INTERNET AND HUMAN RIGHTS

by

MIRIAM STARKL-MOSER

LLM Vienna, 1999

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF LAWS

in

THE FACULTY OF GRADUATE STUDIES
(FACULTY OF LAW)

We accept this thesis as conforming to the required standards

THE UNIVERSITY OF BRITISH COLUMBIA

April 2002

© Miriam Starkl-Moser 2002
In presenting this thesis in partial fulfilment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Faculty
Department of Law

The University of British Columbia
Vancouver, Canada

Date April 24, 2002

DE-6 (2/88)
Abstract

This thesis provides an overview over the existing and emerging correlation of the Internet and Human Rights with the main focus on the human right to freedom of expression. It looks at how freedom of expression is protected and curtailed at the same time by regulation in the global context and nationally and how it could be protected in the future.

Firstly, it will address general issues and problems connected with the Internet and Human Rights, like equal access to the new technology, and terrorism and the defence of freedom. It will look at the relationship of freedom of expression and other human rights, especially the right to privacy.

Secondly, it will examine the applicability of international human rights agreements and the opportunities offered by them. It will also look at the possibility of drafting a new piece of international legislation and the effectiveness of national regulation.

Although in some areas international consensus may be easier to achieve, for example in many aspects of criminal law enforcement, it is unrealistic to expect that countries with different cultural values will agree upon a single set of rules for the whole world. International harmonisation strategies are clearly an important response to the jurisdictional difficulties of Internet regulation, but they can’t be the ultimate and single solution. But national regulation faces its problems, too. Due to the character of the Internet as a transnational medium and its borderless flow of information the nation state only has limited possibilities to effectively regulate the Internet within its borders and it has to accept a loss of sovereignty in cyberspace. Although regulation in some areas may be effective, complete control is impossible which will be shown.
Thirdly, it will consider the different approaches that are available to regulate and control content on the Internet, their effectiveness and their influence on the human right to freedom of expression. It will illustrate in various examples in form of case studies the difficulties of Internet regulation. It will also provide an overview over self-rating schemes and filtering and blocking software and the problems connected with them. The liability of Internet Service Providers will be examined and alternatives to government control of the Internet will be discussed.
Table of Contents

Abstract ii
Table of Contents iv
List of Tables vii

Chapter I Overview and Summary 1

1.1 Introduction 1
1.2 Methodology 2
1.3 Summary of Findings 2
1.4 General Observations 4
1.5 The Internet 7
  1.5.1.  An Internet Primer 8
  1.5.2.  A brief history 9
1.6 Access 10
  1.6.1 The Barriers that Hinder Equal Access to the New Technologies 11
  1.6.2 Benefits of the New Technologies 14
1.7 The Human Right to Communicate 16
1.8 Internet and Human Rights 18
1.9 Freedom of Expression 20
  1.9.1 Terrorism and the Defence of Freedom 25
1.10 Privacy 29
  1.10.1 Separate but Related Concepts of Privacy 30
  1.10.2 The European Union Data Protection Directives 32
Chapter II  Human Rights Agreements

2.1 International Agreements that Manifest a Commitment to the Right of Freedom of Expression

2.1.1 Universal Declaration of Human Rights

2.1.2 International Covenant on Civil and Political Rights

2.1.3 International Covenant on Economic, Social and Cultural Rights

2.2 Regional Agreements

2.2.1 European Convention for the Protection of Human Rights and Fundamental Freedoms

2.2.1.1 Case Law of the European Court of Human Rights Relevant to the Internet

2.2.2 Charter of Fundamental Rights of the European Union

2.2.3 OSCE Commitments and Instruments Related to Freedom of Expression

2.2.4 American Declaration of the Rights and Duties of Man

American Convention on Human Rights

Inter-American Declaration of Principles of Freedom of Expression

2.2.5 African Charter on Human and Peoples' Rights

2.3 Summary of the Relative Effectiveness of these Various Instruments

Chapter III  Internet Control

3.1 General Observations

3.2 Content Control Overview

3.2.1 Convention on Cybercrime

3.2.2 Internet in China
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.3 The United States and the</td>
<td>85</td>
</tr>
<tr>
<td>Communications Decency Act</td>
<td></td>
</tr>
<tr>
<td>3.3 Self-Rating Schemes and Filtering and Blocking Software</td>
<td>92</td>
</tr>
<tr>
<td>3.4 Liability of ISPs</td>
<td>101</td>
</tr>
<tr>
<td>3.4.1 Yahoo Case</td>
<td>106</td>
</tr>
<tr>
<td>3.5 Voluntary Codes of Conduct</td>
<td>108</td>
</tr>
<tr>
<td>3.6 Hotlines</td>
<td>112</td>
</tr>
<tr>
<td>3.7 Educate and Empower Users</td>
<td>113</td>
</tr>
<tr>
<td>Chapter IV Conclusion</td>
<td>116</td>
</tr>
<tr>
<td>Bibliography</td>
<td>123</td>
</tr>
</tbody>
</table>
List of Tables

Table 1  62
Chapter I  Overview and Summary

1.1  Introduction

This paper provides an overview over the existing and emerging correlation of the Internet and Human Rights with the main focus on the human right to freedom of expression. It looks at how freedom of expression is protected and curtailed at the same time by regulation in the global context and nationally and how it could be protected in the future.

In Chapter I the context for further analysis is set. It includes a short history of the Internet and an Internet primer, definitions of freedom of expression and privacy, and it addresses general problems in context with the Internet, like equal access to the new technology, and terrorism and the defence of freedom.

Chapter II gives an overview over the existing international and regional Human Rights agreements that have helped to enshrine the right to freedom of expression world wide. It examines their applicability to the Internet with regard to their language and scope and looks at the effectiveness of their enforcement mechanisms.

Chapter III addresses the issues of Internet control, especially content control and government censorship, and what means are available to protect freedom of expression on the Internet. It looks at international legislation, like the Convention on Cybercrime, national attempts to regulate the Internet, and it illustrates in various examples in form of case studies the difficulties of Internet regulation. It provides an overview over self-rating schemes and filtering and blocking software and the problems connected with them. The liability of Internet Service Providers is examined and alternatives to government control of the Internet are discussed.
1.2 Methodology

The research for this thesis consisted of a review of primary and secondary literature, including (but not limited to) government and multilateral organisation reports and statements, papers, reports and statements of NGOs, periodicals and newspapers, academic writings, and books. This included heavy reliance on the wealth of material available on the Internet.

1.3 Summary of Findings

To protect human rights and freedom of expression on the Internet it won't be enough to just draft a new piece of international legislation to regulate the Internet. Although in some areas international consensus may be easier to achieve, for example in many aspects of criminal law enforcement, like the fight against child pornography online, or cybercrime, it is unrealistic to expect that countries with different cultural values will agree upon a single set of rules for the whole world, even a set of lowest-common-denominators. Furthermore, international agreements tend to emphasise commercial interests, especially with the rise of e-commerce and the expansion of the global economy international organisations. They do not generally recognise the broader values of cultural, social, political, or artistic activities. Rights accorded under national laws may not be recognised by international legislation. International harmonisation strategies are clearly an important response to the jurisdictional difficulties of Internet regulation, but they can't be the ultimate and single solution.

But national regulation faces its problems, too. Due to the character of the Internet as a transnational medium and its borderless flow of information the nation state only has limited possibilities to effectively regulate the Internet within its borders and it has to accept a loss of sovereignty in cyberspace. Although regulation in some areas may be
effective, complete control is impossible which will be shown. Despite this fact we should keep in mind that there are good reasons for regulatory differences among nations. A primary virtue of decentralised law making by nation states is that it allows populations to implement policies that reflect these differences. Still, single national regulation won't do either due to the global structure of the Internet as mentioned above.

Therefore it is necessary to combine many different approaches. Governments, International Organisations, NGOs and users have to work together to achieve the goal of protection of human rights and freedom of expression on the Internet.

If international agreements are established their application and implementation has to be watched carefully to ensure that fundamental human rights and the free flow of information on the Internet are protected. It is also necessary to reaffirm the support for the existing international and regional human rights agreements and promote public awareness of the protections granted in these agreements.

The development of new technologies to enhance the protection of privacy and personal data should be encouraged. Efforts by governments to restrict access to information on the Internet or to limit the distribution of information on the Internet in form of government censorship should be opposed. The decision to choose filtering and blocking software to limit access to certain information should stay with the individual user.

The strengthening of the public voice and the active participation of civil society are also central to the protection of human rights and freedom of expression on the Internet. Users become empowered through education and awareness of their rights. The work of NGOs should be encouraged. They bring a public voice to emerging digital
age issues and successful policies for the Internet must include the voices of users in order to be most effective.

1.4 General Observations

The end of the 20th century and the beginning of the 21st brought a lot of changes and new developments with it. The ongoing process of globalisation of the economy, whether one likes it or not, and the new communication technologies challenge the existing structures in which we organise our society and ask for new creative approaches in governance and legislation. They also challenge the mind, imagination and creativity of each human being in understanding and adjusting to these new developments and processes.

Since the Internet has become a global medium many expectations and hopes have been put into it. It will promote democracy through facilitating participation in government and expanding access to government information, it will strengthen civil society through the building of networks among individuals, and it will broaden access to traditional media and promote pluralism. Information and knowledge will be available for everybody. But with all this enthusiasm we should not be short sighted and not only look at the promises the new technology brings, but also see some of its dangers.

Technology in all forms is only a means. Having access to information does not per se mean that people will learn more, increase their knowledge and become more intelligent, or better persons. The advantage of having access to on-line resources is an undeniable advantage for today's students. But learning is still a human activity in which the interaction between teacher and student is very important.
The new technology was created by people who grew up and were educated in the “old” world of books and a certain kind of education. We come to the information offered on the ‘Net with this experience. But the new generation, which has only in part experienced that kind of education, and depends for its primary learning on the new technology, is likely to be effected very differently. The assumption that there is no problem for these users simply because they are fluent users conversant with the new tools, is very dangerous.¹ This danger lies in the unmediated character of the Internet. Freedom of expression – if and when misused – can sadly entail dangerous misinformation of the individuals. Through its unique feature as an active medium everyone can be a publisher and post anything, from scientific research to gossip and lies. On the ‘Net you will find no criteria by which one can decide if the information provided is useful or true. If you have no help, no editor or educator, you are left alone to make up your mind.

Another feature of technology is that it has always been a tool of human interests and human objectives, which tends to mirror the society, which invents it. We look to cyberspace to solve problems that have been created in the “real” world and may encounter that we cannot find a solution.² We are often blinded to the consequences of our actions in the offline world and the same might happen online.

One example is the so-called “digital divide”. Despite many efforts to close the technology gap between the developed and the developing world, the new medium has not done much to overcome inequality. The majority of Internet users is still located in the developed world, because using the new technology not only depends on access to hardware and software, but also on so simple things like literacy. Giving the illiterate computers won’t make them literate.

¹ B.R. Barber, “Which technology for which democracy? Which democracy for which technology?” (Winter 2000/2001) 6 International Journal of Communications Law and Policy at 1
² ibid. at 2
Another example is the belief that the Internet paves the way to reviving participation in politics and therefore promotes democracy. Especially in western countries the fear of a further decline in the turnout of elections and growing voter apathy has led to numerous initiatives promoting the Internet as a political tool. Without doubt, the Internet provides opportunities for people to participate in forums and discussions over issues that concern them. But simply setting up a forum where politicians and the public can participate in dialogue and engage in the political process is no more than a technical fix and doesn’t necessarily mean that people will log on. The fundamental question why people shy away from political engagement is neglected. The Internet is just a communications tool. If people want to participate in politics, they will choose to do so with little regard for the technology of the times.3

We also live in a largely commercialised world which is very much reflected on the Internet. When we take a look at the history of the Internet we can see that until the 1990’s, when commercial players discovered the enormous potential of the ‘Net, it was of limited interest to the public. Today probably 95 % of the traffic on the Internet is commercial, which is controlled by the same players that control the commerce in the “real” world. E-commerce doesn’t make the difference! The only real advantage is that even more potential consumers can be reached world wide to increase profit, and further project our western, commercialised image around the world.

Different technologies also imply different political possibilities that depend on the social context. The invention of the internal combustion engine and the automobile is associated with the freedom and individuality of American culture. In Europe the same invention led to the development of diesel engines and public transport systems. The decision between investment in public or private transportation was also a political and

not only technical one. We have to be aware of the fact that available technology always serves both sides of a policy debate.

Despite the interactive character of the Internet, it can be very isolating. We can send e-mails, participate in chat rooms, and discussion forums, shop online, or work from home, therefore we increasingly use the computer alone in private, that means, in an office, at home, behind a screen, which leads to social isolation. We can talk to people across the world via the Internet, but the question is: “Do we really have something to say?”

