 1 of article 10, the supervision must be strict, because of the importance of the rights in question" (Autronic AG 1990: Para.61). Since perceptions on whether information should be restricted on morals grounds vary considerably from country to country; national standards are challenged by the borderless nature of Internet. Digitalised information flows freely from one country to another, and it is more difficult for at state to protect national moral standards by banning online information than it is in the physical world.

The borderless nature of Internet challenges the national protection of morals in several ways. One problem is determining ownership of the information; where the information originates[49]. Another problem is related to the fact that information being subject to content ban in one country can easily move to a server in another country, from where it

[47] "Whilst the adjective "necessary" within the meaning of Article 10, paragraph 2, is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable. Nevertheless it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of necessity in this context" (Handyside 1976: Para.48 shortened).

[48] Margin of appreciation is *a certain measure of discretion* left to the states (Van Hoff 1998:83).

[49] "Generally the laws governing ownership and control of a host computer linked to the Internet are the laws of the place of jurisdiction where the host is physically located – typically a state or country. However, the governing laws also can be those of the legal home of the host's owner – for example a corporation in Delaware can operate a computer in New York, and the laws of either state (or both) may apply" (Tolhurst quoted in Lessig 1999:19).

is just as accessible for the user[50]. A third problem concerns the balance of protecting legal standards in one country without infringing on the freedoms of citizens in another country. In the French Yahoo! case[51], where the Nazi information in question was located on a server in the US, the French court ruled that Yahoo France was obliged to find a way to stop French users from participating in auctions of Nazi memorabilia on its US website, to redress violations of French laws banning advertisement, sale or exhibition of any object that might insight racial hatred. Yahoo! implemented the court order by removing the Nazi action site from their US server thereby protecting French legal standards but at the same time infringing on the Americans' constitutionally protected freedom of speech, since the information was legal in the US. The problem relates to the difficulty in restricting online information to certain users or geographical districts, since Internet is not zoned according to identity or geography, which I shall return to in the following chapter.

As illustrated above, Internet challenges the concept of a national margin of appreciation, which has so far been the primary means for the Court to deal with the moral diversity within the member states. In chapter five we shall explore how the American Courts have dealt with the issue of varying moral community standards, and how the EU proposes to deal with the problem.

Summing up on Article 10, it can be said that generally restrictions are interpreted narrowly. However, case law seems to indicate that political ideas in the broadest sense ("public interest speech") leads to a more narrow margin of appreciation, whereas cases concerning "morals" leads to a broader margin of appreciation[52]. Thus the systems' discretion when restricting lifeworld expressions in the field of morals is broader than in the field of political expressions. After this examination of the legal point of departure for freedom of expression, I will illustrate some of the recent international policy tendencies in the field of Internet and freedom of expression.

---

[50] "When a text is published on the Internet, it becomes almost unstoppable; thanks to the solidarity of the Internet, and the activism of various freedom fighters, it can be copied, protected and presented in many places, on mirror sites on every continent (Reporters sans frontiers 2001:1).

[51] In November 2000 a French court ordered Yahoo! to devise a way to block Nazi paraphernalia from being auctioned through its site in countries where the items are outlawed, such as France. The court said Yahoo! would be charged a fine of $13,905 (100,000 francs) each day for supporting the Nazi items on its auction site (International League against Racism and Anti-Semitism (LICRA) and The Union of French Jewish Students (UEJF) v. Yahoo, Tribunal de Grande Instance de Paris, decision of 24.11.00).

[52] It should be noted that the number of cases, which support this conclusion are still relatively few (Van Hoof 1998:578).

4.4. Political statements

As outlined in chapters two and three, Internet bears potential for an empowered lifeworld by providing individuals with essentially new means of communicative actions. Let me illustrate how the political system has addressed this potential.

In the Council of Europe's 1982 *Declaration on the Freedom of Expression and Information*, the member states explicitly addressed the issue of information and communication technology stating that "the continued development of information and communication technology should serve to further that right, regardless of frontiers, to express, to seek, to receive and to impart information and ideas, whatever their source" (CoE 1982:1)[53]. To support this aim, the member states has agreed to the following objectives (excerpts, my emphasis) (Ibid:1-2).

- Absence of censorship or *any arbitrary controls* or constraints on participants in the information process, on media content or on the transmission and dissemination of information.
- The pursuit of an open information policy in the public sector, including access to information, in order to enhance the individual's understanding of, and his ability to *disseminate freely* political, social, economic and cultural matters.

And to intensify their co-operation in order:

- To promote the *free flow of information*, thus contributing to international understanding, a better knowledge of convictions and traditions, respect for the diversity of opinions and the mutual enrichment of cultures.
- To ensure that new information and communication techniques and services, where available, are effectively used to *broaden the scope* of freedom of expression and information.

Also UNESCO has addressed the issue of Internet and freedom of expression in a 1999 draft on *Cyberspace Law*, which is a set of principles to be promoted by UNESCO (excerpts, my emphasis) (UNESCO 1991:4-5).

- Communication Principle: The right of communication is a *fundamental human right.*

[53] CoE (the MM-S-OD specialist group) is currently (June 2001) preparing a draft recommendation on self-regulation on Internet, but the draft is not yet public. For further information see http://www.humanrights.coe.int/media/events/2001/FORUM-INFO(EN).doc

- Universal Service Principle: States should promote universal services where, to the extent possible given the different national and regional circumstances and resources, the new media *shall be accessible at community level* by all individuals, on a non-discriminatory basis regardless of geographic location.
- Ethics Principle: States and users should promote efforts, at the local and international levels, to develop *ethical guidelines* for participation in the new cyberspace environment.
- Free expression Principle: States should promote the right to *free expression* and the right to receive information regardless of frontiers.
- Access to Information Principle: Public bodies should have *an affirmative responsibility to make public information widely available on the Internet* and to ensure the accuracy and timeliness of the information.
- States should *preserve and expand the public domain* in cyberspace.

The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr Abid Hussain, has also stressed Internet's effect on freedom of expression. In his annual reports of 1998, 1999 and 2000 to the Commission on Human Rights, the Special Rapporteur underlines the importance of Internet in the free flow of information, ideas and opinions. For instance, Internet's potential for bringing out dissenting voices and shaping the political and cultural debate (E/CN.4/2000/63). According to the Special Rapporteur, Internet is inherently democratic, and online expressions should be guided by international standards and be guaranteed the same protection as is given to other forms of expression (Ibid).

As illustrated above, international organisations have made rather strong statements related to Internet and freedom of expression. CoE stress the absence of any arbitrary controls or constrains on participants in the information process and argues for a free flow of information, thus *broadening the scope* of the freedom of expression. The Special Rapporteur wishes to give online expressions *the same protection* as is given to other forms of expression, and UNESCO underlines the issue of general access to Internet at community level. UNESCO also stress that states should preserve and expand the public domain in cyberspace, which, according to the framework of Habermas, can be seen as an encouragement to protect the lifeworld-oriented communicative sphere in cyberspace. UNESCO further proposes the development of ethical guidelines for

participation in cyberspace, which could imply common codes of conduct implemented by private parties, as I shall return to in chapter six. Even though neither the CoE Declaration, the UNESCO draft on Cyberspace Law or the annual reports by the Special Rapporteur have legal standing, they all point to the international political focus and awareness on cyberspace, not least in the field of freedom of expression.

5. Cases

I will now examine some recent cases, which deal with the dilemma of online content regulation. Since there have not been any cases concerning Internet and freedom of expression before the European Court, I will employ some of the most well-known US judgments in the field of Internet communication. Chapter five will explore the main arguments of the cases, whereas chapter six will use the cases to discuss the legal and political space so far defined for regulating online expressions drawing on the framework of system and lifeworld. The cases concern the two main types of content regulation. The first type is state regulation on individuals' right to express opinions and receive information. The second type is private parties' self-regulation. Here follows a brief introduction to the cases concerning state regulation.

5.1. State regulatory cases

Restrictions on the right to express opinions

The most well known legislation on online content regulation is the *US Communication Decency Act* (CDA), which passed as part of the Telecommunications Act in 1996. The CDA sought to impose criminal penalties on anyone who used Internet to communicate material that, under contemporary community standards, would be deemed patently offensive to minors under 18 of age. The CDA provided two affirmative defences to prosecution: 1) use of credit card or other age verification system and 2) any good faith effort to restrict access by minors. The law was passed by congress and signed by the president in January 1996, but was ruled unconstitutional first by the District Court for the Eastern District of Pennsylvania in June 1996[54] then by the Supreme Court in June 1997[55].

[54] US District Court for the Eastern District of Pennsylvania: "Reno, Attorney General of the United States; et al. v. American Civil Liberties Union et al." Civil Action no. 96-963, decided 11.6.1996. Referred to as (District Court on CDA).

[55] "As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of 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 benefit of censorship" (concluding paragraph). US Supreme Court: "Reno, Attorney General of the United States; et al. v. American Civil Liberties Union et al."

Following CDA, the *Child Online Protection Act* (COPA) was enacted in Congress in October 1998, as an attempt to cure the constitutional defects of CDA. COPA sought to impose criminal penalties against any commercial website that made material that is deemed "harmful to minors" available on the World Wide Web to anyone under 17 years of age. Thus COPA was narrower in scope aiming only at commercial communications published on WWW. Federal judges struck down COPA in 1998, 1999 and 2000[56] and the Supreme Court has now (May 2001) decided to hear the arguments on COPA.

Restrictions on the right to receive information

The latest initiative from the American Congress aiming at protecting children on Internet is the *Children's Internet Protection Act* (CHIPA) targeted at all schools and public libraries that accept federal money. The law mandates that Internet-connected computers be equipped with software that block or filter out material deemed "obscene" or "harmful to minors." Adults must also use filtered terminals, but they have the option of asking library supervisors to override the filter for "bona fide research or other lawful purpose." CHIPA was attached to the federal budget bill and passed in Congress December 2000. In March 2001, the American Civil Liberties Union[57] and the American Library Association, along with several individual users, libraries and public agencies, filed lawsuits in federal court calling the law unconstitutional[58].

Another important case concerning public libraries and Internet is the *Loudoun Co. Library Case*; a US civil action concerning a public library policy, which prohibited library patrons' access to certain content-based categories of Internet publications. Ten individual plaintiffs claimed that the library's Internet policy infringed on their right to free speech under the First Amendment. Defendant, the Board of Trustees of the Loudoun County Library, argued that a public library has an absolute right to limit what it provides to the public and that any restrictions on Internet access do not implicate the

Case no. 96-511, decided 26.6.1997. Referred to as (Supreme Court on CDA).