It is undeniable that the Internet is an important new channel through which communication, ideas and knowledge can flow. But technology is always a cold and neutral medium. The people, who use it, bring it to life. If the new medium shall be everything its inventors aimed for, we can’t just lay back and enjoy the possibilities the new technology brings. The debate has to continue and look at the social and cultural impacts the Internet will have in the future.

1.5 The Internet

A short history and an Internet primer to set the context and to clarify some terms used in this thesis. The terms Internet, Cyberspace and the Web or Net are used interchangeably for the purpose of this thesis although I know that they don’t necessarily always mean the same.
1.5.1 An Internet Primer

What is it?

The Internet is a global connection of networks connected and sharing information through a common set of protocols. It allows computers attached to the networks to communicate openly and effectively regardless of make, architecture, operating system or location. All resources and network management are widely distributed.

Who owns and controls it?

There is no owner of the Internet. Each network in the collection of interconnected networks is in charge of its own area, each is owned by distinct stakeholders, and all work together according to a common set of rules and standards. There is no central point of control and it has no single central governing body.

Who are the providers?

Internet Service Providers (ISPs) provide the public with access to the Internet. Users, who may be individuals or companies, contract with these ISPs for a dial-in or dedicated connection to the provider's equipment, which then gives them access to the Internet. The ISP may be a private for-profit organisation, a non-profit community organisation, an educational institution, or a government agency. Any user may be client or host, that means you may be accessing information or supplying it.

---

The Web or WorldWideWeb (www)

The Web is the visual component of the Internet. It is a virtual space of information. Connections are hyperlinks, which are links between documents. Web pages can include text, pictures, sound clips, video, and much more. The Web makes the Internet more useful because people can get information from thousands of locations without having to know about the technical architecture of the network.

1.5.2 A Brief History

The first research into internetworking technologies occurred in the 1960's at various US universities and research institutions. The goal of the research was to create a communication system that operates so randomly that it would not be possible to shut it down or prevent transmission of messages even if some of its nodes (computers linked by it) were blocked or damaged by sabotage, attack, or covert operations. This means that the Internet was designed to insure that messages transmitted through it would reach their destination in any event.

The initial network was called ARPANET and it grew slowly in the early 1970's. The membership consisted solely of universities and research labs. In the 1980's the development of the Transmission Control Protocol/Internet Protocol (TCP/IP) standard, of name servers, and electronic mail standards led to a network growth. Despite those factors it was of limited interest to the public and still a non-commercial network.

The massive entry of commercial players in the 1990's that discovered its enormous potential, which results from its capacity to carry multi-media messages into the world, transformed a former secret, closed technology into a pervasive, open, uncontrolled system spanning the globe.

Some of the multitude of possibilities offered to users of the Internet for communication or transferring information include: person-to-person e-mail, moderated or unmoderated discussion and newsgroups, facilities for posting and transferring files, and reading or viewing files of printed or kinoaudiovisual material, and the WorldWideWeb (www), which permits the display and online manipulation of all varieties of material, online radio and TV broadcast, online libraries, online shopping etc.\(^6\)

The Internet offers people, at least in the developed world and more and more in developing countries, the means to gather information and participate in activities on a much larger scale than in the past. It offers an open and democratic forum for interactive discussion on any subject and allows a wide public use. The transmission of information and knowledge is no longer restricted to a privileged group who controls the media, like television or print media.

1.6 Access

The idea that the Internet has made the world smaller by making communication between people around the world easier and faster and that the planet has become a global village is a common phrase often used nowadays. Everyone has a right to

access cyberspace and be part of the information society. Unfortunately, this cliché is not quite accurate if you take a closer look.

The typical internet user worldwide is male, under 35 years old, with a college education and high income, urban-based and English-speaking – a member of a very elite minority globally.\(^7\)

In addressing the problem of freedom of expression and content control in terms of censorship on the Internet, the discussion focuses on how they impact on a minority only. Therefore it has to be said that issues of freedom of expression and the Internet must also address the fundamental fact that a majority of people by not having access to the new technology is being effectively silenced. Today 79% of Internet users live in OECD countries, which contain only 14% of the world's people.\(^8\) There are more Internet hosts in Finland than the whole of Latin America and the Caribbean, more in New York City than on the entire continent of Africa.\(^9\)

1.6.1 The Barriers that Hinder Equal Access to the New Technology

Many inventions that are decades old have not been fully adopted around the world despite their enormous potential. Electricity has not reached some 2 billion people, a third of the world's population. In 1998 average electricity consumption in South Asia and Sub-Saharan Africa was less than one-tenth that in OSCE countries. Although the telephone has been around for more than a hundred years there is still a great disparity in its distribution. The term “universal service” was first used by Theodore Vail, the

---


President of AT&T in the 1910 Annual Report of the company. He referred to universal service to having a phone and affordable phone service in every home.\textsuperscript{10} While there is more than one mainline connection for every 2 people in OSCE countries, there is just 1 for every 15 in developing countries—and 1 for every 200 in the least developed countries. Such differences impede Internet access and hinder connections to the network age.\textsuperscript{11}

Although recent investments in infrastructure, institutional reforms and innovations in technology have accelerated the spread of electricity and telephone connections there still remains another very important factor, and that is cost.

At the very least, a potential Internet user needs a reliable source of electricity, a telephone line and a computer plus a modem to access the Internet. These requirements impose in many parts of the world a tremendous financial burden on potential Internet users. In China, for example, the fee for a phone line can be close to US$ 600, however the annual average income in China’s urban areas is only about US$ 375.\textsuperscript{12} Even if one has a telephone connection, the low number of service providers forces users in some developing countries to rely on calling international providers. Yet, international phone calls are much more expensive.

The cost of computers and modems are also several times higher in developing countries than in developed countries, because they have to import high-tech products and this increases the price. While some developing countries, like Korea, Malaysia or Mexico are using the latest technology competitively in manufacturing industries,


\textsuperscript{11} supra note 2

shown by their success with high-tech exports, in Sub-Saharan Africa, the Arab States and South Asia high-tech exports still account for less than 5 per cent of the total exports.\textsuperscript{13}

Not to forget a third major factor: knowledge. I don't specifically refer to the knowledge needed to get the computer working and how to use the Internet to get all the information you want. I think it starts at the very basics. If one can't read or write what use is a computer anyway? Another barrier in this context is language. If you look at the history of the Internet you will see that it was developed in Northern America, therefore the main language of the Internet is English. So for those who wish to access the Internet at least basic knowledge of English is a prerequisite, which requires a western-influenced education. This can lead to an erosion of cultural identity, national values and cultural integrity through standardising cultures.\textsuperscript{14}

Still, Internet use is exploding even in developing countries. In Brazil the number of users climbed from 1.7 million in 1998 to 9.8 million in 2000, in China from 3.8 million to 16.9 million and in Uganda from 2,500 to 25,000. Yet because they are starting from a very low base, the portion of population reached retains very small.\textsuperscript{15}

But the diffusion of the Internet has not only been uneven between countries. It also has been uneven within countries. Even in the developed world internet use is still concentrated. In most countries Internet users are predominantly:\textsuperscript{16}

\begin{itemize}
  \item \textit{Urban and located in certain regions}: In China the 15 least connected provinces, with 600 million people, have only 4 million Internet users – while Shanghai and
\end{itemize}

\textsuperscript{13} supra note 7
\textsuperscript{14} J. Everard, \textit{"Virtual States, The Internet and the boundaries of the nation-state"}, (London: Routledge, 2000) at 23
\textsuperscript{15} ibid.
\textsuperscript{16} ibid.
Beijing, with 27 million people, have 5 million users. In Thailand 90 % live in urban areas, which contain only 21 % of the country's population.

- **Better educated and wealthier.** In Chile 89 % of Internet users have had tertiary education, in Sri Lanka 65 % and in China 70 %.

- **Young:** Younger people are more apt to be online. In Australia 18 – 24-year-olds are five times more likely to be Internet users than those above 55.

- **Male:** Men make up 86 % of users in Ethiopia, 70 % in China and 67 % in France, to give some examples.

1.6.2. **Benefits of the New Technologies**

The benefits of the new technologies are just beginning to emerge. The Internet increases access to information and communication, breaks barriers to knowledge and participation. Modern communications are widely perceived as vital to international competitiveness. Therefore it is a prime concern of many countries, developed or developing, to spread Internet access as rapidly as possible to an increased number of communities across the nations. But can these benefits reach poor people?

The potential is only beginning to be explored. Initiatives at the global level, like the Digital Opportunities Task Force, or dot force, is a collaboration of the G8 Group of Nations, the developing countries, the private sector and NGOs. It will provide a vital co-ordinating mechanism for efforts to bridge the global digital divide.\(^{17}\)

\(^{17}\) supra note 8
Such initiatives hint at tremendous possibilities:

Political participation may be redefined by the creative use of two-way communications. Greater transparency in planning and transactions can make markets and institutions work better. Further benefits of these new technologies will depend on the development of low-cost, easy to use devices and the set up of providing access through public or market centres in developing countries, especially for poor users.

Some concrete examples:

- Inventive use of the Internet may lead to increasing income in developing countries. Farmers, for example, are getting information such as market prices, which enables them to negotiate better.

- Where health problems are rooted in lack of information, new solutions are emerging. Healthnet is a network launched in 1989 for health care professionals – especially in remote areas – in Africa, Asia and Latin America. It enables them to procure equipment efficiently, co-operate with medical institutions world wide and provide information on emerging outbreaks.\(^\text{18}\)

- In attempts to narrow the technological divide between rich and poor many governments of developing countries have opened “infocentres”, offering free public access to the Internet. In Venezuela, for example, the Ministry of Science and Technology has set up 240 such “infocentres” – each of which consists of a number of personal computers, printers and scanners – in libraries, museums, art galleries,
parks and other public spaces.\textsuperscript{19} The aim is to bring the Internet to the people, to those who have no computer at home or cannot afford Internet access.

\subsection*{1.7 The Human Right to Communicate}

Communication as a human right, distinct from freedom of expression, has been discussed in context with universal access. The Right to Communicate has received increasing focus with the 50\textsuperscript{th} anniversary of the Universal Declaration of Human Rights. The development of a global information infrastructure has increased the need to establish global recognition of the Right to Communicate and the Communication of Rights. Although a universal Right to Communicate has yet to become a part of accepted international law, there are several initiatives which are promoting the discussion globally.\textsuperscript{20}

Communication in this context is defined as a democratic and balanced dialogue between two or more parties. Essential elements of a right to communicate are the right to hear, to be heard, to inform others and to be informed. Individuals may live in a society which grants freedom of expression, but which places heavy restrictions on access to media necessary to convey expression. People may want to protest the violation of rights, but are unable to access media. The right to communicate, thus, can be defined as a universally recognised legal right, which if not granted would cause the lives and livelihoods of human beings and communities to be impeded or harmed. It differs from freedom as a right insofar as that a freedom is not imperative to be exercised in order to avoid impeding the lives and livelihoods of human beings. Freedom of expression can be seen as addressing the formulation and content of

\textsuperscript{19} M. Pineda, "Communication-Venezuela: "Infocentres" Bring Internet to the People" (2001), online: IPS-Inter Press Service <http://www.oneworld.org/ips2/aug01/17_58_052.html> (date accessed: 4 April 2002)

\textsuperscript{20} See for example: online: <http://compositive.uqam.ca/videaz/indexen.html> or <http://soeweb.syr.edu/thefci/tashcom.htm> or <http://www.pccharter.net/> (date accessed: 4 April 2002)
communication, whereas the right to communicate addresses both the critical day-to-day communications needs of people, and a right necessary for the protection of other rights. Communication is a basic human need because it is a fundamental social process necessary for expression and all social organisation in civil society.\textsuperscript{21}

An early basis of a human right to communicate is supported by three provisions of the Universal Declaration: Article 19, Article 27 section 1, and Article 28. Such a right should support the principles of pluralism, direct communication flows within a society without external control, social function, media analysis, and appropriate use of technology.\textsuperscript{22}

The question is if the implementation of a human right to communicate in the framework of international human rights would help the cause of providing universal access to Cyberspace or if it would just be another right to discuss upon?

Most human rights instruments include freedom of thought, belief, opinion and expression; including freedom of the press and other media of communication. But this reflects an outmoded concept of communication as only encompassing a traditional one-way mode. Incorporating a right to communicate into those instruments would provide a process for considering not only universal access, but important related issues of freedom of information, such as intellectual freedom, intellectual property rights, language rights, and cultural identity.\textsuperscript{23} It has become increasingly evident in this context that we need to recognise and affirm cultural rights as human rights.

\begin{flushright}
\textsuperscript{22} ibid.
\end{flushright}
1.8 Internet and Human Rights

In the past half-century human rights have been established, promoted, and protected through numerous international and regional declarations, treaties and agreements. Most states and governments are eager to assure and reassure their commitment to human rights to the public. Success has been variable.

The real task lies in the enforcement of human rights. There are still many countries, which violate human rights and do not live up to their promises made in the international arena. Monitoring the implementation of human rights treaties and exposing violations is really an exercise in democracy. There is no international "human rights enforcement troop" which would be able to exercise coercive power on an international level, like the police on the national level. States can't be arrested and put in jail for their actions. The enforcement of human rights works through the means of political and social pressure. States who violate human rights are put in the pillory and exposed in the international community. Non-governmental organisations (NGOs) also play a very important role in identifying and revealing human rights violators and reporting them to the international community.

Therefore information is the main means of action. New information technologies and new media permit one to break down walls and censorship barriers of authoritarian regimes and help to report human rights violations more efficiently. Among the first to use the Internet were human right activists. In 1992, the International Freedom of Expression eXchange (IFEX) was established to provide accurate and timely information regarding censorship and attacks on journalists.24 Pictures and words,

---

testimonies of atrocious human rights violations around the world, can reach a broader audience than ever on the Net.

The Internet has also considerably widened the field of gathering information and of investigation, opening up many windows on until now invisible or inaccessible information sources. With the introduction of search engines and the help of relay organisations like Human Rights Internet, the Internet has greatly facilitated the perusal of data bases, and the location of documents, experts, and witnesses. Web sites set up by international organisations and NGOs offer great resources and links if you want to find out what's going on in human rights.

The Internet has also opened up a new field of struggle for human rights. Those in power are fearing the new possibilities offered by the Internet and censorship directed against the new medium has appeared in several forms, which will be further explored in this thesis. Advocating freedom of expression and the protection of privacy on the Internet has become necessary to ensure the free flow of information on the Internet.

There is one thing, however, that should not be overlooked. Events, like the ones in Bosnia or Rwanda a few years ago, showed the limits of information. Despite hundreds of hours of footage, public opinion and governments were not disturbed by ethnic cleansing and genocide. The century's first genocide, the massacre of the Armenians, occurred in the highlands of Anatolia, practically without witnesses; the century's latest atrocities were committed in front of the world's eyes, in prime time, in the new era of information technology. Despite all the positive effects the new medium has, it seems that the human rights movement still needs the participation and the support of people in the “real” world to be most effective. To motivate a passive public and to show the

26 ibid.
deeper and universal values contained in human rights, sitting in front of a computer is simply not enough.

1.9 Freedom of Expression

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

Universal Declaration of Human Rights, Article 19

Freedom of expression as a human right is well enshrined in our society and is an essential component to guaranty human freedoms and dignity.

The right to free expression arose in the 17th century in response to intrusive, authoritarian governments. It was conceived of as a "negative right": All individuals were to be free from government interference when speaking. There are two rationales for extending the guarantee widely. The first is instrumental in nature and is reflected by the metaphor of the "marketplace of ideas." Suppression of ideas in the name of truth is notoriously dangerous.

It is believed that the free flow of ideas is the best way to get at the truth. The second rationale values expression less for the results it produces than for its intrinsic worth to the individual. Expression is seen as a vital element of individual autonomy, personal growth, and self-realisation. The ability to say what one thinks and to follow whatever

lines of inquiry that occur to one’s imagination is an essential attribute of a free society. The First Amendment to the Constitution of the United States stipulates that “Congress shall make no law...abridging the freedom of speech, or of the press, or of the right of people peaceably to assemble and petition the Government for a redress of grievances”. Does that mean that freedom of expression is absolute and it precludes any law limiting what individuals can say or publish? The answer is surely no. To take a familiar example, freedom of expression does not protect the right, falsely, to shout “Fire!” in a crowded theatre. That means, freedom of expression is not absolute. There are situations in which the freedom of the individual must be curtailed so that other important social values can be protected.

The American approach has been to accord near-absolute respect to expression deemed worthy of the constitutional guarantee; however, the American courts define freedom of expression narrowly so as not to include forms of speech that do not qualify for protection.

The Canadian Supreme Court has adapted a different method to reconcile respect for this vital freedom with competing claims. It has said that the structure of the Charter, and in particular section 1, requires that freedom of expression be given a broad definition with virtually no limitations, and that any curtailment of expression be justified under section 1 as a limit that is reasonable in a free and democratic society.

---

29 Schenck v. United States, 259 U.S. 47 at 52 (1919), Holmes J.
30 supra note 28
31 ibid.
32 ibid.
33 In Irwin Toy Ltd. v. Quebec (A.G.), [1989] 1 S.C.R. 927, 58 D.L.R. (4th) 577, the Supreme Court described in a formal manner the framework for interpretative analysis to be followed in a freedom of expression case. There are three stages, and given the generous scope of the definition of expression used by the Supreme Court most claims for Charter protection will survive stage one and two. There remains, however, the third stage of analysis under section 1 of the Charter. Here the burden is on the state to justify the limit it seeks to impose as being reasonable in a free and democratic society.
The demands for the regulation of the Internet have also raised the spectre of censorship, which has always been a weapon of the state to silence those voices it doesn’t want to be heard.

Arguments both for and against the regulation of Internet content may be drawn from classical liberal ideas. Mill’s “On Liberty”\(^{34}\) offers a useful source of concepts and methods, which have been used by both sides in the debate. But it is principally the defenders of the free flow of information who have deployed Mill’s notion of moral independence, his plea for toleration and analysis of the link between freedom of thought and freedom of publication, and his focus on the importance of a range of opinions for social and individual improvement, to allow for the possibility of learning through errors and experience. The Millian commitment to freedom of opinion and freedom to publish is a bulwark for civil libertarians.

Since the earliest times freedom fighters have relied on information, print, and images as a preferred weapon, because the more people that can be informed and won for a certain cause the better. The advent of new technologies, like television or the Internet, have increased the number of people that can be reached. Information is the main means of organisations involved in the struggle for democracy and the protection of human rights. Therefore it is no surprise that human-rights advocacy groups were among the first to use the advantages of the new information technologies and turn them against authoritarian regimes.\(^{35}\)

The evolution of freedom of expression has more or less paralleled the development of the media and techniques for the production, storage, and distribution of information. But it seems that people always have been concerned about who reads what and gets

---


\(^{35}\) for example: In 1992, the International Freedom of Expression eXchange (IFEX) was established to provide accurate and timely information regarding censorship and attacks on journalists.
which information. Even Plato expressed concerns about access by people who were not “suitable” for the material presented.36 Therefore at each stages of the development of the media, mechanisms of control were created, in most cases by states, not only to protect so-called “public interest”, but also because new media often get involved in struggles for new freedoms.37 Those in power fear the threat of people trying to extend their political and social rights.

Traditionally, there have been four principal means of restricting freedom of expression:38

a) Legislation regulating content

The most common legal form to curb freedom of expression are censorship laws which make it illegal to write, publish, or disseminate content, which is considered “illegal or harmful” by the legislators. When legislation is enacted, it means that the state can use its power of coercion legally to enforce these rules. Penalties and enforcement vary, they include warnings, suspensions, fines, imprisonment, etc. Despite the fact that the guarantees of freedom of expression today are enshrined in many international human rights treaties and therefore protected by international law, in many countries around the world regulatory frameworks39 are promulgated which are not in accord with these agreements. Although governments of democratic countries avoid open censorship laws, even there hidden ones may be found.

36 Plato, “Phaedrus and Letters VII and VIII”, (Harmondsworth: Penguin Classics, 1973) “[o]nce a thing is committed to writing it circulates equally among those who understand the subject and those who have no business with it; a writing cannot distinguish between suitable and unsuitable readers. And if it is ill-treated or unfairly abused it always needs its parent to come to its rescue.”
38 Ibid.
b) Administration

A second type of censorship used is administrative in character. These measures may include obligations to register, to obtain authorisation for publication (licensing), or to deposit financial guarantees. Through lengthy administrative procedures and a high level of bureaucracy potential new media can be hindered or even avoided.

c) Violence

If legal means of coercion cannot silence unwelcome media, beating, kidnapping or arbitrary arrest of journalists and media personnel are still common in some countries.

d) Economic pressure

This efficient way of controlling the media has a long history. In 1712, in a move intended to silence a wave of fresh criticism in the press, the government of Queen Anne in England imposed four taxes on pamphlets and newspapers. These taxes were clearly intended to put the press out of the financial reach of the majority.\textsuperscript{40} Today economic pressure is applied, for example, through charges of high registration fees for ISPs or Internet users, high licensing fees for broadcasting stations, etc.

The advent of the digital era and the Internet has brought a new way of curbing freedom of expression. For the first time, technology can be used as a means of censorship, the instruments of control can be directly integrated with the medium.\textsuperscript{41} Through filtering and blocking software information can be destroyed even before the potential user even knows that it exists. This serves political authorities extremely well,

\textsuperscript{40} supra note 37
\textsuperscript{41} ibid.
because it allows them to control the flow of discourse and information on the Internet invisibly, permanently and globally.\(^\text{42}\)

While during the Inquisition in Italy and Spain book-burning scenes of seized books, which were prohibited by the authorities, in public spaces were laden deliberately with symbolism to stir up fear and obedience amongst the public, the current trend in censorship methods is to be increasingly invisible to be more efficient.\(^\text{43}\)

1.9.1 Terrorism and the Defence of Freedom

On September 11, 2001 thousands of people tragically lost their lives in a brutal terrorist attack on the American people and the American form of government. We still mourn the loss of these innocent lives and have to insist that those who perpetrated these acts be held accountable.

But this tragedy also requires us to examine carefully the steps countries are taking to reduce the risk of future terrorist attacks. Authorities instil within society a culture of fear, leading people to accept that their rights – and the rights of others – be trampled on for the sake of the fight against terrorism and the common good. They accept the loss of rights they have been fighting for, like the right of privacy, and a state of surveillance they would otherwise not accept.

Politicians were fast to play the “terrorist card” to justify stealth measures of control not only on the Internet and to call the Internet a “terrorist network”. No longer is it enough

\(^{42}\) See for example: Chapter III, 3.2.2 Internet in China at 81
\(^{43}\) supra note 37
that the Internet is full of child pornography, dot-con artists, and hackers, it is also being used as a means of communications amongst terrorist organisations.\footnote{J. Horvath, "The Internet: A Terrorist Network?" (Munich: Verlag Heinz Heise, 2001) in Telepolis, Magazin der Netzkritik online: Verlag Heinz Heise Homepage <http://www.telepolis.de/english/inhalt/te/9350/1.html> (date accessed: 23 April 2002)}

When US President Bush signed the USA Patriot Act\footnote{H.R. 3162, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001", 1\textsuperscript{st} session, 107\textsuperscript{th} Congress of USA, 2001; online: Thomas, Legislative Information on the Internet <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:> (date accessed: 8 April 2002)} into law on October 26, 2001 he significantly boosted the government’s law enforcement powers while continuing the trend to cut back on the traditional checks and balances provided by the Constitution to protect civil liberties. Among the USA Patriot Act’s most troubling provisions\footnote{ibid., Title II, Sections 201-217} are measures that minimise the judicial supervision of federal telephone and Internet surveillance performed by law authorities and expand the ability of the government to conduct secret searches. It extends the use of the FBI’s e-mail interception system, known as Carnivore, and the National Security Agency’s Echelon surveillance system by establishing a very low threshold of proof for access to Internet communications that are far more revealing than numbers dialled on a telephone. The provision apparently applies to law enforcement efforts to determine what web sites a person has visited, so the low standard of proof is extended to actual content information.\footnote{American Civil Liberties Union (ACLU), "USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances" (2001) (Legislative Analysis) online: ACLU <http://www.aclu.org/congress/1110101a.html> (date accessed: 4 April 2002)}

Plans to ban strong encryption systems on the grounds they limit the ability to conduct searches and execute wiretaps have been dropped after industry pointed out the devastating impact such laws could have on business and e-commerce. After all, the vast majority of cryptography users today are not terrorists and drug dealers but businesses. Encryption protects consumers making purchases over the Internet.
Other countries followed the example of the United States and also enacted tough new legislation to fight terrorism. In Canada, for example, Bill C-36\(^{48}\), the Anti-Terrorism Act, received royal assent on December 18, 2001. The Act will give law enforcement new investigative tools to gather knowledge about and prosecute terrorists such as enhancing the ability to use electronic surveillance. The Criminal Code has been amended to eliminate online hate propaganda\(^{49}\) and the Canadian Human Rights Act was amended to clarify that the prohibition against spreading repeated hate messages by telephonic communications includes all telecommunications technologies.\(^{50}\) And although the government ensures that the Act contains rigorous safeguards to uphold the rights and freedoms of Canadians it also was heavily criticised by civil libertarians and human rights activists because of its impact on civil liberties.

Only the European Union ignored a request by the Bush administration to revise a data-protection law it was drafting to allow authorities greater access to information about telephone calls and Internet messages.\(^{51}\)

And, after all, the question remains: Will tougher laws and more law enforcement power make the world a safer place? For several decades, electronic systems have been quietly put in place to intercept satellite communications, phone calls, monitor e-mail and Web traffic. What happened to those high-tech surveillance tools like Echelon or Carnivore that were supposed to provide early warning needed to thwart out terrorist plots?