[56] "We will affirm the District Court's grant of a preliminary injunction because we are confident that the ACLU's attack on COPA's constitutionality is likely to succeed on the merits" (p.4). US Court of Appeals For The Third Circuit: "Reno, Attorney General of the United States; et al. v. American Civil Liberties Union et al." Case no. No. 99-1324, Opinion filed 22.6.2000. Referred to as (Appeals Court on COPA).

[57] "This is the first time since the development of the local, free public library in the 19th century that the federal government has sought to require censorship in every single town and hamlet in America" (Senior Attorney Chris Hansen in ACLU News Wire, 19.12.2000).

[58] US District Court for the Eastern district of Pennsylvania, "Multnomah Public Library v. U.S." Complaint 2 April 2001. Referred to as (Lawsuit on CHIPA).

First Amendment. In its judgment, the District Court for the Eastern district of Virginia stressed that although defendant is under no obligation to provide Internet access to its patrons, it has chosen to do so and is therefore restricted by the First Amendment in the limitations it is allowed to place on patron access[59].

In December 2000 the Danish Parliament considered a proposal, *B46*, to mandate the use of filtering technology on all public computes in order to protect children. Following the first hearing in Parliament the proposed Act was replaced by a parliamentary recommendation, which proposes that libraries, schools and so forth should establish local Net-etiquettes[60]. Subsequently, Birkerød Public Library announced that they had installed filter software on all their public computers in order to prevent library patrons and minors from accessing websites containing pornographic information. According to Birkerød library, pornographic material is not information within the library's definition of information, and therefore has no protection as such[61].

In the following I will explore the cases using the structure of: Public space and cyberspace, Internet as media, right to impart information, margin of appreciation, necessity test, and the right to receive information.

The proposed legislation in CDA, COPA, and CHIPA can all be categorised as state attempts to regulate the communicative sphere of Internet. Whereas CDA is directed at all communications taking place on Internet, thus encompassing both system and lifeworld, COPA is restricted to communications in the commercial sphere of Internet. If we look at the kind of communication the Acts are aiming at, CDA and COPA both seek to restrict individuals' rights to express opinions, whereas CHIPA and B46 aim at restricting individuals' right to receive information. This is also the question at issue in the two Library cases, Loudoun and Birkerød, which both concern library policies that

[59] "Defendant has asserted a broad right to censor the expressive activity of the receipt and communication of information through the Internet with a Policy that (1) is not necessary to further any compelling government interest; (2) is not narrowly tailored; (3) restricts the access of adult patrons to protected material just because the material is unfit for minors; (4) provides inadequate standards for restricting access; and (5) provides inadequate procedural safeguards to ensure prompt judicial review. Such a Policy offends the guarantee of free speech in the First Amendment and is, therefore, unconstitutional" (VII:Conclusion). US District Court for the Eastern district of Virginia: "Mainstream Loudoun, et al. v. Board of trustees of the Loudoun Country Library, et al., Civil action no. 97-2049-A, Opinion of 7.4.1998. Referred to as (District Court on Loudoun).

[60] For speeches of the Parliament Hearing on B46 see http://www.ft.dk/Samling/20001/MENU/00550064.htm (in Danish)

[61] For the Library's arguments on the filter debate see http://www.birkerod.bibnet.dk/filterdebat.htm (in Danish)

restrict individuals right to receive information by the use of mandatory filters. Common to the cases on self-regulation, which I shall return to later, is the fact that they are content restrictions enforced by private parties. The various means of self-regulation might be subject to government support, as exemplified by the EU supporting the development of codes of conduct, but their enforcement is neither subject to democratic control nor judicial review.

5.1.1. Public space and cyberspace

The cases, which most explicitly discuss Internet's nature as public, private and commercial sphere, are the District and Supreme Courts' judgment on CDA. When examining the proposed content restriction on online speech in CDA, the Court takes as a precondition that Internet communication is entitled to First Amendment protection, thus First Amendment protection applies with the same force on Internet as it does in the print media or in the physical public sphere. The Court acknowledges that Internet is both a means of public, private and commercial communication, that is encompasses both system and lifeworld[62].

In assessing the public sphere of Internet, the Courts stress the communicative potential for individuals and NGOs and argue that Internet is an attractive means for non-profit entities or public interest groups to reach their desired audience. As examples are cited Human Rights Watch website on reported human rights abuses around the world and the Critical Path Aids Project, which offers information on safer sex, the transmission of HIV and the treatment of AIDS (District Court on CDA:15). Using the terminology of system and lifeworld, we could say that the Courts emphasise Internet's potential for empowering lifeworld by underlining the new communicative potentials for civil society. When comparing cyberspace with physical space, the Supreme Court stressed the wide variety of communication methods, which Internet contains and its essentially unique nature as a medium, which I will return to below.

The most explicit comparison to physical space, however, is when the Court assesses CDA in the light of physical zoning regulation, and discusses to what extent CDA can be

[62] When discussing Internets nature the Court differentiates between readers and publishers. From the readers' viewpoint, Internet is compared to "a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services". From the publishers' point of view, it constitutes "a vast platform from which to address and hear from a world wide audience of millions of readers, viewers, researchers, and buyers" (Supreme Court on CDA:6).

said to constitute a sort of "cyber zoning" on the Internet. In the physical world, a zoning law is valid if (1) it does not unduly restrict adult access to the material; and (2) minors have no First Amendment right to read or view the banned material (Supreme Court on CDA:20). In its physical zoning regulation the Court has taken as a precondition that an adult zone, once created, can actually preserve adults' access while denying minors' access to the regulated expressions. "Before today, there was no reason to question this assumption, for the Court has previously only considered laws that operated in the physical world, a world that with two characteristics that make it possible to create "adult zones": geography and identity" (Ibid:21). For instance, a minor in the physical world can attend an adult dance show only if he enters an establishment that provides such entertainment. And should the minor attempt to enter, he will not be able to conceal completely his identity (or his age). Thus, the twin characteristics of *geography and identity* enable the establishment to prevent children from entering, but to let adults inside (Ibid).

Cyberspace is fundamentally different, as outlined in chapter three, since it allows speakers and listeners to mask their identities, given that it is a virtual world. Even though cyberspace reflects some form of geography (for example locations on WWW), users can transmit and receive messages on Internet without revealing their identities or age. In a dissenting opinion Supreme Justice O'Connor states that it is technically possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws. However, he also acknowledges that this transformation of cyberspace is still underway and until gateway technology is widely available, a speaker cannot be reasonably assured that the speech he displays will reach only adults because it is impossible to confine speech to an "adult zone" (Ibid). Thus, the only effective way for a speaker to avoid liability under the CDA is to refrain completely from using indecent speech. This forced silence impinges on the First Amendment right of adults to make and obtain this speech and reduces the adult population on Internet to expressing only what is fit for children (Ibid). The Court therefore held that several of the CDA provisions failed to adhere to the first of the limiting principles mentioned above, since it restricted adults' access to protected materials in certain circumstances.

The Court also stressed that physical zoning regulation, such as keeping adult movie theatres out of residential neighbourhoods, aims not at the content of the films shown in the theatres, but rather at the secondary effects, such as crime and deteriorating property values, that these theatres foster. Since CDA applies broadly to the entire universe of cyberspace and since the purpose of CDA is to protect children from the primary effects of "indecent" and "patently offensive" speech, rather than any secondary effect of such speech, CDA is found to be essentially different from real world zoning regulation. “The CDA is a content based blanket restriction on speech, and, as such, cannot be "properly analysed as a form of time, place, and manner regulation” (Ibid:12).

Summing up on the Courts’ assessment of cyberspace compared to physical space, it is stressed that:

- Internet contains private, public and commercial communication, thus encompasses both system and lifeworld.
- Internet especially empowers individuals and NGOs by providing them with easy and inexpensive means of communication.
- Internet lacks the physical world’s characteristics of geography and identity, thus making it difficult to zone cyberspace according to place or identity. Accordingly, it is difficult to protect minors’ access to “indecent” expressions, without unduly restricting adults’ freedom of expression.

5.1.2. Internet as media

The main case dealing with Internet’s feature as a medium has been the District and Supreme Court’s judgment on CDA. The diversity of Internet functionality and content was stressed in both the CDA judgments. The Supreme Court speaks of the dynamic multifaceted category of communication, which includes traditional print and news services, but also audio, video and still images, as well as interactive real time dialogue (Ibid:8). The District Court speak of Internet content being as diverse as human thought (District Court on CDA:15). Both Courts agree that the diversity is possible because Internet provides an easy and inexpensive way for a speaker to reach a large audience. When assessing Internet as media the Supreme Court applied the notions of “regulation history”, of “frequency scarcity” and of “invasive nature”, which were recognised as justifying regulation of the broadcast media. The Supreme Court agreed that these three factors were not present in cyberspace, and therefore previous broadcasting cases

provide no basis for qualifying the level of First Amendment scrutiny that should be applied to Internet (Supreme Court on CDA:12).

In arguing for the less invasive nature of Internet, the Courts stressed (1) the *element of affirmative steps*. Contrary to mass media, the receipt of information on Internet requires "a series of affirmative steps more deliberate and directed than merely turning a dial" (Ibid:4). Whereas users might be unprepared for pictures and sound from television and radio, which enter the living room once the devices are turned on, Internet requires the user to take affirmative steps by typing in keywords in a search engine and choosing the site to access, in order to encounter information. Similarly, accessing newsgroups, bulletin boards, and chat rooms requires several steps. Merely turning on the computer does not provide the individual with unwanted information[63]. The District Court stated, that evidence adduced at the hearing showed significant differences between Internet communication and communications received by radio or television. Although content on Internet is just "a few clicks of a mouse" away from the user, a child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended (District Court on CDA:17).

The Courts also underlined the (2) *element of pre-warning*. The Courts agreed that in most cases the user receives some kind of information on websites' content before taking the deliberate decision to access the content, thus "users do seldom encounter content by accident" (Supreme Court on CDA:8). Due to the element of pre-warning, which was found to be essentially different from the element of "assault" involved in broadcasting, the Court agreed that communications over the Internet do not to the same degree "invade an individual's home or appear on one's computer screen unbidden" (Ibid:12). The Court also found that almost all sexually explicit images are preceded by warnings as to the content, thus users are not likely to come across a sexually explicit sight by accident[64].

[63] "Demonstrations at the preliminary injunction hearings showed that it takes several step to enter cyberspace. On the World Wide Web, a user must normally use a search engine or enter an appropriate address. Similarly, accessing newsgroups, bulletin board, and chat rooms require several steps" (District Court on CDA:16-17, shortened).
[64] The governments witness, Agent Howard Schmidt, Director of the Air Force Office of Special Investigation, testified that the "odds are slim" that a user would come across a sexually explicit site by accident (District Court on CDA:17).