---

\(^{48}\) Bill C-36, An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism, 1\(^{st}\) session, 37\(^{th}\) Parl., 2001 (assented to 18 December 2001, S.C.2001, c. 41)

\(^{49}\) ibid., Part 1 cl. 2 sec. 23, 31-34


Echelon is said to be the most comprehensive and sophisticated global surveillance network, yet officially unacknowledged. It reportedly has the capability to monitor every communication transmitted by satellite outside of U.S. borders. According to a European Parliament report released in September 2001, Echelon collects information through a complex web of radio antennae at listening stations across the planet. Investigations cited by the ACLU and others report that Echelon rakes the immense volumes of data it collects through dictionary software that operates on a vast computer network hosted by intelligence agencies of five countries – the United States, Great Britain, Australia, Canada and New Zealand. Echelon has supposedly been used to churn data into knowledge about foreign governments, corporations and even specific individuals since the 1970s. Subjects of surveillance are reported to have even included the likes of Princess Diana, whose work eliminating land mines ran counter to U.S. policy.\(^{52}\)

Another government snooping technology is Carnivore which is devised to intercept data traffic sent over the Internet to assist federal authorities in criminal investigations. In theory it is only installed with the co-operation of an ISP and after obtaining appropriate judicial approval to track e-mail, instant messages and Web search trails. The system inspects only those communications that are legally authorised for interception. But it could be used to monitor much more than that civil liberties organisations worry; at least it opens formerly locked doors to enforcement authorities.\(^{53}\)

It also has to be noted that law enforcement authorities in many countries even before September 11\(^{th}\) already had broad measures in place to fight not only against terrorism but drug dealing and organised crime. So, how could a band of terrorists, including

\(^{52}\) K. Hogan, "Will Spyware Work?" MIT Technology Review (December 2001) 43 online: Technology Review Homepage <http://www.technologyreview.com>

\(^{53}\) ibid.
many already suspected as such, operate within those systems for years and still escape detection – undoubtedly making phone calls and exchanging e-mail messages?

Well, even the most advanced spying technologies and toughest laws can’t guarantee success when pitted against the malevolent combination of human ingenuity and capacity for evil. As with drugs trade, child pornography, and other such clandestine networks, those involved in illicit activities will always find a way to operate and communicate with one another – with or without the Internet. The capacity of turning the world into a surveillance society the likes of which we have never seen before clearly exists. But we should not let politicians use the fight against terrorism as an excuse to clamp down on civil liberties and further restrict the flow of information on the Internet.

1.10 Privacy

Privacy is a fundamental human right recognised in all major international treaties and agreements on human rights. The protection of privacy and all its aspects would be the topic of a separate thesis, therefore in this chapter I will just give a brief overview over the basics. In my opinion free expression is not possible without the protection of privacy, although privacy involves prohibitions on divulging information in some circumstances. These two interests are complimentary and should be pursued jointly particularly as issues considering the design of new information technologies. Without the protection of privacy people won’t feel free and secure to express their opinions and views. This will curtail their right to freedom of expression.

Article 12 of the Universal Declaration states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks
upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Nearly every country in the world recognises privacy as a fundamental human right in its constitution, either explicitly or implicitly. A lot of industrialised countries support comprehensive privacy and data protection acts and have, or are in process of, enacting such laws.

Of all the human rights in the international law, privacy is perhaps the most difficult to define. Definitions vary widely according to context and environment. In many countries, the concept has been fused with data protection, which interprets privacy in terms of management of personal information. Outside this rather strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs.  

1.10.1 Separate but Related Concepts of Privacy:

- Information privacy: Involves the establishment of rules governing the collection and handling of personal data such as credit information, medical or government records. It is also known as "data protection."

- Bodily privacy: Concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing, and cavity searches.

- Privacy of communications: Covers the security and privacy of mail, telephones, e-mail and other forms of communication.

---

54 supra note 27
Territorial privacy: Concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.\(^{56}\)

The growth of government and commercial transactions and the increase in technological developments over the last 50 years have heightened threats to privacy. Today the Internet accelerates the trend toward increased information collection and facilitates unprecedented flow of personal information. Electronic communication systems generate vast quantities of transactional data that can be readily collected and analysed. The Internet has made this kind of collection and analysis easier and much more efficient. Rather than rely on secondary sources of consumer information, or engage in cumbersome telephone and mail-in information collection practices, companies can collect data online, through registration and as a transaction is carried out. Technologies such as “cookies”, written directly onto a user’s hard drive, enable web sites to collect information about online activities, creating a wealth of behavioural and preference information.\(^{57}\)

Confronted by these challenges and while dangers to privacy capture our attention, we also have to look at the unprecedented gains in privacy protection that have also been achieved over the last half of the twentieth century. In many cases the legal system has laid a foundation for privacy protection. Two crucial instruments evolved from these laws. The CoE’s 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data\(^{58}\) and the OSCE Guidelines Governing the


Protection of Privacy and Transborder Data Flows of Personal Data\textsuperscript{59} set out specific rules covering the handling of electronic data. These two agreements have had a profound effect on the enactment of laws around the world.

\textbf{1.10.2 The EU Data Protection Directives}\textsuperscript{60}

In 1995 and 1997, the European Union enacted two directives to harmonise laws throughout the EU to ensure consistent levels of protections for citizens and to allow for the free flow of personal information throughout the EU. Several principles of data protection are strengthened under the Directives: the right to know where the data originated, the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing and the right to withhold permission to use data in some circumstances. In July 2000, the European Commission issued a proposal for a new directive on “the processing of personal data and the protection of privacy in the electronic communications sector”\textsuperscript{61}. The proposed directive replaces existing definitions of telecommunications services and networks with new definitions of “electronic communications services and networks.” The existing protections are extended to a broader, more technology neutral approach.

A key concept in the European model is “enforceability”. The EU is concerned that data subjects have rights that are enshrined in explicit rules, and that they can go to a person or an authority empowered to act on their behalf. Every EU country has a Data Protection Commissioner or agency that enforces the rules. It is expected that the


\textsuperscript{60} EC, Council Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the protection of personal data and on the free movement of such data, [1995] O.J. L. 281/31

countries with which Europe does business will need to provide a similar level of oversight. Article 25 of the Directive imposes an obligation on Member States to ensure that the personal information relating to European citizens has the same level of protection when it is exported to, and processed in, countries outside the EU.

This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. Those countries that refuse to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data.

Some countries, such as the United States, have avoided enacting general data protection rules in favour of specific sectoral laws, governing, for example, video rental records and financial privacy. This sectoral approach relies on a mix of legislation, regulation and self-regulation. Although it was never formally ruled upon by the European Commission, there were serious doubts whether the U.S. approach would pass the adequacy test laid down by the Directive. Therefore in 1998, the U.S. began negotiating a “Safe Harbour” agreement with the EU in order to ensure the continued transborder flow of personal data. In July 2000 the EU approved the “Safe Harbour” agreement with the U.S. Companies that voluntarily agree to the safe harbour principles of notice, choice, and access must notify consumers of the purpose of data collection. They must also give users access to their personal information and allow them to not share their data with third parties.

Privacy advocates and consumer groups both in the U.S. and in Europe are highly critical of the European Commission's decision to approve the agreement, because the agreement rests on a self-regulatory system whereby companies merely promise not to violate their declared privacy practices. There is little enforcement or systematic review of compliance. The Safe Harbour status is granted at the time of self-certification.
There is no individual right to appeal or right to compensation for privacy infringements. Therefore the agreement will fail to provide the same adequate protection as the EU Directive.

Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept up with the technology, leaving significant gaps in protections. In other countries, law enforcement and intelligence agencies have been given significant exemptions. There are widespread violations of laws relating to surveillance of communications, even in the most democratic of countries. There are a number of important trends that contribute to privacy invasion. Globalisation removes geographical limitations to the flow of data. Convergence is leading to the elimination of technological barriers between communication systems. Multi-media fuses many forms of transmission and expression of data and images so that information gathered in a certain form can be easily translated into other forms.\textsuperscript{62}

In many countries, human rights organisations, journalists and political dissidents are the most common targets of surveillance by government and law enforcement agencies. Following closely on the success of forcing telecommunications equipment manufacturers and companies to build in surveillance capabilities, intelligence and law enforcement agencies have now turned their attention to the Internet and possibilities to monitor its vast flow of information.

One way for computer users to guarantee that their sensitive data remains secure and is protected against interception is the use of cryptography. Modern encryption technology – a mathematical process involving the use of formulas (or algorithms) – was traditionally deployed most widely to protect the confidentiality of military and diplomatic communications. Today it is widely used in the civilian sector and has

\textsuperscript{62} supra note 51
become an integral component of the global economy. Encryption ensures the confidentiality of personal records, such as medical information, personal financial data, and electronic mail. It can also be used to allow for the anonymous dissemination of information, such as reports on human rights abuses, and to ensure that documents of human rights groups are not tampered with or altered after release.

The international relaxation of regulations concerning encryption has largely succeeded. The rise of electronic commerce and the recognition of the need to protect privacy and increase the security of the Internet has resulted in the development of policies that favour the spread of strong encryption world wide. In 1997, the OECD issued guidelines on cryptography policy. They identify basic principles that countries should adopt in establishing cryptography policies at the national and international level. Most countries today impose no restrictions on the use of cryptography. It may be freely used, manufactured, and sold without restrictions.\(^{63}\)

There are a small number of countries where strong domestic controls on the use of cryptography exist. These are mostly countries where human rights command little respect, most notably Russia and China. The rapid growth of e-commerce and the lack of international consensus on restrictions will further isolate these countries and make it difficult for them to continue these policies. Export controls remain the most powerful obstacle to the development and free flow of encryption but they are steadily being relaxed because of the Internet and demands for secure electronic commerce. The decision by the U.S. to liberalise its own encryption export regulations in January 2000.

has had the effect of weakening the position of those who favour strict controls on cryptography.\textsuperscript{64}
Chapter II Human Rights Agreements

Over the past fifty years international and regional Human Rights agreements have helped to enshrine the right to freedom of expression world wide, becoming part of international law and affecting the domestic laws of many nations. The question is whether these human rights instruments are applicable to the Internet with regard to their language and scope and how they can be enforced?

In some respects the study of these instruments is encouraging; they seem to be drafted in very forward looking language and there is evidence of an international consensus on the scope of freedom of expression: it applies to all forms of media, and to the ability to receive and to impart information, and it is subject to limited restrictions only.¹

2.1 International Agreements that Manifest a Commitment to the Right of Freedom of Expression

2.1.1 Universal Declaration of Human Rights²

The promotion and protection of human rights was a fundamental priority of the United Nations in 1945, when the UN's founding nations resolved that the atrocities of the Second World War should never be repeated. Three years later the United Nations

---

General Assembly adopted the Universal Declaration of Human Rights. In my opinion it is very important that the fundamental rights articulated in the Universal Declaration should not be lost as a result of rapid developments in technologies, globalisation and increased commercialisation in the digital age.

Article 19\(^3\) of the Universal Declaration proclaims the right to freedom of expression. The language of Article 19 can be called “foresightful” in regard to the Internet. First, the Internet is global in its reach and transcends national borders. Article 19 states that freedom of expression is protected “regardless of frontiers”. The rights to “seek” and “impart” information may apply to surfing and posting information on the Internet, the right to “receive” information may apply to electronic mail and the downloading of information.\(^4\)

Article 12 of the Universal Declaration states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

These two Articles build the foundation of the protection of freedom of expression and privacy as human rights and bear directly on the protection of human dignity in the new information age.

---

3 "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any medium and regardless of frontiers."

4 supra note 1
Enforcement:

The Universal Declaration is not a treaty. Therefore States have no legal obligation to respect the rights listed in the Declaration. It is possible, however, that the Universal Declaration, at least in some parts, may subsequently have become binding as a new rule of customary international law. UN General Assembly resolutions, even if they are not binding, may have normative value. They can provide evidence important for establishing the existence of a rule or the emergence of an opinio juris. But this is still a subject of discussion among legal scholars. Nevertheless the Universal Declaration has influenced subsequent international and regional treaties of more direct effect, decisions of international tribunals, and domestic constitutions and legislation.

In 1993, the UN Commission of Human Rights established the position of a Special Rapporteur of the Commission of Human Rights on the protection of the right to freedom of opinion and expression. The mandate of the Special Rapporteur is concerned with the promotion and protection of the right to freedom of opinion and expression, including the right to seek, receive and impart information. In view of the complexity and multifaceted nature of this right, the Special Rapporteur views the mandate as not focusing only on individual cases and incidents or being confined only to the issue of freedom of the press or the media. The work of the Special Rapporteur, therefore, involves both action on individual cases and incidents as well as consideration of laws and practices relating to the rights to freedom of opinion and expression and to seek, receive and impart information. Any individual, group, non-governmental organisation, intergovernmental agency or government with reliable knowledge of situations and cases in areas relating to the mandate are encouraged to bring the relevant information to the attention of the Special Rapporteur.