In arguing for the lack of spectrum scarcity related to Internet communication, the Supreme Court underlined that, whereas censorship of radio and television is based on spectrum scarcity[65], Internet can hardly be considered a scarce expressive commodity, since it provides relatively unlimited, low cost capacity for communication of all kinds (Supreme Court on CDA:8). In assessing broadcast regulation, the Court argued that whereas radio and television has a long history of regulation, Internet has no comparable history to broadcast regulation, and has not been subject to the type of government supervision and regulation that has attended the broadcast industry (Ibid:12). Thus the District and Supreme Courts agreed that Internet is essentially different from broadcasting media, and represents "a unique and wholly new medium of worldwide human communication" (District Court on CDA:16). The District Court also stressed the fact that Internet bears stronger resemblance to telephone communication than to mass media. Due to the unique characteristics of Internet, the Supreme Court agreed that Internet as a medium, unlike broadcasting media, receives full First Amendment protection (Supreme Court on CDA, Syllabus:B).

Summing up on the Courts' assessment of Internet as a media, it is stressed that:

- Internet does not have broadcasting's history of extensive government regulation, the scarcity of available frequencies at its inception, nor its invasive nature; therefore, the factors justifying broadcasting regulation is not present in cyberspace.
- Internet as a media receives full First Amendment protection.

5.1.3. Right to express opinions

Individuals' right to express opinions and impart information is addressed most thoroughly in CDA and COPA. However, whereas COPA is directed at commercial parties (system sphere), CDA imposes restrictions on all Internet communications, whether these originate from individuals, non-profit organisations or commercial parties (both lifeworld and system sphere). In both cases, the Court stated that the law in question is a content-based restriction on speech and should be subject to strict scrutiny.

[65] In the US indecency laws are unconstitutional when applied to print media, while broadcast spectrum scarcity has been used as a rationale to apply indecency laws to broadcast media. Fur further information see http://www.spectacle.org/freespch/faq.html.

In assessing the scope of the CDA, the Courts agreed that it violates the First Amendment due to its vagueness, over broadness and many ambiguities concerning the scope. The communication at issue, whether denominated “indecent” or “patently offensive” is entitled to constitutional protection and the CDA as a government-imposed content-based restriction on speech must only be upheld it is justified by a compelling government interest and if it is narrowly tailored to effectuate that interest (District Court on CDA:23). The Supreme Court stated that CDA’s use of undefined terms such as “indecent” and “patently offensive” was likely to provoke uncertainty among speakers as to content and relation between the two terms (Supreme Court on CDA: Syllabus: D). For instance, each of the two parts of the CDA uses a different linguistic form. The first uses the word "indecent", while the second speaks of material that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs". The linguistic vagueness combined with the severity of CDA’s criminal penalties “may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas and images” (Supreme Court on CDA:8). The Court found that the uncertainty of the terms used undermines the likelihood that the CDA has been narrowly tailored to the goal of protecting minors from potentially harmful material. Thus the scope of the Act being overly broad was a main defect found by the Court. Applying the terminology of the European Court, the Act was not proportionate to the legitimate aim pursued, nor was the law precise enough.

The Court confirmed that the government has a compelling interest in protecting children, but argued that although the protection of children is an important goal, it should not interfere with the legitimate rights of adults to speak or listen to matters not fit for children. As an example, the Court mentions chat rooms. If, for instance, an adult knows that one or more members of a 100 person chat group is a minor, and it therefore would be a crime to send the group an indecent message, this would surely burden communication among adults (Ibid:15).

Regarding the issue of potentially harmful material, the Court stressed that potentially harmful material is not by nature different than other material, since sexually explicit material is an integral part of the different kinds of Internet communications and a search engine might retrieve material of a sexual nature through an imprecise search, just as it might retrieve other irrelevant material. “The accidental retrieval of sexually explicit

material is one manifestation of the larger phenomenon of irrelevant search results" (District Court on CDA:16). When evaluating adults' freedom of expression, the Court made it clear that the First Amendment protects sexual expressions, which are indecent but not obscene, and that the fact that society may find speech offensive is not a sufficient reason for suppressing it (Supreme Court on CDA:15).

When assessing CDA's likely effect on the free availability of online material, the Courts found that in many cases it would be either technologically impossible or economically prohibitive to comply with the CDA without impeding the posting of online material, which adults have a constitutional right to access (District Court on CDA:25). Online speakers "talking" through chat rooms or newsgroups have no practical means of controlling who receives the information, neither can content providers determine the identity and age of every user accessing their material. Implementation of age verification systems would place an inappropriate burden not least on individuals and non-profit organisations. Concerning the affirmative defences in CDA, the Court concluded that such defences would not be feasible for most non-commercial web publishers, and that even with respect to commercial publishers, the technology had yet to be proven effective in shielding minors from harmful material.

In COPA the scope of communications was narrowed to "web communications made for commercial purposes" (Court of Appeals on COPA:6). Commercial purposes were defined as those individuals or entities that are "engaged in the business of making such communications"[66]. In narrowing the scope of communications, COPA sought to encompass the Supreme Court's criticism of the CDA's wide scope. However, when assessing COPA, the Court again stressed that web publishers cannot prevent users from certain geographical districts.

The District Court on COPA also discussed the costs and burdens COPA imposes on web publishers and on the adults who seek access to sites covered by COPA. The Court found that the only affirmative defences available were the implementation of credit card or age verification systems, and that either system would impose significant residual or

[66] "COPA defines a person engaged in the business as one who makes a communication, or offers to make a communication, by means of the world wide web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such persons trade or business, with the objective of earning a profit as a result of such activities" (Court of Appeals on COPA:8).

indirect burdens upon web publishers (Ibid:14). Both systems would require an individual seeking to access material, otherwise permissible to adults, to reveal personal information. Because of the likelihood that many adults would choose not to reveal this personal information, websites complying with COPA might experience a loss of traffic, thus be discriminated compared to other commercial sites simply because they contained material, which might be harmful to minors. Pursuant to the strict scrutiny analysis of COPA the Court held that COPA placed too large a burden on protected expressions. In particular, the high economic cost related to implementing an age verification system could cause web publishers to cease to publish the material. Furthermore, the difficulty in shielding minors from potentially harmful content might lead web publishers to censor more information than necessary. Therefore, both CDA and COPA would impose a disproportionate burden on web publishers, and might have a negative effect on the free availability of constitutionally protected material. The Court concluded that the government lacks an interest in enforcing an unconstitutional law, and that "losing First Amendment freedoms, even if only for a moment, constitutes irreparable harm"(Ibid:16).

In assessing less restrictive means, the Court examined filter solutions, which I shall return to below. The conclusion was that the public interest factor weighs in favour of having access to a free flow of constitutionally protected speech, and that the government had not proved that less restrictive means would not be at least as effective in achieving the legitimate purposes of CDA and COPA.

Summing up on the Court's assessment of individuals' right to impart information on Internet, a few points should be emphasised:

- Online communication, whether denominated "indecent" or "patently offensive" is entitled to constitutional protection, hence the Courts stress the diversity of online expressions protected.
- A content-based restriction on online speech must only be upheld it is justified by a compelling government interest and if it is narrowly tailored to effectuate that interest.
- The protection of children is an important goal, but it should not interfere with the legitimate rights of adults to speak or listen to matters not fit for children.

- Existing technology does not permit material to be restricted to particular states or jurisdiction, thus web publishers cannot prevent users from certain geographical districts.

5.1.4. Margin of appreciation

In both the CDA and COPA, the notion of "indecency" is defined in terms of "community standards" (Court of Appeals:5). Since Internet communication is global this would imply that any communication available to a worldwide audience would be judged by the standards of the community most likely to be offended by the message. In other words, online speakers should comply with the "lowest common denominator".

Accordingly a parent who sent his 17 year old college freshman information on birth control via e-mail could - according to CDA - be imprisoned even though neither he, his child, nor anyone in their home community, found the material "indecent" or "patently offensive," if the college town's community thought otherwise (Supreme Court on CDA:16). The regulated communication might also extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and arguably the card catalogue of the Carnegie Library (Ibid). Given that existing technology does not permit material to be restricted to particular communities, online speakers cannot prevent content from entering a geographic community nor prevent users from certain communities from accessing their site. Internet is a network of networks as described in chapter three, and any network connected to Internet has the capacity to send and receive information to any other network[67]. Accordingly, Internet gives a speaker a potential worldwide audience, whom he/she has no means of restricting without refraining from speaking altogether.

In summary, the community standard, combined with the difficulty in zoning Internet into specific communities, implies that communication complying with CDA would be restricted, not only to expressions suitable for minors, but to expressions where the level of "decency" would be acceptable for the community most likely to be offended by the message. This would not be proportionate to the legitimate aim pursued.

[67] "When the UCR/California Museum of photography posts to its website nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinatti, Mobile, or Beijing – wherever Internet users live. Similarly, the safer sex instructions that Critical Path posts to its website, written in street language so that the teenager receiver can understand them, are available not just in Philadelphia, but also in Provo and Prague" (District Court on CDA:16).

5.1.5. Necessity test

In assessing the proportionality of CDA, the Court states that due to the breadth of the restriction on speech, the Acts impose an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective. The possible alternatives referred to include the tagging of "indecent" material in order to facilitate parental control of material coming into their homes (Ibid). In addressing the issue of possible tagging of "indecent" material, the Court mentions the development of filter software - especially the Platform for Internet Content Selection (PICS), mentioned in chapter two. The Court stresses that until a majority of sites have been rated by a PICS rating service, PICS will function as a "positive" rating system, in which only those sites that have been rated will be displayed using PICS compatible software (District Court on CDA:11). This means that the PICS standard will function as an information inclusion list rather than an exclusion list thus only sites, which have a PICS rating for appropriate content will be accessible, while non-rated sites will be blocked. This type of positive rating is thereby restricting minors' access to a majority of content on Internet, including material of artistic or educational value (Ibid). The Court also mentions various type of stand-alone software intended to enable parents and other adults to limit the Internet access of children, such as Cyber Patrol[68], Cybersitter, Net Nanny, and Surfwatch.

Summing up on the use of filters as a less restrictive means by which to achieve the government's compelling objective of protecting minors, the Court on CDA found that currently available software suggests that a reasonably effective method will soon be widely available (Supreme Court on CDA:3). The Court on COPA also considered parental blocking or filtering as a less restrictive means and went a bit further than the Supreme Court. The Court on COPA acknowledged that, while filter software is both over and under inclusive in the breadth of the material that it blocks, it is likely to be as effective as COPA, while imposing fewer constitutional burdens on free speech (Court of Appeals on COPA:11).

[68] Cyber Patrol developed by Microsoft was the first application to be compatible with the PICS standard and works on the basis of a CyberNot list containing sites in twelve categories ranging from violence/profanity to material related to the sale of consumption of alcohol, beer or wine (Ibid:12).

5.1.6. Right to receive information

The cases selected for dealing with restrictions on the right to receive information are the Loudoun and Birkerød library case, the Danish proposal for mandatory filtering on public computers (B46) and Children's Internet Protection Act (CHIPA).

In the Loudoun and Birkerød library case, the libraries justified their content regulation through the use of mandatory filters with three main arguments:

- A public library has a right to choose which publications to purchase.
- A public library has an absolute right to limit what it provides to the public.
- Pornography is not information according to the library's definition, and therefore not protected as such (Birkerød).

In the Loudoun case, the Court stated that by purchasing Internet access, the library had made all Internet publications instantly available to its patrons. Unlike a book purchase, no extra expenditure of library time or resources is required to make a particular Internet publication available to a library patron. In contrast, a library must expend resources to restrict access to a publication that is otherwise immediately available. (District Court on Loudoun:5). The Court compared Internet to a collection of encyclopaedias from which the library had removed portions deemed unfit for library patrons. "As such the Library's Board action is more appropriately characterized as a removal decision" (Ibid). In assessing the library's purchase argument, the Court concluded that the Library had misconstrued the nature of Internet, since by purchasing "one such publication" (Internet) the library had purchased them all.

Regarding the discretion assigned to the library in selecting material, the Court stated that First Amendment applies to, and limits, the discretion of a public library to place content-based restrictions on access to constitutionally protected materials within its collection. A public library "like other enterprises operated by the State, may not be run in such a manner as to prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion" (Ibid:6). The selection of content is also mentioned in the Danish Library Law where it is stated that materials must not be excluded on the ground of religion, politics or morals[69], and that Danish public libraries are obliged to provide

[69] "§ 2. The aim of public libraries is achieved through quality, diversity and actuality when selecting the material, which is made available. In the selection process only these criteria, and not the materials religious, moral or political character, must be decisive" (Danish Library Law 2000:Article 2, my

access to electronic information resources, including Internet (Ibid:Article 1). With reference to the line of argument from the Loudoun case, one could argue that the decision to exclude access to pornographic websites for patrons at Birkerød Library is an active removal decision based on a moral criteria defined by the library.

Regarding Birkerøds Library's argument on pornographic material not being information, thus not deserving protection under freedom of expression, one should recall the Handyside judgment referred to in chapter four. The judgment underlined the diversity of content protected by Article 10, including information "that offend, shock or disturb the state or any sector of the population". With reference to the European Court's previous assessment it is therefore difficult to imagine that a Court would agree, that pornography - simply by character of the content - would not be information in the sense of Article 10.

The issue of libraries' restrictions on content was also at issue in the Danish Parliament proposal on use of mandatory filters on public computers (B46). In the B46 hearing the Danish Minister on Information Technology and Research opposed the proposal and argued that filter software is overly broad in scope, thereby restricting "relevant and sober" information and potentially infringing on children's right to receive information[70]. The minister also stressed that children will have a variety of means to access information (due to new generations of mobile phones) within a few years, thus public computers will only play a marginal role in children's means of accessing Internet. Finally, she referred to the Danish educational tradition based on dialogue and critical information assessment, rather than filters and censorship[71].

The Danish proposal for mandatory filters on public computers should be seen in the light of the Danish Library Law, by which public libraries are obliged to provide Internet access. Granting every Danish citizen Internet access in public libraries is part of the Governments IT policy, which stresses that public libraries are an important resource in

translation).

[70] The issue of filters being too broad in scope has also been addressed by the President of the American Library Association: "If the same standards used in online filters were applied to a library's books, our shelves would be practically empty" (American Library Association President Nancy Kranich in Seattle Post-Intelligencer, 27 March 2001).

[71] The Danish Minister of Information Technology and Research, Ms Birthe Weiss, at the Parliament Hearing on B46. 5.12.2000.

the Government's efforts to develop a network society for all[72]. The Danish government has thus decided on the importance of citizens' access to Internet, but has not made any statements on the issue of mandatory filters, for example in Birkerød library. It is currently unclear whether Birkerød's filter initiative can be said to violate citizens' right to receive information in the same way as the Loudoun library case, since the case has not been tried before a Danish court.

The Loudoun judgement is also interesting in light of the upcoming case on CHIPA. According to CHIPA there is no universal service for schools or libraries that fail to implement a filtering or blocking technology for computers with Internet access. Accordingly libraries are obliged to install a filter technology in order to filter or block child pornographic materials, obscene materials, and materials deemed harmful to minors. In the lawsuit against CHIPA, the main arguments concern (Lawsuit on CHIPA:3-4):

- Congress is "invading and distorting" the traditional functions of public libraries by requiring them to violate patrons' constitutional right to receive information.
- Meeting the Act's requirements will inevitably lead to the suppression of vast amounts of protected Internet speech that would otherwise be available to public library patrons.
- Congress' use of its spending power to conscript public libraries into its censorship program, thus requiring libraries to do what Congress could not: directly restrict access to information in a traditional sphere of free expression.
- Currently available filtering software is created and maintained by private parties, whose content-based and viewpoint-based filtering decisions are seldom made public, and who were never subject to judicial scrutiny[73].

[72] "The public libraries are an important resource in the government's efforts to develop a network society for all. A new Act on library activities will give the population better possibilities of having access to information. In accordance with the Bill, the public libraries will, in addition to books, etcetera, be under an obligation to provide access to the Internet and digital information resources and to lend music media and CD-ROMs. Finally, in accordance with the Bill, it will be possible to search and order materials at the libraries via the Internet" (The Ministry of Research and Information Technology 2000: Para.11).

[73] "The Act therefore present public libraries with an impossible choice: either install mechanical, imprecise, and incredibly broad speech restrictions on Internet resources, or forgo vital federal funds to which the libraries are otherwise entitled" (Lawsuit on CHIPA:4).

- Library employees are granted unbridled discretion in deciding whether to disable the blocking software "for bona fide research or other lawful purposes", thus inviting abuse and discriminatory treatment.

As stated above, the CHIPA case has yet to be decided, and time will show how the Supreme Court assesses the arguments presented above, not least in the light of the CDA and Loudoun cases.

Summing up on restrictions on individuals' right to receive information enforced through library policies, the Court has stressed that:

- By purchasing Internet, a library had purchased "all the publications" contained in cyberspace. If a library, after having purchased Internet, restricts access to part of the publications, it is an active removal decision.
- By use of filters, a library is spending resources to restrict access to a publication that is otherwise immediately available.
- First Amendment applies to, and limits, the discretion of a public library to place content-based restrictions on access to constitutionally protected materials within its collection.

Concluding on the level of protection, which (American) Courts have assigned to online expressions up till now, the Courts have decided on *full First Amendment protection* and stressed the *diversity of expressions* protected in the communicative sphere of cyberspace. Furthermore, the Court has stressed the *limits in a public library's discretion* in restricting individuals' right to access online material. The level of protection provided for online expressions will be further discussed in the following chapter employing Habermas' concepts of system and lifeworld.

After this examination of the legal space so far defined for exercising freedom of expression in cyberspace, I will now turn to the issue of self-regulation; more precisely, the issue of private parties restricting freedom of expression on Internet.

5.2. Self-regulatory cases

As outlined in chapter two, a current trend in online content regulation is the development of self-regulatory schemes. Self-regulation refers to situations in which an

industry, of its own accord, devises its own means of regulation. The means of self-regulation take many forms, and I have chosen a few illustrative examples, which concern: content restrictions through customer contracts, content restrictions through access denial, content restrictions through code(s) of content and/or combined with rating and filtering systems, and content restrictions enforced through chat and newsgroups policies.

Especially in Europe, the support for self-regulation has long been a proposed path for regulating content on Internet in order to strengthen the protection of minors and human dignity within the member states, as outlined in the *Action Plan on Promoting Safer Use of the Internet* (Decision No 276/1999/EC). As part of the Action Plan, the PICS rating standard are supported as a means of "neutral content labelling"[74]. In assessing self-regulation, the Commission stresses that the various industries have a key role to play in developing and implementing solutions to the problem of protecting minors and human dignity. It is therefore vital that they be mobilised and organised effectively at European level. According to the Commission, the main tasks, which the Industry should work on, are: (COM 96, 483:20)

- Drawing up codes of conduct and concrete measures within a framework defined by the cooperation between national governments departments.
- Identifying areas where there may be a need for common standards on the labelling of material.
- Promoting the PICS standard or equivalent systems with a view of reaching – as quickly as possible – a critical mass of labelling material and navigation systems and/or parental control devices, which are mutually compatible.

In a Communication on the follow-up to the *Green paper on the protection of minors and human dignity in audiovisual and information services*, the Commission proposes *common guidelines* for the implementation of a self-regulation framework at national level[75]. These guidelines are to be implemented by service providers themselves and contain codes of conduct, which should at least provide basic rules on protection of minors and human dignity. It is stressed that the proportionality of the rules should be

[74] I will discuss the regulatory means of rating and filtering in the following chapter.
[75] "Whereas, as a supplementary measure, and with full respect for the existing regulatory frameworks at national and Community level, greater self-regulation by operators should contribute to the rapid implementation of concrete solutions to the problems of the protection of minors and human dignity, while maintaining the flexibility needed to take account of the rapid development of audiovisual and information services" (COM 97, 570:9).

assessed in the light of the principle of freedom of expression, protection of privacy and the free movement of services. The codes aim at voluntarily adoption and implementation by the private parties concerned. One of the objectives is “to ensure that minors do not gain access, without the consent of their parents or teachers, to legal content, which may impair their physical, mental or moral development” (COM 97, 570:13). The EU policy can be seen as reflecting the difficulties related to different Europeans standards on morals, where self-regulation is proposed as a path to extend international control over expressions. The implementation of codes of conduct by private parties, as proposed by the EU, is one example of states encouraging self-regulation in order to deal with the issue of legal but potentially harmful content on Internet.