Upon receipt of prima facie credible and reliable information, the Special Rapporteur transmits the information to the government concerned and requests it to provide him with comments and observations. Upon receipt of the replies, the Special Rapporteur establishes whether the information received can be considered as explaining to his satisfaction the circumstances of the case, the applicable laws and regulations and the reasons for the act or omission on the part of the State that provided the initial ground for an allegation of an impermissible infringement on the right to freedom of opinion and expression.\(^7\)

The Special Rapporteur can only make recommendations to the States concerned. The enforcement of these recommendations works through means of social and political pressure. States are put in the pillory and exposed in the international community. Unfortunately all this has proven only partially successful. Many countries still violate human rights and do not live up to their commitments made. But, as mentioned above, the Universal Declaration has helped to establish a basic framework lining out the right to freedom of expression accepted by the international community.

2.1.2 *International Covenant on Civil and Political Rights*\(^8\)

The principles first enunciated in the Universal Declaration are reiterated and expanded upon in the ICCPR. The difference between the Universal Declaration and the ICCPR is that the ICCPR is an international treaty.\(^9\) When a treaty is adopted, legally binding international obligations for signatory members are created. When national

\(^7\) ibid.


\(^9\) An international treaty is a formal agreement between States that defines their mutual duties and obligations. Other terms for treaty interchangeably used are "convention" or "covenant".
governments ratify\textsuperscript{10} treaties, they become part of the nation's legal obligations as a member of the global community. In general, in order to have legal status, an international instrument must have been adopted by a majority vote of the States present and voting at an international conference. It must also have been ratified by a certain number of States in order to be activated.\textsuperscript{11} Protocols attached to treaties provide for complaint procedures.

Article 19 of the ICCPR restates Article 19 of the Universal Declaration almost verbatim. The ICCPR recognises that freedom of expression may be curtailed under certain circumstances, but the restrictions have to be narrowly defined and may not be arbitrary.

Enforcement:

The ICCPR establishes a Human Rights Committee which is composed of eighteen members elected by the States parties. The only compulsory mechanism under the ICCPR is a reporting system (Article 40), requiring States to submit reports on the national human rights situation every five years. These reports are studied and commented upon by the Committee, which then can make recommendations and general comments. As an optional procedure (Article 41) States may grant other States the right to bring a complaint against them before the Committee alleging the violation of human rights. Both States concerned must have accepted the procedure, and all local remedies must first be exhausted. This procedure is not very effective, because it can ultimately only lead to a conciliation attempt and there is no reference to a judicial body which could make a binding decision. Another problem arises from the large number of various kinds of reservations entered by contracting States to their

\textsuperscript{10} Ratification means the formal procedure by which a State becomes bound to a treaty after signing it as acceptance.

acceptance of the obligations of the ICCPR, which tend to undermine its effective implementation.\textsuperscript{12}

The First Optional Protocol\textsuperscript{13} to the ICCPR gives the Committee the power to consider complaints from individuals who claim that their human rights contained in the ICCPR have been violated. States that are party to the ICCPR do not automatically become party to the Optional Protocol as well. They must separately decide to accept the procedure under the Optional Protocol. The procedure under the Optional Protocol is of particular significance, because it contributes to the recognition of the individual as a legitimate subject of international law. It is one of very few mechanisms which enable individuals to submit petitions at the international level.

Although State compliance with the views of the Committee has not always been encouraging, it has to be said that many States have responded to the Committee's views. Laws have been changed, prisoners have been released and compensation has been paid to victims of human rights violations. To ensure compliance with its views the Committee must rely heavily on publicity. In recent times, it has taken steps to increase media interest in its work and therefore it is likely to continue to grow in influence and play an increasingly significant role in the protection of human rights throughout the world.

\textsuperscript{12} supra note 5 at 215
\textsuperscript{13} First Optional Protocol to ICCPR, 16 December 1966, 999 U.N.T.S. 171 (entry into force 23 March 1976) [hereinafter Optional Protocol]
2.1.3 International Covenant on Economic, Social and Cultural Rights\textsuperscript{14}

Article 15 of the ICESCR recognises the important "benefits to be derived from the encouragement and development of international contacts and co-operation in the scientific and cultural fields." Accordingly, the signatories pledge to "diffuse science and culture" and to "respect the freedom indispensable for scientific research and creative activity." These provisions proclaim the importance of freedom of expression across borders to realise social, scientific and cultural advancements. Furthermore Article 15 establishes that all individuals are entitled "to enjoy the benefits of scientific progress and its applications."

The Internet opens new doors for the realisation of these provisions, because it enables people from around the world to share valuable scientific research and social insights. It can also help to advance the awareness of human rights issues in the social context.

Enforcement:

The ICESCR only provides for a reporting system. No provision is made for inter-state complaints or individual petitions. The rights of the Covenant are formulated not as directly binding obligations, but described in terms of a programme depending on the goodwill and resources of the States. Since 1987 there has been a Committee on Economic, Social and Cultural Rights of independent experts who prepare "general comments" and issue general views on particular rights in the Convention. The legal obligations arising of the ICESCR are rather weak.\textsuperscript{15}


\textsuperscript{15} supra note 5 at 216
2.2 Regional Agreements

While conflicting ideologies and interests make it difficult to reach consensus at an international level about human rights, agreement at a regional level is easier to achieve, because States have more common values and interests. Regional Human Rights Agreements in Europe, the Americas, and Africa establish the right to freedom of expression.

2.2.1 European Convention for the Protection of Human Rights and Fundamental Freedoms

In 1950 the Council of Europe drafted the European Convention, which covers with its protocols much the same ground as the Universal Declaration. Since the Convention and protocols are legally binding on the States parties to them, they are formulated in much more detail than the Universal Declaration. The vast majority of European States have signed and ratified the European Convention. Article 10 of the European Convention protects the right to freedom of expression. Closely linked to Article 10 are Article 8, which contains the right to respect for correspondence and privacy, Article 11, which contains the right to freedom of peaceful assembly and freedom of association, and Article 9, which contains the right to manifest one’s religion or belief.

Article 10 is not stated in absolute terms. Its second paragraph specifies that freedom of expression can be curtailed. Any restriction must be “prescribed by law” and

---


17 For more information visit online: Council of Europe Homepage <http://www.coe.int/> (date accessed: 19 September 2001)

18 Armenia and Azerbaijan have signed the European Convention in 2001 but not ratified yet, Bosnia-Herzegovina, the Federal Republic of Yugoslavia and Belarus have not signed the European Convention. For further information visit online: Council of Europe <http://www.coe.int/>
“necessary in a democratic society”. Application of the exceptions in the second paragraph will always turn on the factual and legal context, considered on a case by case basis.

Most European countries that are party to the European Convention have made it part of their national law, meaning that it can be invoked in the national courts.

Enforcement:

The new European Court of Human Rights (ECHR) came into operation on 1 November 1998 with the entry into force of Protocol No. 11. Any contracting State (State application) or individual claiming to be a victim of a violation of the European Convention (individual application) may lodge directly with the Court in Strasbourg an application alleging a breach by a contracting State of one of the Convention rights. All final judgements of the Court are binding on the respondent States concerned. Responsibility for supervising the execution of judgements lies with the Committee of Ministers of the Council of Europe. It is thus for the Committee of Ministers to verify whether states in respect of which a violation of the Convention is found have taken adequate remedial measures to comply with the specific or general obligations arising out the Court’s judgements.

The ECHR has jurisdiction over 40 countries with a combined population of 800 million people. It is the last resort to which citizens may turn once they have exhausted all other legal means of redress.

---

19 It has been widely discussed whether these exceptions are too broad.
20 For more information about the European Court of Human Rights visit online: European Court of Human Rights <http://www.echr.coe.int/> (date accessed: 19 September 2001) [hereinafter ECHR]
2.2.1.1 Case Law of the ECHR Relevant to the Internet:

In Handyside v. the United Kingdom\textsuperscript{22} the ECHR describes the scope and importance of the right to free expression under Article 10 of the European Convention. The Court has described freedom of expression as "one of the basic conditions for the progress of democratic societies and for the development of each individual."\textsuperscript{23}

Under the European Convention, freedom of expression is not absolute. The State may validly interfere with such freedom (irrespective of the medium through which opinions, information and ideas are expressed) but only under the conditions laid down in Article 10, paragraph 2. The ECHR applies a three part test. Any restriction of the right to freedom of expression must

- be prescribed by law
- have as its aim a goal legitimate under paragraph 2 of Article 10 of the European Convention
- be necessary in a democratic society to achieve that goal.\textsuperscript{24}

The ECHR has stated that the exceptions in paragraph 2 "must be narrowly interpreted and the necessity for any restrictions must be convincingly established."\textsuperscript{25} The relationship between the third sentence of Article 10, paragraph 1 and paragraph 2 is worth noting. The Court has stated the purpose of the third sentence in the judgement of "Informationsverein Lentia and others v. Austria".\textsuperscript{26} The ECHR has also pointed out

\textsuperscript{23} ibid, at para. 49
\textsuperscript{25} The Sunday Times v. the United Kingdom (No. 2), ibid.
\textsuperscript{26} Informationsverein Lentia and others v. Austria (1993), 276 Eur. Ct. H.R. (Ser. A) at para. 32
that freedom of expression applies differently to distinct media. The nature and extent of permissible restrictions depends on the nature of the medium. The potential impact of the medium concerned has to be considered.\textsuperscript{27} The necessity test has several elements: First, any government action must be effective, that means it has to be reasonably likely that the action in fact serves one of the permitted governmental interests. Second, any restriction has to be proportional and not overbroad, and third, government restriction should not be permitted if a less restrictive alternative would serve the same goal.

The restrictions on the exercise of freedom of expression and information that are admissible according to Article 10, paragraph 2, fall into three categories:

1. those designed to protect public interest (national security, territorial integrity, public safety, prevention of disorder or crime, protection of health or morals);
2. those designed to protect other individual rights (protection of the reputation or rights of others, prevention of the disclosure of information received in confidence);
3. those that are necessary for maintaining the authority and impartiality of the judiciary.

This list may seem to be extensive, but in order to be admissible, any restriction must be prescribed by law and be necessary “in a democratic society”.

The right to freedom of expression and information recognised in Article 10 includes, inter alia, freedom to receive and impart information and ideas by broadcasting media.\textsuperscript{28} With regard to radio and television broadcasting and the cinema, it is stipulated in the third sentence of Article 10, paragraph 1, that “\textit{this Article shall not}

\textsuperscript{28} Sacchi v. Italy (1976), 5 Eur. Comm. H.R. D.R. 43
prevent States from requiring the licensing of broadcasting, television or cinema enterprises." The wording doesn't seem to be declarative in nature. With regard to the Internet Article 10, paragraph 1, allowing the licensing of broadcasting, television and cinema does not implicitly prohibit the licensing of internet enterprises. As mentioned above, freedom of expression in the European Convention is not absolute and the State may validly interfere with such freedom irrespective of the medium through which opinions, information and ideas are expressed.

The Court delivered in March 1990 for the first time a judgement on electronic media, in the "Groppera Radio AG and others v. Switzerland" case. It concluded that the prohibition imposed by the Swiss authorities on Swiss cable network operators, on re-broadcasting programmes from Italy had not infringed these companies' rights to impart information and ideas regardless of frontiers guaranteed by Article 10. The Court decided in particular in this case that the prohibition had not gone beyond the margin of appreciation left to the national authorities to interfere in the exercise of freedom of expression, insofar as it was not a form of censorship directed against the content or tendencies of the programmes, but a measure taken against a station which the Swiss authorities could reasonably hold to be, in reality, a Swiss station operating from the other side of the border in order to circumvent the statutory telecommunications system in force in Switzerland.

With regard to the Internet this decision seems to be interesting in the light of content providers who seek the most favourable set of rules in one legislation to transmit their content aimed at a certain audience in a country or countries in order to circumvent the legislation in force there.

---

But even if a law can be justified and upheld under the necessity test, the various forms of government Internet censorship used at the moment aren’t likely to be effective, because users will be able to find ways around them. There are many examples of how banned Internet content shows up at mirroring sites and messages from people in repressive countries travel around the globe. In addition, to further protect themselves from government control, speakers can render themselves unidentifiable using encryption tools.

In many circumstances Government censorship won’t meet the proportionality test. If, for example, information is banned because it is deemed harmful to minors, it will result in making the same information unavailable to adults, who would have the right to see it.