Another example of self-regulation is the Global Business Dialogue on Electronic Commerce (GBDe), referred to in chapter two, which is a partnership among executives of the leading e-commerce industry - established in January 1999. GBDe points to the inconsistent international regulation and the inflexible regulatory constrains in cyberspace, and argues that parliaments are challenging them to develop effective self-regulatory and market-driven mechanisms that are not limited to national borders, and to address critical policy issues[76]. "We feel we have a role to play in the shaping of public policy. We are capable of rising above narrow geographic issues and competitive issues to realize the majesty of this new medium"[77]. GBDe is primarily working in the field of e-commerce, but the issue of content is also addressed under the organisations “Principles and Recommendations”. The work on content, led by Walt Disney Company, stresses that governments should recognize freedom of expression on the Internet to the same extent as it is recognized in "conventional", offline forms of communication. Furthermore, it stresses that it is the role of business to continue the development of and promote adherence to online codes of conduct and other self-regulatory mechanisms, in order to discourage the distribution of harmful and illegal content and to protect the interests of all users of electronic commerce, particularly minors (GBDe Paris Recommendations 1999:3). Judging from the information on their website, GBDe has not yet taken further steps in regulating content on Internet. However, with the main

[76] GBDe recommends appropriate business and government action on the following issues: Authentication and Security, Consumer Confidence, Content/Commercial Communications, Information Infrastructure (including interoperability and Internet governance), IPR, Jurisdiction, Liability, Protection of Personal Data, and Tax/Tariffs (GBDe, Working Groups 2001).
[77] Chairman of Time Warner, Gerald Levin in Wall Street Journal, 15 January 1999.

partners from the IT and media industry collaborating, the means for developing self-regulatory schemes in the field of content regulation for example by implementation of common codes of conduct is a possible scenario, not least given the objective of protecting minors.

Another means of content regulation is through the conditions, which Internet Service Providers set out in their customer contracts. One example is the Danish Internet Service Provider, Cybercity, whose customer guidelines contains the following statement: "Homepages must not contain any kind of pornography, racist expressions or expressions, which might degrade minority groups or people with certain sexual orientations". "Rules for homepages also apply for communication in newsgroups and for imparting of e-mails" (Cybercity Guidelines:1, my translation).

As illustrated, individuals are - according to Cybercity's guidelines - not permitted to impart legal pornographic material, discuss such issues in newsgroups, nor communicate it using e-mail. I will return to the consequences of such privatised content restrictions in the following chapter, but first a few more illustrative cases on self-regulation.

Another example of content regulation has recently occurred in Sweden, where the website Flashback (www.flashback.se) has been subject to access restriction. Flashback is a website, which allows dialogue on controversial subject such as nazism, paedophilia, and Hell's Angels, as long as the communications comply with Swedish legislation. Flashback has been denied Internet access by all Swedish Internet Service Providers, and is now hosted by a foreign Internet service provider (Politiken Internet, 12 May 2001).

Finally, there is the issue of content regulation in chat fora and newsgroups, where expressions are restricted typically by topic or decency norms defined by the content provider. In the Chat forums of the Danish content provider Jubii.dk, robots and censorship is used for individuals to "feel more welcome" and to keep troublemakers out (Politiken.dk, 12 January 2000). Robots are used to get people involved in chatting, each robot equipped with its own personality. Users often do not know that they are discussing with robots, which have the task of making especially new Chat users feel at ease by engaging them in conversations. Jubii Chat is also automatically altering "dirty" language, without informing the users. This is done in order to protect other users from

indecent or irritating material[78]. For example, the expression "dick" automatically changed to "rose", while the expression "hooker" is automatically changed to "aunt".

Another example is the chat rooms of America Online, which (as most chat rooms) is subject to a decency policy. The policy implies that users agree not to distribute or link to any content that contains vulgarities, graphic descriptions or account of sexual acts, depicts violence in a gratuitous manner without journalistic, literacy or artistic merit, or otherwise use the service in a manner deemed inappropriate by AOL (AOL Guidelines for Groups:1)[79]. American Online stresses that groups that are found to be in violation of the guidelines are subject to removal without notice. AOL also reserves the right to investigate a private group when a violation has been reported or suspected by AOL. The decency policy is enforced through an AOL Community Action Team, which deletes messages deemed unwanted from discussion groups, and which have the right to forbid virtual communicators from ever trading messages again (Klein 2000:184). "Virtual community babble aside, AOL is, above all, a branded media empire over which it exercises as much control as Disney does over the fence colours in Celebration, Florida" (Ibid:185). AOL's power, as a private party regulating online expressions, should be seen in light of their market share, where AOL in mid-1999 had 15 million subscribers or 43 percent of the US Internet service market. AOL's closest competitor, Microsoft, had only 6.4 percent (Ibid:184).

After this illustration on self-regulative tendencies concerning freedom of expression on Internet, I will use the cases to discuss the two main questions of this dissertation. 1) Which level of protection should we assign to freedom of expression on Internet, and 2) How to protect freedom of expression in a communicative sphere managed by private parties.

6. Discussion

6.1. Level of protection

The protection of freedom of expression provided for by Article 10 mainly concerns public sphere communication, hence it is crucial when discussing the level of protection,

[78] "We are not the police, but we have made rules, which apply to everyone and which secures, that users can feel secure and think that it is nice to be on the Chat" (Partner in Jubii Martin Thorborg in Politiken.dk, 12 January 2000 (my translation)).

[79] "We are a service that prides ourselves of a wide-ranging appeal to a wide range of individuals. But at the same time we are also a family service" (AOL Vice President Katherine Bourseenik in New York Times, 31 January 1999.

which should be provided for Internet communication, that we determine Internet in terms of public versus private sphere.

The commercial sphere of Internet is comparable to the commercial sphere in the physical world, but providing the individual with essentially new means of being a consumer, due to the possibility of virtually attending every shop in the global universe of cyber-commerce. The public sphere of Internet is comparable to physical public space in the sense that it is in principle accessible for all, but with essentially new means for individuals *to be* in the public sphere. When individuals express themselves on a website, or discuss various topics in newsgroups, they participate in the public sphere with radically stronger means of imparting information, than if they went down on the street to express their opinion. In this sense, Internet is both a new means of expressing opinions in the public sphere and also a new means for being in the public sphere.

In the judgments on CDA, the Court emphasised that *especially* for the lifeworld (individuals and non-profit entities), Internet holds strong potentials. The Court acknowledged that expressions on Internet *are* entitled to First Amendment protection, and that not even the authorities' legitimate aim to protect children must unduly infringe on adults' freedom of expression in cyberspace. Hence, the Court acknowledges Internet as a communicative sphere, where freedom of expression should receive the highest level of protection. The Court also stressed that cyberspace differs from physical space in terms of geography and identity, thereby making it difficult to zone cyberspace in "adult places" in the sense we know from the physical world. Speakers in cyberspace cannot be expected to know their audience, and therefore it would be unbalanced to restrict the adult population on Internet to expressing only what is fit for a certain community, such as children[80]. As discussed in chapter four, also the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has emphasised that on-line expression should be guided by international standards and be guaranteed the same protection as is awarded to other forms of expression (E/CN.4/2000/63:21).

The Courts on CDA further stressed the diversity of expressions protected on Internet. In line with the assessment by the European Court (Handyside 1976), the Courts agreed that online communication, whether denominated "indecent" or "patently offensive", is

[80] The Yahoo! case differs in the sense that the Nazi material in question was legal in the US and illegal in France. However, Yahoos implementation of the French Court Order (removing the content altogether) points to the difficulty in restricting access to online content for a certain community.

entitled to constitutional protection, thus providing for Internet speak the same level of diversity protection as would apply to communication in the physical world. As discussed in chapter three, the variety of expressions, as they exist in society, are more accessible in cyberspace. Due to geographical limits, people only encounter a very limited degree of the existing expressions in the physical world. On Internet however, people can access a great variety of expressions and be disturbed accordingly. This makes the public cyber sphere both more open and accessible but also more potentially provoking. On Internet, freedom of expression is for real.

Following the Court's assessment in the CDA judgments and the statements of the Special Rapporteur, Internet is acknowledged as partly public sphere with strong lifeworld potentials. Internet has given new means for individuals to voice their opinion, disagree, seek information - thus *be* in the public sphere. Therefore expressions in the public cyber sphere should be entitled to the same level of protection, which is provided for expressions in the physical public sphere. The alternative would be a less protected sphere, where the rights of expression would not apply with the same force as they do in the physical world.

6.2. Internet and mass media

The Courts decision *not* to perceive Internet as a mass media is important, because it points to the essential different nature of Internet communication. In relation to mass media, Article 10 does not include a general right to have access to broadcasting time on radio or television. This limitation is due to the specific characteristics of mass media; the inherent resource limitations on infrastructure due to the scarcity in broadcasting channels and broadcasting time. Therefore, Article 10 cannot provide the individual with a general right to voice their opinion through mass media[81]. As stressed by the CDA judgments, these preconditions do not exist in cyberspace, since Internet has no limitations - neither in channels nor in broadcasting time – but in principle provides for unlimited "airtime" for every individual. Acknowledging that Internet is not a scarce commodity further implies that the scarcity argument used for content regulation of mass media cannot be used on Internet.

[81] In relation to mass media, the Commission has stressed that certain circumstances may occur in which the barring of a specific person or group may result in a violation of Article 10, either in combination with Article 14 or by itself, since the individual access to broadcasting time must not be discriminatory (X and association of Z 1972:86).

Furthermore, Internet does not have the invasive nature of broadcasting. As outlined in chapter three and stressed by the Courts, Internet is characterised by active information retrieval, where the individual makes several affirmative steps in order to process information. Also, the element of pre-warning was emphasised as fundamentally different from the element of "assault" involved in broadcasting. Using Habermas' terminology, we could argue that these characteristics of Internet communication are precisely what makes cyberspace resemble lifeworld, and what gives it its potential for strengthening the public sphere. On Internet, virtually as many people express opinions as receive them and there is a chance immediately and effectively to answer back any opinion expressed in public. This is in contrast to mass media, where a system enrolled in system codes of money and power is assigned to represent lifeworld.

Accordingly, it is misguiding to use the mass media concept on Internet. As stressed in chapter three and emphasised by the Courts on CDA, Internet is more than a new media. Internet is a commercial sphere but it is also a public and personal sphere, used by individuals when they speak, discuss, meet, or search for information. Internet is a wholly new means for human communication, which combines, adds to - and differs - essentially from previous media. When assessing the level of protection that should be provided for Internet communication it is therefore more adequate to compare Internet to physical public space than to mass media, thus provide for online expressions the highest level of protection.

6.3. Filters and the right to receive information

As illustrated in chapter four, the Court has ruled that the right to receive information prohibits a government from restricting a person from receiving information that others may wish or may be willing to impart to her (Leander 1987). The unlimited right to receive information is also implied in the CoE Declaration, referred to in chapter four, where member states have agreed to the objective of absence of censorship or any arbitrary constraints on participants in the information process, on media content or on the transmission and dissemination of information. It is also in accordance with the statements made by the Special Rapporteur. In his 2000 annual report, the Special Rapporteur states that measures to restrict online communication "on the ground that control, regulation and denial of access is necessary to preserve the moral fabric and cultural identity of societies is paternalistic, and presume to protect people from themselves" (E/CN.4/2000/63:20). The Special Rapporteur further argues that such

restrictions on individuals' right to access information are inherently incompatible with the principles of the worth and dignity of each individual (Ibid).

The Court in the Loudoun case compared Internet to a large number of publications already published and stressed that by purchasing Internet, the library has purchased all the publications contained in cyberspace. Accordingly, when the library decided to restrict access to part of the cyber publications, they took an active removal decision, thus decided to restrict the individual from receiving part of the publications already purchased. Both in Loudoun and Birkerød library, as well as CHIPA, the restriction on individuals' right to receive information is carried out through the use of filter software. As the library patrons do not have access to the blocked material, they have no means of knowing, which information is being excluded, thus which cyberspace conversations they are not allowed to take part in. Since filter software is one of the preferred means for restricting information access on Internet, let us examine the use of filter software in the light of the previous discussions.

As outlined in the CDA judgments the most recent filter software development builds on rating, thus the ability to categorise and declare information[82]. In order for rating-based filters to work, the information must be declared in the same sense, in which we categorise food or movies according to nutrition or recommended age-level for access respectively. However, if we build on the presumption that Internet is partly lifeworld, and that part of the cyber communications are taking place in a public sphere similar to speaking to people on a street corner, we begin to see the radical demand we are imposing on cyber speakers by asking them to declare their online expressions. We are thus asking them to categorise their expressions according to a meta-standard of decency. "Is this expression very harmful, partly harmful or not harmful at all"? "Does this discussion involve indecent language to a small, medium or large degree"? Recalling the distinction of system and lifeworld, we can argue that declaration of goods and services is natural when seen from a system perspective, where it meets consumer demands. However, when seen from a lifeworld perspective, it would be akin to asking people to declare their 'speak' as a precondition for speaking. As stressed in chapter

[82] Filter software can generally speaking be divided in two groups. 1) Screening programs that black or white list material according to criteria set out in the programs. 2) Programs that comply with a meta-standard such as PICS. The second group does not contain criteria themselves, but filter content according to a prior PICS rating of the material. They therefore precondition that all material is rated according to the PICS standard or equivalent (Lessig 1999:35).

four, an important feature of freedom of expression is the individual's right to express him or herself, whatever the content, free from arbitrary restrictions. Having to declare your 'speak' as a premise for speaking would surely impose restrictions on you as a speaker. Once more it depends on the perspective we have on Internet. If we acknowledge lifeworld elements in cyberspace, we should also acknowledge individuals' right to freely express themselves without having to declare their expressions in advance.

Another problem relates to the element of arbitrariness and invisibility involved in filtering. Defenders of the PICS rating scheme stress the fact that the rating standard is horizontal neutral, meaning that it allows users to choose from a variety of software products as long as these are compliant with PICS[83]. Critics stress that PICS is not just horizontal, but also vertical neutral, allowing the filter to be imposed at any level in the distribution chain. Thus, nothing in the design of PICS prevents parties that provide access to Internet from filtering content further upstream in the distribution chain; for instance at the library level, at the Internet Service Provider level, or at the level of jurisdiction, within which the user lives[84]. When using a filtered access point, Internet users have no means of knowing, which content is excluded, and in some cases they might not even know that they are subject to access restrictions.

In this respect, access restrictions through filter software are essentially different from state attempts to restrict online expressions through legislation such as CDA or COPA. Whereas CDA and COPA aim at restricting the speaker in "speaking indecent language" when minors are listening, filters aim at restricting the minor (and potentially others) from listening to a major part of the conversations going on in cyberspace. Filters are commercial products and the inherent norms can expand as broadly as the consumer wants or go as far upstream as the demand for access restriction goes[85].

Rating and filter systems can be seen as commercial attempts to codify lifeworld norms, either defined through the filter software itself (model one) or through the rating scheme (model two), hence define common moral standards on the nature of information. Since private parties define the content-based criteria for rating or filtering, the inherent norms

[83] For instance both Microsoft and Netscape have PICS-compliant filters within their browser software.
[84] "Filtering in an architecture like PICS can be invisible, and indeed, in some of its implementations, invisibility is part of its design" (Ibid:178).
[85] Currently, PICSRules 1.1 facilitate the implementation of server/proxy based filtering thus providing means of enabling upstream filtering, beyond the control of the end-user (Ibid:177)

are not transparent and have never been subject to judicial review. As long as filters are only implemented at end-user level, this is not necessarily a problem, since the user (unless she is a child) has a free choice when using the filter and the inherent norms. However, the problem arises if filters are expanded vertically and implemented at common access points. Then the user has no longer a choice, but to subject him or herself to the commercial norms of the filter thereby only gaining access to a limited part of the cyber conversations.

As stressed in the Danish debate on B46, and also in both judgments on CDA and COPA, filters are also overbroad in scope; they restrict more than intended by the inherent moral norms. Recalling the European Court's principle of non-discrimination, we can therefore argue that should authorities by legitimate means restrict individuals' right to receive information, then this restriction should be applied in a non-discriminatory fashion. The non-discriminatory principle is also part of the UNESCO Universal Service Principle outlined in chapter four, whereby Internet shall be accessible by all individuals, on a non-discriminatory basis regardless of geographic location. I would argue that applying filters to Internet access in public libraries is discriminatory in two senses.

Firstly, it discriminates against those *citizens* who have no other means of Internet access, thereby undermining the equalizing aspect of providing Internet in public libraries as stressed in the Danish IT-policy. Citizens with no access to the public sphere of Internet are currently restricted in their information access and have no other means but the physical public space to seek information and express their opinions. They are excluded from the radically stronger means of appearance on Internet, hence referred to the physical public sphere and its inherent limitations. Providing Internet in public libraries is a means for ensuring cyber-access for all. When the library restricts Internet access by the use of mandatory filters, they discriminate the citizens who access Internet through their public library by allowing them to access only a limited part of the cyber conversations.

Secondly, applying filters on Internet in public libraries also provides for discriminatory *information access*, since information is being excluded on normative grounds (defined by private parties) that are neither visible nor transparent to the individual seeking information in the public sphere of Internet. As stressed in the Danish debate on B46, in

the CDA judgment and in the lawsuit on CHIPA, filter software with built-in norms (model 1) is overbroad in scope thus restricting more content than intended by the norms[86]. But even if filters functioned perfect, we could still argue, that is it disproportionate to restrict individuals' right to receive information by technical means, that determine which legal information should be accessible for adults and which should not. The right to receive information implies a free choice on the individual to choose, which information to encounter in the public cyber sphere. Regarding minors the aim to protect them from potentially harmful is legitimate. However, even with minors filters might be disproportionate since they do not take into account the different age groups, family norms, cultural diversity and so on. The lifeworld norms, which filters attempt to standardise are anchored in the individual, the language and the culture, and will vary accordingly.

As stressed by the Court on CDA, also the rating-based filtering (model two) is problematic. Rating-based filtering function as an inclusion list, thus only material that has been subject to prior rating will be "receivable". Therefore, until all online content has been rated, this type of filtering will be discriminatory, not least against the lifeworld conversations (individuals or non-profit organizations), which are imposed a burden of rating as a precondition for appearance in cyberspace.

Following the Courts assessment in CDA and the Loudoun case, we should protect individuals' right to express themselves without the demand of rating their expression and to receive information in the public sphere of cyberspace without arbitrary information exclusion. Filter software with built-in moral criteria defined by private parties and used in public libraries, provides for discriminatory information access *and* furthermore discriminates against citizens who have no other means than to access the public sphere of Internet at their public library.

6.4. Online decency and moral standards

The problem of varying moral standards was raised in the CDA case, where the government sought to define "decency" in terms of local community standards. The Court stressed Internet's global character, and the unduly infringement on online

[86] The American organization Peacefire.org has made an assessment of five blocking programs: Cyber Patrol, SurfWatch, Bess, AOL Parental Controls, and SafeServer to examine how many sites each program blocked as "pornography", and of those sites, how many were actually pornographic. Peacefire's error rates ranged from 20% (AOL) to 80% (Cyber Patrol) (Peacefire 2000:1).

speakers if they were to comply with the standard of the community most likely to be offended by the expression. Due to the difficulty in zoning Internet speakers cannot be demanded to speak according to the standards of the community with the lowest common denominator, since they have no means of restricting their expression from entering *any* community in the public cyber sphere. Contrary to physical public sphere, the public cyber sphere is global - hence you potentially speak to a world audience.

Internet thereby accentuates the problem of varying moral standards, which the European Court up till now has dealt with in terms of a national margin of appreciation. The focus on developing ethical guidelines for participation in cyberspace, as proposed in UNESCO's Ethics Principle (chapter four), or the EU suggestion of common codes of conduct (chapter five) both point to the difficulty of varying moral standards in the public sphere of cyberspace. However, as discussed in chapter three, Internet provides the individual with stronger means of avoiding information, since information retrieval is to a stronger degree based on affirmative steps. One could therefore argue that the very nature of Internet bears part of the solution to the problem of varying moral standards on legal content - namely that Internet provides individuals with new means of seeking, but also avoiding, information.

Nevertheless, the problem still prevails when information is legal in one country and illegal in another, as illustrated by the Yahoo! example. Precisely because Internet cannot be zoned in geography, Yahoo! found no other means but to remove the Nazi material from their US servers in order to comply with the French Court order, thereby removing the information from the public cyber sphere altogether.

If the common moral or ethical standards proposed by the EU and UNESCO are implemented by private parties' self-regulation or the use of filters at common access points, it would run contrary to CoEs policy objective regarding absence of any arbitrary controls or constraints on participants in the information process, since both self-regulatory schemes and filters are potentially arbitrary in their exclusion of information. Self-regulatory schemes managed by private entities would lack the legitimacy of the rule of law and transparency, which is part of democracy. The use of filters at common access points would restrict individuals' right to freely choose, which information to receive. Hence the encouragement of private parties to increasingly self-regulate in order to provide a "safer" online environment is a problematic path seen

from a democratic perspective. This leads me to the second question of the dissertation, namely how to protect freedom of expression in a communicative sphere managed by private parties.

6.5. Regulation of cyber assemblies

The issue of cyber assemblies exemplified by Jubii and AOL touches the very core of cyberspace being a public, private and commercial sphere, but managed by private parties. The question points to the dilemma of whether to perceive cyber assemblies as public sphere - where communication is protected under the right to freedom of expression -, or whether to perceive them as privatised meeting forums, thus subject to privatised restrictions. Currently, they are services provided for in the commercial sphere of cyberspace connected to commercial content providers. Since they are privately managed, it implies a legitimate right to subject the services to restrictions; for instance by automatically altering expressions such as “dick” or “whore” in order to secure a “clean” environment. AOL and Jubii are commercial parties, and they have a legitimate right to regulate according to the codes of their system. Or do they? It all depends on whether we apply a system or lifeworld perspective.