Finally, the user-controlled nature of the Internet makes government control in a lot of cases unnecessary, because it offers alternative means of achieving the same goal. This point can be especially relevant in the area of protection of morals. Many of the proposed governmental controls on content on the Internet are put forth in the name of protecting children from harmful content. But to protect children from potential harmful content, parents are in a far better position than the government to control what their children see, through supervision, education, or use of filtering software.31

There are a number of decisions which are particularly relevant to the Internet, given the practice of mirroring content, which hold that the prohibition on publishing certain content was “not necessary in a democratic society” if the information was available otherwise. Perhaps the most important case on this subject is the famous “Spycatcher”

31 Although the use of filtering and blocking tools raises serious freedom of expression concerns, it can be seen as an alternative to government regulation. For further discussion and details, see Chapter III, 3.3 Self-Rating Schemes and Filtering and Blocking Software at 91.
case, involving the memoirs of a former member of the British Security Service. The Court held that the injunction against publishing the book was no longer appropriate under Article 10 after the book was published in the United States.

The Court has also recognised a distinction between those who make certain offensive statements, and those who serve as the conduits for that information to the public. The distinction arose in a case concerning the liability of a journalist, but it may have relevance to the question of ISP liability for content they did not create. The Court said that a journalist could not be prosecuted for publishing remarks uttered by others. It has also drawn a distinction between the author of statements and the conveyor of those statements. Seeing ISPs in the same position as a journalist, a conveyor of content they did not create, this can be seen as a statement of the importance of not holding ISPs liable for content they did not create.

The ECHR also concluded that contracting states are under a positive obligation under Article 10 to take measures to ensure pluralism in the media. As a result of technological progress, restrictions on new media in form of a public monopoly could no longer be justified.

2.2.2 Charter of Fundamental Rights of the European Union

The foundation of the European Union served primarily economic purposes and therefore in the beginning not much attention was paid to human rights within its legal framework. Furthermore the existence of the European Convention seemed to be

---

33 supra note 27
34 For more details see Chapter III, 3.4 Liability of ISPs at 100
35 supra note 26
sufficient for the protection of human rights within the Member States of the European Union. With the growing number of Member States, the scope and purpose of the European Union had been enlarged, too. The Amsterdam Treaty\(^\text{37}\) proclaims that "the Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms and the rule of law." Any Member State violating human rights in a "serious and persistent" way can lose its rights under the Treaty. The European Court of Justice has long required the Community to respect fundamental rights and the European Council has issued several major statements emphasising the importance of respect for human rights.\(^\text{38}\)

Finally, the European Union solemnly proclaimed the EU Charter at the meeting of the European Council held in Nice in December 2000. Article 11 contains the right to freedom of expression and information. It corresponds to Article 10 of the European Convention. Pursuant to Article 52(3) of the EU Charter, the meaning and scope of this right are the same as those guaranteed by the European Convention.

Enforcement:

Article 51(2) of the EU Charter states that "the Charter does not establish any new power or task for the Community or the Union, or modify powers and tasks defined by the Treaties." That means there is no separate enforcement mechanism or body set up to guard the protection of human rights in the European Union. The Community has to rely on the existing framework and organisation. That means that the European Court


of Justice, which has jurisdiction over the European Union’s 376 million citizens is still in charge of the human rights enforcement within the Member States.

It is especially interesting to look at the European human rights system because its enforcement is transnational. The two European Courts\(^\text{39}\) place in their verdicts international human rights law above domestic constitutional law and countries are complying without a murmur.\(^\text{40}\) Prominent examples are Germany and Great Britain\(^\text{41}\), but even Turkey has been stopped cold in its plans to execute Kurdish rebel leader Abdullah Ocalan, because Mr. Ocalan’s lawyers have appealed to the ECHR, and Turkey does not dare to imperil its chances of joining the European Union.\(^\text{42}\)

The message sweeping across Europe and into the world is that the nation state is no longer sacrosanct and that jurisprudence has gone global in its approach to law. Governments can no longer rely on the sanctity of the nation state to provide cover for human rights violations. That will have enormous implications for the future legislation and regulation of the Internet world wide, because if borders disappear in Europe why shouldn’t they anywhere else?

2.2.3 OSCE Commitments and Instruments Related to Freedom of Expression\(^\text{43}\)

The Organisation for Security and Co-operation in Europe (OSCE) is the largest regional security organisation in the world with 55 participating States from Europe, Central Asia and North America.\(^\text{44}\)

\(^{39}\) The European Court of Justice of the European Union and the European Court of Human Rights

\(^{40}\) supra note 21

\(^{41}\) After a decision of the ECHR Britain must admit gays into its military, and Germany must allow women to serve in combat roles in its armed forces after a European Court of Justice decision.

\(^{42}\) supra note 46


\(^{44}\) For more information see: online: OSCE <http://www.osce.org/>
From the Helsinki Final Act in 1975\(^{45}\) to the Charter of Paris in 1990\(^{46}\) to the OSCE Istanbul Summit in 1999\(^{47}\) the OSCE has shown its commitment to protect the right to freedom of expression.

Freedom of expression, and its corollary, freedom of the media, is one of the most basic human rights. In order to ensure a high level of commitment with the norms and standards accepted by the OSCE participating States, the position of the OSCE Representative on Freedom of the Media was established in December 1997. The function of the OSCE Representative on Freedom of the Media is to observe relevant media developments in OSCE participating States with a view of providing early warning on violations of freedom of expression. The Representative's second main task is to assist participating States by advocating and promoting full compliance with OSCE principles and commitments regarding freedom of expression and free media.\(^{48}\)

The Representative on Freedom of the Media works in close co-ordination with the Chairman-in-Office of the OSCE. The Representative routinely consults with the Chairman-in-Office and reports on a regular basis to the Permanent Council, recommending further action where appropriate. The Representative himself does not have any means of enforcement at his disposal.

On March 12\(^{th}\) and 13\(^{th}\) 2001 the OSCE held a supplementary human dimension meeting on freedom of expression in Vienna. There was broad consensus that the OSCE could play an even more active role in promoting freedom of expression, including through legislative and technical assistance to governments, by providing


\(^{48}\) online: OSCE <http://www.osce.org/fom/overview/> (date accessed: 22 September 2001)
training and by promoting better access to new information technologies. In the final report the importance of the Internet was stressed and recommendations to the OSCE participating States include:

- The free flow of information on the Internet should not be regulated, except by the end user.

- To protect citizens from harmful material States should regulate content in accordance with Article 10 of the European Convention on Human Rights.

- Any person restricted in their freedom of expression should be able to challenge the validity of that restriction before an independent court or tribunal.

Furthermore the importance of international standards such as the ICCPR and the European Convention on Human Rights are recognised as applicable to the Internet and OSCE Participating States should ensure that their domestic legislation fully complies with these standards.

2.2.4 American Declaration of the Rights and Duties of Man, American Convention on Human Rights and Inter-American Declaration of Principles on Freedom of Expression

50 OAS, 9th International Conference of American States, American Declaration of the Rights and Duties of Man, OEA/Ser.L/V/1.4 rev. 8 (1948), online: Organization of American States <http://www.cidh.oas.org/Basicos/basic2.htm> (date accessed: 7 April 2002) [hereinafter American Declaration]
The American Declaration was the first international human rights instrument, predating even the Universal Declaration. It was adopted by the 9th International Conference of the American States in Bogotá in 1948. Although it was originally adopted as a declaration the Inter-American Court of Human Rights and the Inter-American Commission on Human Rights have held that it is today a source of international obligations for the OAS\textsuperscript{53} member states.\textsuperscript{54} Article IV of the American Declaration states that “Every person has the right to freedom of ... expression and dissemination of ideas, by any medium whatsoever.”

The American Convention was adopted by the OAS in 1969. Article 13 proclaims the right to freedom of thought and expression. Article 11 (right to privacy) and Article 12 (right to freedom of conscience and religion) are also closely linked to Article 13.

The American Convention has several features that go beyond other human rights instruments. It states explicitly that the right to freedom of expression “shall not be subject to prior censorship.” It applies to private action and makes it clear that the right to expression may not be restricted by indirect methods or means.\textsuperscript{55} There is a list of permitted grounds for restriction set forth by the American Convention: Restrictions on speech must be “expressly established by law to the extent necessary to ensure [either] respect for the rights or reputation of others ... or the protection of national security, public order, or public health or morals.”

\textsuperscript{53} Organisation of American States [hereinafter OAS]
\textsuperscript{55} Article 13(3) of the American Convention, supra note 48
The plain language of the American Convention seems to be clearly applicable to the Internet, as it is the case with the international and European counterparts.

Enforcement:

The protections of the American Convention are enforced by the Inter-American Court of Human Rights\textsuperscript{56} and the Inter-American Commission on Human Rights\textsuperscript{57}, which are institutions of the OAS.

The Inter-American Court is the principal judicial organ of the inter-American system. Proceedings are instituted by the filing of an application either by a State Party or by the IACHR. Article 62 of the American Convention states that a State Party has to declare that it recognises the jurisdiction of the Inter-American Court as binding. Such a declaration can be made unconditionally, on the condition of reciprocity, for a specific period, or for specific cases.

According to Article 44 of the American Convention, petitions containing denunciations or complaints of violations of the convention by a State Party may be lodged at the IACHR by any person, any group of persons, and any non-governmental organisation legally recognised in one or more Member States of the OAS.

Individuals are not allowed to directly make an application to the Inter-American Court and until recently they had no standing before the Court, but on November 24, 2000 the Inter-American Court introduced new Rules of Procedure (effective since June 1, 2001), that contain a series of provisions to grant alleged victims, their next of kin or

\textsuperscript{56} [hereinafter Inter-American Court]
\textsuperscript{57} [hereinafter IACHR]
their duly accredited representatives direct participation (locus standi in judicio) in all stages of the Court's proceedings once an application has been presented.

The principal function of the IACHR is to promote the observance and defence of human rights and to serve as an advisory body to the OAS on this subject. The IACHR investigates and rules on complaints on human rights violations, conducts on-site visits, prepares draft treaties and declarations on human rights and prepares reports on the human rights situation in countries in the region.

At its 97th regular session in October 1997 the IACHR decided to create the Office of the Special Rapporteur for Freedom of Expression. In creating this Office the Commission sought to stimulate the awareness of the importance of full observance of freedom of expression and information. The duties and the mandates of the Special Rapporteur correspond with those of the Special Rapporteurs established within the UN and OSCE frameworks mentioned above.

The Inter-American Declaration of Principles of Freedom of Expression was approved by the IACHR during its 108th regular session. It reaffirms that freedom of expression is a fundamental right recognised in the American Declaration and American Convention and recognises that the Member States of the OAS are subject to the legal framework established by these instruments. The principles announced more or less sum up all the "basics" building the framework for the right to freedom of expression established in the Universal Declaration, the ICCPR, the European Convention, the American Declaration and the American Convention.
2.2.5 African Charter on Human and Peoples' Rights

The African Charter has been ratified by 53 countries of the Organisation for African Unity. In Article 9 it declares the right to freedom of expression. The general terms used in the African Charter make it relatively easy to apply them to the Internet.

Enforcement:

The African Charter establishes the African Commission on Human and Peoples' Rights which is responsible for the enforcement of the Charter provisions. Member States have to report on a regular basis to the Commission about their implementation of rights guaranteed under the African Charter. The Commission can issue general observations and recommendations.

In 1997 an additional Protocol on the Establishment of the African Court on Human and Peoples' Rights was adopted by the Member States of the Organisation of the African Unity. Although generally only the Commission or Member States can bring cases before the Court, Article 6 of the protocol provides in exceptional cases individuals or a group of individuals standing before the Court.

2.3 Summary of the Relative Effectiveness of these Various Instruments

The existing framework of international and regional human rights agreements offer a solid basic ground for the protection of freedom of expression. Most of their provisions

---


59 See Article 47 and Article 62 of the African Charter, ibid.

with regard to freedom of expression seem to be applicable to the Internet, although concrete examples or cases on the international level where provisions actually have been applied in that context are rare or non-existent. Significant decisions concerning the Internet will be made by governments and international organisations in the next few years. It has to be seen how they actually reflect and build upon existing agreements.

International and regional human rights instruments offer opportunities to those who seek to challenge regulation of the Internet. In some cases, the most promising venues may be under the regional agreements, because they offer stronger enforcement mechanisms and individuals or private parties may seek to take their cases before the Courts established in the regional agreements.

It seems very important to me that on the international level even more efforts should be made to promote the public awareness of the protections granted in international and regional agreements and specific research on the application of the key principals to new communication technologies and the digital age should be pursued. International educational programmes can also promote the understanding and awareness of the Universal Declaration and its companions. The more people get to know their rights, the harder it will be to justify their violation and to explain why they should not be applicable to the Internet.
Chapter III  Internet Control

3.1 General Observations

The open and complex nature of the Internet, its international character and fast development over the past decade and its unique opportunity for freedom of expression and communication, for a free exchange of creative discovery in the arts and other areas of cultural production, and for freedom in research and the dissemination of ideas, is very positive and welcomed all around the world but it has, on the other hand, raised severe concerns. It is argued that the Internet is a major means for hawking pornography, terrorism, drug culture and racial hatred, thus endangering society and their members, especially children, who use the Net.