Seen from a system perspective they are merely following the “rules of the game” – money, corporate profile and customer demand. However, looked upon from a lifeworld perspective, freedom of expression is the protection of every minority to voice her opinion, to oppose the system. This protection cannot be regulated according to system codes of money and power; the minority protection inherent in freedom of expression is simply not for sale. How would we feel if our physical public spaces were run by private parties who restricted, which expressions they would allow, and decided that certain words would be censored since they could be harmful to minors passing in the street. If there was no longer a single public place, where individuals could exercise their freedom of expression without interference from private parties.

Again, it all depends on the perception of Internet. In cyberspace the only public places to meet and discuss are cyber assemblies – since there is no “public outdoor area”. There is no exit from the privately managed sphere to a public street or park. If we perceive cyber assemblies as public sphere, where individuals can meet and voice their opinion, then we could also call for a positive state obligation to protect the right to freedom of expression in this sphere. Consequently we could argue, that private parties management

of this sphere should comply with the principles we would assign to lifeworld communication in the physical space. That is principles of diversity, non-discrimination, and rights of expression, rather than the rationale of a "decent" and children-safe environment. Alternatively, we should be aware that we are assigning cyberspaces public meeting places to a system sphere where commercial codes prevail over rights of expression. This could possibly mean that the lifeworld potential of Internet - the essentially new means for freedom of expression in the public sphere - will eventually disappear if the present tendencies in the field of self-regulation continues. If we accept that expressions in cyber assemblies (or on personal websites) can be restricted according to system codes, rather than lifewold rights of expressions, we risk loosing the public sphere, which Internet currently holds.

6.6. Regulation of access

As illustrated by the Swedish example, the expressions of Flashback were denied access to cyberspace from every Swedish Internet Service Provider. Thus the only means of appearance for the discussions on Flashback was through a foreign Internet Service Provider. This is not necessarily a problem, as long as the individual can choose another service provider. However, what if service providers on a global level decided that they did not want to host websites with certain types of content? If they all agreed on codes of conduct restricting “morally offensive expressions”. Then the minority protection entailed in the right to freedom of expression would not prevail on Internet. Then certain legal expressions would no longer have means of appearance on Internet.

The customer contract of Cybercity is another example of private parties setting restrictions on expressions. Referring to the discussion above, it is legitimate from a system perspective - but problematic when perceived from a lifeworld perspective. Again we can argue, that if this type of customer contract becomes the norm, one might fear that individuals or organisations with marginalized views - whether of a political, sexual, or religious character - will be denied access to Internet. Currently, individuals have the option to change service provider if they are being restricted. But the tendency outlined in the previous chapter is hard to ignore. Private parties such as the collaboration of GBDe increasingly engage themselves in self-regulation in order to meet the demand of their customers for a safer online environment. And governments, as exemplified by the EU, increasingly encourage this tendency of self-regulation.

GBDe has addressed content as a specific area and has designated Walt Disney as the responsible private party. Will this eventually imply that the diversity of Internet, of expressions as they exist in society, will be replaced by a Disney version of reality? Will the lifeworld elements currently present cease to exist because the reality of the new public sphere is too offensive or provoking? We need to recall that there is nothing in cyberspace that does not exist in the physical world. The variety of expressions on Internet derives from human beings. The only difference is that whereas freedom of expression in the physical public sphere has limited reach and means of appearance, the public cyber sphere is far-reaching and with stronger means of appearance, thus making the diversity of opinions more visible and accessible to everyone. In this sense we could argue that Internet gives freedom of expression practical reality. In the public sphere of Internet, freedom of expression is not merely a principle but effectively a new way for individuals to voice their opinion and seek information. This is what gives the communicative sphere of Internet its potential. But it is also the feature behind the call for content regulation, not least by private parties concerned with consumer demand.

6.7. Positive state obligation

If we acknowledge that part of cyberspace can be perceived as public sphere, the freedom to express opinions in this sphere should be entitled to protection by the state. The protection is not only a matter of non-interference by the state, but might also entail positive state obligations to protect individuals against interference from third parties as discussed in chapter four.

Even though commercial parties in principle have a right to limit, which expressions are allowed on their servers, the current development towards Internet Service Providers setting standards for the legal content allowed to be communicated by their customers is a *de facto* restriction on individuals' right to express opinions in the public sphere of cyberspace and could lead to a situation where certain discussions have no means of appearance. To draw a parallel to the physical public space would be a situation where public space was outsourced to private parties who restricted, which expressions were allowed when individuals met on a street corner, or when they spoke in a public park. The question is whether such a situation would not require positive measures of state protection in order to provide an effective respect of individuals' freedom of expression. If private parties managed physical public space, we could surely demand that it was supervised by the state in order to secure compliance with fundamental rights of the

individual.

A positive state obligation in relation to Internet Service Providers as public sphere managers, could be to secure that rights of expressions prevail in the public cyber sphere, whether in cyber assemblies or on websites. Hence restrictions from private parties should be subject to scrutiny from the state in order to secure, that the principles of freedom of expression is protected. Another aspect of the positive state obligation could be the need to secure that every citizen has means of access to Internet as a new public sphere. Recalling Habermas' description of the public sphere, we could argue that accessibility is a precondition for the public sphere. "The public sphere of civil society stood or fell with the principle of universal access. A public sphere from which specific groups would be eo ipso excluded was less than merely incomplete; it was no public sphere at all" (Habermas 1989:85). By acknowledging Internet as partly public sphere and further acknowledging that access to be in this public sphere - to express oneself and to receive information as provided for in the right to freedom of expression - is vital for democratic participation and development, we can argue that Internet access is crucial for citizens' ability to take part in society. This could call for a positive state obligation not only to protect online expressions from third party restrictions, but also to secure individuals' access to the public sphere of Internet. The positive state obligation could be to provide citizens with Internet access, for instance in public libraries. As illustrated in the previous chapter, Denmark has chosen to provide this cyber-access for all by securing Danish citizens Internet access in public libraries, while at the same time allowing a public library to restrict citizens' right to receive and seek information.

7. Conclusion

Norms codified in codes of conduct, customer contracts and/or access criteria, chat policies, or filtering systems can be effective regulators. However, with the right to freedom of expression, which is by its very nature a protection of minorities or dissenters to voice their opinion, privately defined set of norms to regulate online communication is a problematic path. Since freedom of expression is meant to protect especially those communications that shock, offend or disturb; thus the legitimate right of lifeworld to oppose system, one should be very cautious towards a development where private parties define, which conversations shall be allowed, and which shall not. Self-regulation is a dangerous path when applied to public sphere communication, since it

commercialises something that is not commerceable.

As stated above, there is nothing in the architecture of rating-schemes such as PICS, which prevents rating and filtering systems from expanding vertically. Especially in order to enforce common codes of conduct, Internet Service Providers might decide on implementing filtering systems at access level, thereby meeting the demand for a "safer" Internet for their customers. So far the Internet industry has not agreed on common means for content regulation or on common codes of conduct, but with the tendencies outlined above the call for states to take a stand on self-regulatory schemes becomes still more important. Acknowledging Internet as partly public sphere, it should deserve the same level of protection, which is provided for physical public sphere communication. The alternative is a privatised "wild west", where individuals' expressions and information retrieval is subject to arbitrary restrictions with no judicial review or democratic legitimacy.

In relation to positive state obligations, it is time for states not only to concern themselves with the protection of minors but also more generally concern themselves with the positive protection of freedom of expression on Internet. Individuals' right to freely impart and receive information within a legal frame must be protected from private parties restrictions, as outlined in the above examples. The concern for minors should be balanced with a concern for the principles inherent in freedom of expression, thus the protection of open debate, diversity and minority expressions. Furthermore, individuals' means to participate in the public cyber sphere should be positively secured, for instance by providing Internet access at public libraries.

The time when Internet was merely an alternative communicative channel has passed. Cyberspace today is an important part of living as a private and public individual in the modern world. It is a way of speaking and listening; an essential part of being human. Speaking the language of the European Court, it has strong independent significance. Accordingly, access to communicate in cyberspace should be positively provided for by states, as a natural part of democratic development and compliance with human rights.

In order to protect the communicative sphere on Internet we need to reinforce the state as protector. For the last years states have turned to self-regulation as the preferred path when dealing with potentially harmful content on Internet. However, self-regulation

potentially endangers individuals' freedom of expression because it regulates lifeworld communication according to commercial system codes. Neither the protection of freedom of expression nor human dignity can be left to private parties to regulate. The current tendency with service providers' self-regulation and commercial interests setting the scene are endangering citizens' fundamental rights. Internet is both a commercial sphere (system) and a public communicative sphere (lifeworld) and law, not arbitrary action by private partners, must protect the latter. This is the only way to ensure transparency, accountability and democratic legitimacy.

The good news is that we do not need a lot of new regulation. We have existing international standards in our human rights treaties - human rights, which are characterised by being global in scope, precisely as is Internet. The current challenge - and state obligation - is to ensure that these standards are protected on Internet, by applying the standards in the current Internet policy/regulation discussion, whether it be on freedom of expression, privacy or freedom of assembly. This is not to say that the task is easy, but the foundation is laid and the alternative unacceptable. The alternative implies in the case of freedom of expression private parties' restrictions on individuals' right to express opinions and receive information in the public cyber sphere.

With Internet we have gained new means for humans to express themselves. It is time for states to grant these expressions the same protection, which we apply to expressions in the physical world.

Bibliography

Article 19. *The Right to Communicate, The Internet in Africa*, London, Article 19, 1999.

Article 19. *The Virtual Freedom of Expression Handbook, (*http://www.article19.org).

Council of Europe. *Case-Law Concerning Article 10 of The European Convention on Human Rights,* Strasbourg, Directorate of Human Rights 1999.

Council of Europe. *Declaration on the Freedom of Expression and Information*, Strasbourg, 1982. (http://cm.coe.int/ta/decl/1982/82dec1.html).

Council of Europe. *Media and Democracy*, Strasbourg, Council of Europe Publishing 1998.

Council of Europe. *The European Convention on Transfrontier Television*, Strasbourg, 1989. (http://conventions.coe.int/treaty/EN/cadreprincipal.htm).

European Commission. *Commission Communication to the European Parliament, the Council and the Economic and Social Committee on the follow-up to the Green paper on the protection of minors and human dignity in audiovisual and information services*, COM 97, 570.

European Commission. *Communication on Illegal and Harmful Content on the Internet*, COM 96, 487.

European Commission. *Green Paper on the convergence of the telecommunications, media and information technology sector, and the implications for regulation*, COM 97, 623.

European Commission. *Green paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services*, COM 96, 483.

European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), adopted 4 November 1950, entry into force 3 September 1953.

European Parliament. *Decision No /98/EC of the European Parliament and of the Council of adopting a Multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, /98/EC.

European Parliament. *Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a Multi-annual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, 276/1999/EC.

European Parliament. *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information services, in particular electronic commerce in the Internal Market*, 2000/31/EC.

Gallagher, N. *Middle East and North Africa Human Rights Activism in Cyberspace,* Middle East Studies Association Bulletin, vol. 31, no. 1, 1997.

Gibson, W. *Neuromancer*, New York, Ace Books, 1984.

Global Internet Liberty Campaign (GILC). *Regardless of frontiers*, Washington DC, Center for Democracy and Technology, 1998.

Godwin, M. *CyberRights*, New York, Times Books, 1998.

Goldsmith, J. *Regulation of the Internet: Three Persistent Fallacies*, in "Chicago-Kent Law Review", vol. 73, 1998 (p.1119-1131).

Goldsmith, J. *Unilateral Regulation of the Internet: A Modest Defence*, in "EJIL", vol. 11, no. 1, 2000 (p. 135-148).

Habermas, J. *The Structural Transformation of the Public Sphere*, Oxford, Polity Press 1989.

Habermas, J. *The Theory of Communicative Action, Volume One*, Oxford, Polity Press,

1991.

Habermas, J. *The Theory of Communicative Action, Volume Two,* Oxford, Polity Press, 1992.

Hamelink, C. *The Ethics of Cyberspace*, London, Sage Publications 2000.

Harward Law Review Association. *The Message in the Medium: The first Amendment on the Information Superhighway,* Harward Law Review, March 1994.

Human Rights Watch. *Silencing The Net*, New York, Human Rights Watch, Vol. 8, no. 2, 1996.

Human Rights Watch. *The Internet In The Mideast and North Africa,* New York, Human Rights Watch, 1999.

International Covenant on Civil and Political Rights (ICCPR), adopted by the General Assembly of the United Nations on 16 December 1966, entry into force 23 March 1976.

Jacobs, F.G. and White, R.C.A. *The European Convention on Human Rights*, Oxford, Clarendon Press, 1996.

Klein, N. *No Logo*, London, Flamingo 2000.

Lessig, L. *Code And Other Laws of Cyberspace*, New York, Basic Books 1999.

Liberty (ed.). *Liberating Cyberspace*, London, Liberty Press, 1998.

Luhmann, N. *Social Systems* (*Sociale Systemer)*, Copenhagen, Munksgaard, 1993.

Luhmann, N. *The Reality Of The Mass Media*, Oxford, Blackwell Publishers, 2000.

Mayer, F. *Europe and the Internet: The Old World and the New Medium*, in "EJIL", vol. 11, no. 1, 2000 (p.149-169).

Ministry of Information Technology and Research, *Realigning to a Network Society*, Copenhagen, Ministry of Information Technology and Research, 2000.

Qvortrup, L. *The hypercomplex society (Det hyperkomplekse samfund)*, Copenhagen, Nordisk Forlag, 2001.

Reporters sans frontiers. *The Enemies of the Internet*, Paris, Reporters sans Frontiers, 2001.

United Nations Development Programme (UNDP), *Human Development Report 1999*, New York, Oxford University Press, 1999.

United Nations Economic and Social Council. *Report of the Special Rapporteur, Mr. Abid Hussain, submitted pursuant to Commission on Human Rights resolution 1997/26*, New York: United Nations, 1998 (E/CN.4/1998/40).

United Nations Economic and Social Council. *Report of the Special Rapporteur, Mr. Abid Hussain, submitted pursuant to Commission on Human Rights resolution 1999/36*, New York: United Nations, 2000a (E/CN.4/2000/63).

United Nations Educational, Scientific and Cultural Organization (UNESCO). *Report to the Director-General by the experts meeting on cyberspace law*, 1999.

United Nations General Assembly, 1st session, Resolution A/Res/59(1), New York: United Nations 1946.

United Nations High Commissioner for Human Rights (UNHCHR), CCPR General comment 10: Freedom of expression, 1983.

United Nations Human Rights Committee, 47th session, UN Doc. CCPR/C/47/D/359/1989, New York: United Nations, 1989.

United Nations, *We the Peoples: The Role of the United Nations in the 21st Century*, Millennium Report of the Secretary General of the United Nations, New York: United Nations, 2000b.

Universal Declaration on Human Rights (UDHR) adopted by the General Assembly of the United Nations on 10 December 1948.

Van Hoof, G.J.H and Dijk, P. van. *Theory and Practice of the European Convention on Human Rights*, The Hague, Kluwer Law International, 1998.

European Court of Human Rights

Autronic AG judgment of 22 May 1990, Series A no. 178.
Engel and others judgment of June 1976, Series A no. 22.
Groppera Radio AG and others judgment of 28 March 1990, Series A no. 173.
Handyside judgement of 7 December 1976, Series A no. 24.
Informationsverein Lentia and others judgement of 24 November 1993, Series A no. 276.
Jersild judgment of 23 September 1994, Series A no. 298.
Leander judgement of 26 March 1987, Series A no. 116.
Lingens judgement of 8 July 1986, Series A no. 103.
Müller and others judgment of 24 May 1988, Series A no. 133.
Otto-Preminger-Institut judgment of 20 September 1994, Series A no. 295-A.
Ozgur Gundem judgment of 16 March 2000 (HUDOC REF00001396).
Sunday Times judgement of 26 April 1979, Series A no. 30.
The Observer and Guardian Newspaper judgement of 26 November 1991, Series A no. 216.
X and association of Z, Application 4515/70, 1972.

French and US Courts

Tribunal de Grande Instance de Paris: "International League against Racism and Anti-Semitism (LICRA) and The Union of French Jewish Students (UEJF) v. Yahoo", decided 24.11.2000.

US Court of Appeals For The Third Circuit: “Reno, Attorney General of the United States; et al. v. American Civil Liberties Union et al.” Case no. No. 99-1324, Opinion filed 22.6.2000. Referred to as (Court of Appeals on COPA)

US District Court for the Eastern district of Pennsylvania, “Multnomah Public Library v. U.S.”, Complaint April 2, 2001. Referred to as (Lawsuit on CHIPA)

US District Court for the Eastern District of Pennsylvania: “Reno, Attorney General of the United States; et al. v. American Civil Liberties Union et al.” Civil Action no. 96-963, decided 11.6.1996. Referred to as (District Court on CDA)

US District Court for the Eastern district of Virginia: “Mainstream Loudoun, et al. v. Board of trustees of the Loudoun Country Library, et al., Civil action no. 97-2049-A, Opinion of 7.4.1998. Referred to as (District Court on Loudoun)

US Supreme Court: “Reno, Attorney General of the United States; et al. v. American Civil Liberties Union et al.” Case no. 96-511, decided 26.6.1997.
Referred to as (Supreme Court on CDA)

Newspapers etc.

ASCII Online, *GBDe Press Seminar Held*, 19 August 1999.

ACLU News Wire, *ACLU Files Challenge to Library Internet Censorship*, 20 March 2001. (http://www.aclu.org/news)

ACLU News Wire, *ACLU moves to block Filtering Law*, 19 December 2000.

ACLU News Wire, *Judge Sets Highest Legal Hurdle for Using Blocking Software in Libraries*, 17 April 1998.

Berlingske Tidende, *Get2Net introduces censorship on Internet*, 8 June 2000 (in Danish).

Computerworld Online, *Get2Net: Gone with filthy pages*”, 9 June 2000a (in Danish). (http://www.cw.dk)

Computerworld Online, *Lawyer: Get2Net on the edge of the law*, 9 June 2000b (in Danish).

Computerworld Online, *Riskær criticises Get2Net- censorship*, 9 June 2000c (in Danish).

Computerworld Online, *Indecency: Say no to closure of homepages*, 19 June 2000a (in Danish).

Computerworld Online, *Get2Net: The content on websites does make a difference*, 19 June 2000b (in Danish).

Computerworld Online, *Internet not allowed (forbudt) for children*, 22 January 2000 (in Danish).

International Herald Tribune, *Go easy on Internet, Executives Tell Governments*, 14 September 1999.

New York Times, *As America Online Grows, Charges That big Brother Is Watching*, 31 January 1999.

Politiken.dk, *Cheated on the Chat*, 12 January 2000 (in Danish).
(http://www.politiken.dk)

Politiken Internet, *The Ultimate Freedom of Expression*, 31 May 2001 (in Danish).

Seattle Post-Intelligencer, *Libraries challenge Internet filter law*, 27 March 2001.
(http://wwwseattle-i.nwsource.com)

Wall Street Journal, *Electronic commerce initiative is set by top executives at 17 companies*, 15 January 1999.

Online material

American Online (AOL) Guidelines for Groups
(http://groups.aol.com/_pub/guidelines.adp

BIAC/OECD Forum: Internet Content Self-regulation, Paris 25.3.1998
(http://www.oecd.org/dsti/sti/it/secur/act/selfreg-summary.htm)

Birkerød Library's arguments on the filter debate (in Danish)
(http://www.birkerod.bibnet.dk/filterdebat.htm)

Council of Europe; the MM-S-OD specialist on self-regulation on Internet
(http://www.humanrights.coe.int/media/events/2001/FORUM-INFO(EN).doc)

Cybercity Guidelines (In Danish)
(http://www.cybercity.dk/kundeservice/retningslinjer/)

Electronic Privacy Information Center, *Communication Decency Act: Supreme Court, Background info, Lower Court, Other materials*
(http://www.epic.org/cda/)

Global Business Dialogue (GBDe), *Paris Recommendations 1999*
(http://www.gbd.org/ie/archive/recommendations.html)

Global Business Dialogue (GBDe), *Working groups 2001*
(http://www.gbd.org/ie/index.html)

Peacefire.org, *Study of average error rates for censorware programs*, 23.10.2000
(http://peacefire.org/error-rates/)

Speech of the Danish Minister of Information Technology and Research, Ms Birthe Weiss, at the Parliament Hearing on B46, 5.12.2000 (in Danish)
(http://www.ft.dk/Samling/20001/salen/B46_BEH1_28_18_1.htm)

The Danish Library Law (Lov om biblioteksvirksomhed), No. 340 of 17.5.2000 (in Danish) (http://147.29.40.90/_MAINRF_A577196046/660)

The Danish Parliament Hearing on B46, 5.12.2000 (in Danish) (http://www.ft.dk/Samling/20001/MENU/00550064.htm)

United Nations Educational, Scientific and Cultural Organization (UNESCO), INFOethics (http://www.unesco.org/webworld/public_domain/legal.html)