It is also a great resource for gathering personal data of individuals, which should and would not be accessible otherwise. It opens the door for thieves to steel and sell this data to companies or to use it for their own benefits (e.g. credit card information). It also enables governments and private companies to have more control over their citizens or consumers in using information like where do people shop online, which web sites do they enter, what are their preferred topics of discussion, etc.

Although it is generally conceded that the Internet is not primarily concerned with such negative activities, and, even when it is, to succeed at those activities requires a series of specific decisions accompanied by a knowledge how to access such materials, there continue to be calls for regulation and content control to reduce the harmful influence of the Net and to protect important human rights.
The control of the Internet raises a complex series of questions about how it will transform our way of life, our fundamental institutions and our values. Furthermore we have to ask how far should a society go to protect its members without patronising them and destroying the unique new character of the Internet. As a transnational and borderless data network it reinforces the erosion of the nation state and its powers. There are many states with totally different national rules and laws within the architecture of the Internet.

Due to the Internet's global structure there is a limited possibility of nation-state oriented control and law enforcement although states do have control over cyberspace, at least in some areas which will be shown later on in this thesis. The Internet is multi-jurisdictional in the obvious sense that messages can travel from a network anywhere around the world to any place on the globe where there are computers with access to the Internet's medium of communication. It also allows those who are subject to the rules set up by nation states to change jurisdiction easily and to seek a more favourable legal regime. This leads to the unprecedented and unpredictable situation of a "free market" in legal regimes.\(^1\)

Before we look at specific regulation of certain issues a prior question has to be asked: Who will make and enforce the rules that will govern cyberspace?

Robert Ellickson's framework for behavioural controls is a useful starting point for a discussion of the various forces governing individual behaviour in electronic networks. He identifies five controllers that can provide substantive rules governing an individual's behaviour:\(^2\)

---


<table>
<thead>
<tr>
<th>Controller</th>
<th>Substantive Rules</th>
<th>Sanctions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The actor him/herself (the users)</td>
<td>Personal ethics</td>
<td>Self-sanctions</td>
</tr>
<tr>
<td>Second party controllers, i.e., the person acted upon (Employers, ISPs)</td>
<td>Contractual provisions</td>
<td>Various self-help mechanisms</td>
</tr>
<tr>
<td>Non-hierarchically organised social forces (Family)</td>
<td>Social norms</td>
<td>Social sanctions</td>
</tr>
<tr>
<td>Hierarchically organised non-governmental organisations (Universities, Libraries, NGOs)</td>
<td>Organisation rules</td>
<td>Organisation sanctions</td>
</tr>
<tr>
<td>Governments</td>
<td>Law</td>
<td>State enforcement, coercive sanctions</td>
</tr>
</tbody>
</table>

Table 1

There is something of an asymmetry in the ranking of controllers, at least insofar as the State has a monopoly on the use of coercive sanctions when faced with violations of whatever rules it promulgates. The state can impose its laws on individuals, contracting parties, or organisations lower down in the controller hierarchy, but not vice versa. But the state’s ability to impose sanctions on law-violators is fundamentally constrained by the need for physical proximity and physical control. This is not an absolute constraint; mechanisms do exist whereby individual sovereigns can impose their rules on persons or entities not physically present in the area over which the sovereign has control.
A state may prosecute, for example, its nationals for crimes committed anywhere in the world (active nationality principle). This rule is universally accepted, although states make different use of it.³ A certain co-operation exists between different countries in civil, criminal and administrative matters, based upon multilateral and bilateral treaties. This includes co-operation with regard to extradition: Individuals who have taken refuge in a state which has no jurisdiction to try him are handed over by one state to another state, in order that they may be tried in the latter state for offences against its laws. It also includes the surrender of convicted criminals who have escaped before completing their punishment.⁴

But such mechanisms entail additional enforcement costs, both in terms of the direct costs of projecting sovereign power extra territorially and the costs of co-ordinating and harmonising the legal regimes of competing sovereigns.⁵

Information transmitted over the Internet can appear simultaneously in almost every nation in the world and it can easily flow across national borders without detection. It is generally accepted that a nation can regulate transactions that have local effects. If an Internet transaction has effects in every nation, then every nation can regulate the transaction. Since nations differ in their regulatory approaches, transactions on the Internet will be subject to inconsistent and different regulations. But unilateral national regulation of harmful effects of Internet information flows, is, from a jurisdictional perspective, perfectly legitimate and clearly consistent with international law.

But most unilateral national regulations – and especially the most demanding and restrictive ones – will affect regulatory efforts of other nations and the Internet activities

⁴ ibid. 117
⁵ supra note 1
of parties in other jurisdictions. Extraterritorial spillover effects of national regulation of Internet transactions are inevitable but legitimate. If we look at the discipline of conflicts of law we realise that there are always spillover effects from unilateral regulation of transnational transactions whenever one nation regulates transnational conduct differently than another. This is not a new phenomenon of the Internet age. As long as we wish to maintain national lawmaking and territorial sovereignty, such spillovers are perfectly legitimate in the absence of some international law to the contrary.6

The vast majority of content providers on the Internet need only to worry about the regulations of the nation in which they are physically located, because they have no presence or assets in other jurisdictions that wish to regulate their information. For the most part, a nation can exercise enforcement of jurisdiction only against persons or entities within its territory, although there are exceptions to this point.7 Of course it is possible that content providers can be affected indirectly by local regulations. A nation can regulate access to content, for example, it can penalise in-state end users who obtain or use foreign content or it can regulate ISPs and other local firms that facilitate the local transmission of digital information. Thereby it regulates the flow of foreign provided content.8

National regulation faces two main problems: the loss of territorialsity and national sovereignty in Cyberspace. To further illustrate the problem I have included the so-called “Somm-Case”.9

7 A nation can enforce its laws against persons abroad over whom it can obtain personal jurisdiction and enforce a default judgement abroad. It can also extradite persons from other countries.
8 For a more detailed discussion see Chapter III, 3.4 Liability of ISPs at 100
In the German case, the former CompuServe executive Felix Somm was accused of being an accomplice of the crime of distributing child pornography on the Internet. In November 1995 German police notified Mr. Somm, who was at that time managing director of CompuServe GmbH Germany, of five newsgroups with child pornography content on the servers of CompuServe, Inc. and served on the defendant a list of 282 Usenet newsgroups accessible through CompuServe that supposedly contained pornographic images or could at least be used to place such content. Mr. Somm immediately notified the parent company in the US, asking to “delete or block” those newsgroups, which CompuServe, Inc. promptly did. The result was a wave of protests by users. Therefore, while the five newsgroups that had contained pornographic material relating to children remained permanently blocked, the other 277 newsgroups were re-opened and CompuServe provided their members with “child safeguard software”. On subsequent checks, German police still retrieved individual news postings with “hard pornographic” content from the news servers of CompuServe. Supposedly, it was possible to get those files because the blocking software did not function properly or because the creators of the criminal content somehow avoided the blocking mechanisms. The pornographic charges against Mr. Somm related to 13 of the above mentioned images. The Amtsgericht München held Mr. Somm criminally liable for this third party content and he was found guilty of wilful distribution of pornographic content, pursuant to § 184 par 3 No. 2 StGB. He was given a two year suspended sentence, three years’ probation, and a fine of 100,000 German marks.

The verdict led to harsh reactions of disapproval in Germany and around the world. Even the district attorney in Munich appealed the verdict in favour of the plaintiff, which is possible in German criminal law. On November 15, 1999, the Landesgericht München overruled the judgement of the first instance and acquitted in the appeal proceedings Mr. Somm of the charge of distribution of child pornographic material.
One of the reasons for attempting to convict Mr. Somm was surely the lack of acceptance of the fact that the Internet cannot be controlled on the national level. It was an attempt of national law enforcement within the global Internet, manifested in the conviction of the head of CompuServe Germany, picked by the prosecution because it was unable to sue those it viewed as being principally responsible.

Therefore the obvious solution has seemed to be the regulation of the Internet on an international level. But as easy as this may sound, international law and its enforcement has its pitfalls, too, which will be shown.

### 3.2 Content Control Overview

The regulation of Internet content poses a real challenge to law makers around the world. Not only has the transnational character of the Internet to be considered. There are also the multifaceted possibilities of content available to take into account. It is apparent that the complex nature of this new technology will require a radically different approach to the regulation of its content.

A complex series of tensions have developed between those who stand for no regulation at all, alarmed at possibly loosing a unique international opportunity for freedom of expression and communication, for a free exchange of creative discovery in the arts and other areas of culture, and for freedom of research and the dissemination of ideas, on the one hand, and those who see the Internet as a major means for distributing among other things pornography, hate speech, and terrorism, thus endangering our society and especially children who use the Net.
Long, long ago in the history of the Internet John Perry Barlow, an Internet activist, published a “Declaration of the Independence of Cyberspace”. It was a well-meaning document that captured the spirit of the time, when great hopes still were present that the new, emerging medium would encourage freedom and democracy, and the Internet was a parallel universe of pure data, an exciting new frontier where a lawless freedom prevailed.

“Governments of the industrial world,” Mr Barlow declared, “on behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Cyberspace does not lie within your borders.”

Well, it turned out that the Internet, often perceived as being everywhere yet nowhere is in fact subject to geography after all, and therefore subject to law. And governments do have a great deal of sovereignty over cyberspace. All sorts of new technologies have been developed to speed up the delivery of content, protect networks from intruders, or target advertising depending on a user’s country of origin. Most of those technologies have been developed for commercial uses in the first place, but they have also provided governments with ways to start bringing the Internet under the rule of law.

Presumably, the idea of relying solely on the Netiquette to provide adequate standards for the Internet won’t be regarded as sufficient regulation by a lot of people. It has to be considered that from the early stages of the Internet where it was used


\(^{11}\) ibid.

\(^{12}\) That means to rely on the moral consciousness of the users.
only by a certain number of persons, mostly university and military people situated in northern America, the group of users has changed its face immensely in the last few years. Children and teens have become heavy users of the Internet and tend to be drawn to this new and exciting medium. People around the world from different cultures are connected to Cyberspace. While it was relatively easy to maintain Netiquette in the small and predictable group of early users, it became more and more difficult with increasing variety.

Along with the benefits came risks, including exposure of children and teens to illegal or offensive material on the Internet and contact with individuals who may jeopardise the safety of Internet users. New technologies provide the opportunity to commit new kinds of crimes or traditional crimes using the new means. The advantages offered by the Internet can rapidly disappear if users feel insecure and can’t enjoy the freedom of the new medium. Therefore the calls for regulation became louder and more urgent over time.

In most countries what is illegal offline also is illegal online. The main concern of regulators appears to be various forms of cybercrime and pornography, with particular emphasis on its availability to minors, and the fight against child pornography. However, measures implemented with the intent to combat illegal content usually include among others provisions for the regulation of hate crimes. But these are just the “basics” and the criminal codes and laws differ from country to country. Even the definition of pornography and hate crimes is very controversial. What may be acceptable and legal in one country might be unacceptable in another. Nevertheless child pornography and hate propaganda are particularly troubling, because they pose the greatest and most immediate risk to safety and well-being of users.
The borderless flow of information on the Internet made it clear that international regulation is necessary to combat cybercrime and illegal content. But to find a balance between all the divergent laws, opinions and views and to create an international law that is efficient and not just a watered-down piece of legislation, and therefore useless, is not an easy task. An attempt to create such a document was made by the Council of Europe and led to the first international treaty on criminal offences.

3.2.1 *The Convention on Cybercrime (CCC)*\(^{13}\)

_Council of Europe (CoE)_

The Convention on Cybercrime is the first international treaty on criminal offences committed against or with the help of computer networks such as the Internet. Its main aim, as set out in the Preamble, is to pursue "a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international co-operation."

The CCC was signed on 23 November 2001 in Budapest, by 26 Council of Europe member States\(^{14}\) and the four non-member States which had helped with the drafting (Canada, Japan, South Africa and the United States). It will come into force as soon as five states, at least three of which must be Council of Europe members, have ratified it. This binding treaty will be able to be opened at a later date to other non-member States, at the invitation of the Committee of Ministers.

The CCC is the product of four years of work: In 1997, the Council of Europe's Committee of Ministers asked a committee of experts to "draft a binding legal

---


\(^{14}\) Albania, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the Former Yugoslav Republic of Macedonia, Ukraine and the United Kingdom
instrument" examining the issues of offences, substantive criminal law, the use of coercive powers – including at international level – and the problem of jurisdiction over computer crimes. In April 2000, the draft text was declassified and made public on the Internet so as to garner the opinions of professionals and network users. In March 2001, the Parliament Assembly held a hearing of international experts and then adopted an opinion on the draft text at its April plenary session. The Council of Europe Ministers' Deputies approved the CCC in September 2001. On 8 November the CCC was presented for formal adoption to the Foreign Affairs Ministers meeting in Strasbourg.\textsuperscript{15}

The Convention pursues three aims:\textsuperscript{16}

- to lay down common definitions of certain criminal offences, enabling national law to be harmonised;
- to define investigation and criminal prosecution methods appropriate to the computerised environment and enabling national criminal procedure to be brought more closely into line with each other;
- to define ways and means of co-operating internationally against cybercrime.

The criminal offences concerned are:\textsuperscript{17}

- those committed against the confidentiality, integrity and availability of computer data or systems (such as the spreading of viruses);
- computer-related offences (such as virtual fraud and forgery);

\textsuperscript{16} Guy de Vel, "The cybercrime convention : a pioneering effort of wide legal scope", Conference on Cybercrime, Budapest, 22-23 November 2001
- content-related offences (such as the possession and intentional distribution of child pornography);
- offences related to infringements of intellectual property and related rights

Another objective of the CCC is to facilitate the conduct of criminal investigation in cyberspace by establishing a number of procedural powers, such as the power to preserve data, to search and seize, to collect traffic data and to intercept communications.

Although at the opening Conference on Cybercrime, Guy de Vel, Director General of Legal Affairs at the Council of Europe, pointed out that “the text covers only specific criminal investigations, and certainly does not lend itself to the setting up of an Orwellian-style general electronic surveillance system” and that the Convention had been drawn up with care so as to strike “a precious balance between the requirements of criminal investigations and respect for individual rights”\(^\text{18}\), the CCC was, during its drafting, and still is subject to massive critique from various sides for multiple reasons.

a) Drafting Process

Industry and several NGOs have criticised the non-transparent manner in which the CCC has been developed. Although it was published on the Internet for comments only little effort on the part of the working group of the CoE to directly incorporate the views and concerns of the industry and NGOs on the issues of privacy and civil liberties have been made. The makeup of the working party remained one-sided, with law enforcement at the table and no industry or NGO participation. A large number of

\(^{18}\text{supra note 16}\)
the deficiencies criticised apparently result from the fact that the CoE has not made the best possible use of the available expertise in the matters concerned.\textsuperscript{19}

b) Protection of privacy and data protection

- Article 15

\textbf{Article 15 – Conditions and safeguards}

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, \textit{inter alia}, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Although the legal protections of privacy and personal data in Article 15 have been improved by the reference to various international human rights instruments many data protection experts and civil liberties groups believe that the protections it affords are not adequate to address the significant demands and requirements for privacy-invasive techniques in the rest of the Convention.\textsuperscript{20}

\textsuperscript{19} See, for example: Opinion 4/2001 of the working party on the protection of individuals with regard to the processing of personal data (22 March 2001) online: <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41en.htm> (date accessed: 30 December 2001)

The section does not specifically address the issues of privacy and data protection. The CCC did not fully adopt the important safeguards for protecting citizen’s rights which are lined out in various international documents, like the CoE Convention 108 on Data Protection or the 1997 OSCE cryptography guidelines.\textsuperscript{21}

The requirements for adequate judicial or independent supervision in Article 15.2 are vague and do not set any standards for independence; the definition of independent supervision may vary greatly across nations. Furthermore, under Article 15.3 countries are not explicitly required to pay the costs imposed on third parties for their demands for surveillance. Industry commentators have consistently asked for the inclusion of reimbursement requirements\textsuperscript{22}, because only then must governments consider how much surveillance they actually can afford, and requiring law enforcement to pay for their surveillance provides an important level of accountability through the budget process each year.

- Real-time collection of computer data and Interception of content data

### Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
   a. collect or record through the application of technical means on the territory of that Party, and
   b. compel a service provider, within its existing technical capability:
      i. to collect or record through the application of technical means on the territory of that Party; or
      ii. to co-operate and assist the competent authorities in the collection or recording of,
         traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

\textsuperscript{21} see also: Chapter I, 1.10 Privacy at 29
\textsuperscript{22} supra note 20
3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:
   a collect or record through the application of technical means on the territory of that Party, and
   b compel a service provider, within its existing technical capability:
      i to collect or record through the application of technical means on the territory of that Party, or
      ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 20 and Article 21 mandate that the parties adopt legislative and other measures to empower their law enforcement authorities to directly collect or record content and traffic data with or without the participation of the service providers. A service provider is required to co-operate “within its existing technical capability”, a passage that was included after heavy protests of ISPs which feared the burden of having to install expensive surveillance equipment at their own cost. The interception of content data is only allowed in relation to a range of serious offences which have to be determined by domestic law. Without sufficient privacy and data protection which is noticeably lacking in the CCC (see above) these provisions threaten human rights.23

Allowing law enforcement direct access to a service provider’s network to conduct surveillance24 provides police with the ability to conduct broad sweeps of network communications with no control that they will only collect that data that they are lawfully entitled to collect. This may invite abuse of the most invasive investigative

24 for example the US Carnivore programme
powers. It also represents a threat to the integrity of a providers' network. Consumers won't have sufficient trust and confidence in the products and services of ISPs in case it is not clear who has access to confidential information and communications and when access can occur. Internet business may lose important momentum and participation if the legal safeguards are not clearly in place and businesses don't have concrete ideas as to their obligations and their concrete implementations. The term "serious offences" is rather vague and its definition may vary from one legal system to another.

- Mutual assistance in the absence of international agreements

**Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements**

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
   b The central authorities shall communicate directly with each other;
   c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;
   d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
   a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
   b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or
postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 27 of the CCC obliges the parties to designate a central authority that is responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities designated for their execution if there is no agreement on mutual assistance with the party concerned. Within this obligation data collected in one state, party to the CCC, can be transferred to another state party to support the investigation in criminal matters described in the Convention.

Therefore it is possible that data which was collected in a country which is obligated to guarantee a high level of data protection may be transferred to a country which does not have such guarantees in place, especially because the Convention contains the possibility that states which are not CoE members can nevertheless become parties to the CCC. There is a discrepancy in treatment of CoE member countries and others because CoE members have to respect their obligations following from the European
Convention on Human Rights, CoE Convention 108 on Data protection, relevant CoE Recommendations, the EU Charter on Fundamental Rights, the EU Data Protection Directives and relevant national legislation whereas non CoE countries don't have the same or similar obligations. The CCC does not ensure that the fundamental rights of individuals are adequately protected once the data concerning them have been received from the requested party by the requesting one. Conflicts could arise between the obligation to assist and the obligation to respect fundamental rights as granted by the European instruments and relevant jurisprudence.

- Dual criminality

A deep concern is the treaty's failure to consistently require dual criminality as a condition for mutual assistance. No nation should ask another to interfere with the privacy of its citizens or to impose onerous requirements on its ISPs to investigate acts, which are not a crime in the requested nation. Governments should not investigate a citizen who is acting lawfully, regardless of whatever mutual assistance conventions are in place.

- Encryption (Article 19.4)

Article 19 – Search and seizure of stored computer data

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

The use of encryption technology has been liberalised in the last few years after considerable international debate over surveillance. Only a few authoritarian

---

25 supra note 19, Several EU member States have implemented Directive 95/46/EC in the third pillar for processing of personal data in criminal matters. Their national laws thus require that personal data can in principle only be sent to non-EU countries if these countries do provide an adequate level of protection of individuals with regard to the processing of their personal data.

26 supra note 20
governments such as China still do not permit its use. Article 19.4 seems to require that countries adopt laws that can force users to provide their encryption keys and the plain text of encrypted files to the authorities.

The approach in this article also raises the issues involving the right against self-incrimination, which is respected in many countries worldwide. The privilege against self-incrimination forbids a government official from compelling a person to testify against himself. Requiring the disclosure of encrypted documents may violate the right against self-incrimination. Many European scholars believe that requiring the disclosure of encryption keys violates the European Convention on Human Rights. The EHCR has stated that the right of any "person charged" to remain silent and the right not to incriminate himself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6 of the European Convention on Human Rights. The burden of proof cannot be reversed for the suspect to provide the requested evidence or prove his/her innocence.  

In the U.S., this issue has not been directly addressed by any courts yet but many legal scholars believe that it would not be permissible under the 5th Amendment of the Constitution to force an individual to disclose an encryption key or pass code that was not written down anywhere.

c) Additional Protocol to ban racist and hateful content


The CCC will be supplemented by a protocol eliminating racist and hateful web sites from the Internet and defining and criminalising hate speech on computer networks. The category of content-related offences in the Convention only concerns a number of acts connected with child pornography. There are many people, especially in Europe, who would have liked the convention also to make it an offence to disseminate certain unlawful content, such as racist propaganda, via the Internet.29

But the issue of racist Web sites was dropped from the convention itself because co-signatories including the U.S. opposed such a ban. The U.S. Constitution’s First Amendment, which guarantees freedom of speech, would have prevented the U.S. from signing the whole convention. To avoid such a consequence the issue was separated in the additional protocol.

A specific committee of experts will draw up within a year a draft protocol to be added to the convention. The protocol will have two levels: those countries that go ahead and ban racist online material in their country by signing the additional protocol; and those countries that don’t sign, but agree to remove such material if it originates in their country and is aimed at an audience in another country.30 The protocol especially should consider ways of preventing “illegal hosting” – a practice whereby servers hosting racist or hateful content are being located in a country with less strict regulations in order to sidestep the law. A recent report estimates that at present there are around 4,000 racist Web sites, including 2,500 in the United States.31

But it will have to be seen how much effect the additional protocol will have, especially in the U.S. A source at a well-known Internet company said that “It is very unlikely the

29 supra note 16
United States would co-operate in the way the CoE would want it to by removing Web content classified as racist by another country's courts. The Justice Department fought hard to have the racist bits pulled from the Cybercrime Convention itself. I can't imagine they will let freedom of speech be curtailed via the backdoor in this way.\footnote{supra note 27} This opinion is also backed up by several civil liberties groups that oppose the additional protocol, because it may threaten recognised free expression rights in many nations.\footnote{supra note 24}

We have to face the fact that cybercrime is part of the new age of the Information Society. Due to the borderless character of the Internet the response to these criminal problems can come only from concerted action by the international community, each individual state being unable to deal on its own with offences committed transnationally. No investigation will be able to progress without efficient and speedy international co-operation.

The CoE has a longstanding experience and tradition both in international co-operation in criminal matters as well as in Human Rights. I generally support the efforts being made by the CoE to combat cybercrime in the way that they can contribute to improve security for all users of the Internet. But it seems to me that the CoE has not paid enough attention to the need to strike a fair balance between the efforts to combat cybercrime and fundamental human rights, such as the rights to privacy and personal data protection of individuals as regards the extent to which measures are proposed in the CCC. Due to the "newness" of the CCC it is difficult to predict its effectiveness in the fight against cybercrime and its influence on fundamental human rights. In my opinion it is a necessary step in the right direction to combat criminal activities in
cyberspace. Nevertheless its application and implementation must be watched carefully to ensure the protection of fundamental human rights.

As the Internet grew not only cybercrime, but also the wealth of information readily available on the Internet to those who posses the technological means to access and contribute to it have worried governments around the world, and in many countries restrictions on the Internet have been posed by them in an attempt to limit the presence within their borders of information that they deem offensive and threatening. A host of measures have been invoked by authorities, particularly in several authoritarian regimes in Asia, which has become a hot-bed for all kinds of censorship.34 A prominent example for that fact is China:

3.2.2 Internet in China

Since 1995, when Chinese authorities began permitting commercial Internet accounts, the government became more and more determined to censor on-line content and to tighten controls on ISPs and users. As recently as July 11, 2001, President Jiang Zemin condemned the spread of “pernicious information” on the Net and called existing legislation “inadequate”.35 Improved infrastructure, the introduction of mobile phones and other low-cost methods of connection to the Internet, as well as increased local language content, have fuelled its growth. By July 2001 there were some 620 Internet Service Providers who served some 1,600 Internet Content Providers and an estimated 26,000,000 users by the government’s own conservative estimates.36 Sales of personal computers are booming, and China’s leaders have often stressed the

---

35 Agence France Presse, “Jiang Renews Warning Against “Pernicious” Internet”, July 11, 2001
36 “China to Speed up Internet”, People’s Daily (11 July 2001). See also: online: China Internet Network Information Center Annual Internet Survey <http://www.cnnic.net.cn/develst/e-cnnic200101.shtml> (date accessed: 16 September 2001)
importance of keeping up with the United States, Europe and Japan in developing Internet technologies.

Nevertheless at least sixty sets of regulations have been issued aimed at controlling Internet content. The regulations became progressively more comprehensive, moving from efforts to regulate Internet businesses to restrictions on news sites and chat rooms. These regulations give the government wide discretion to arrest and punish any form of expression. Violation of the regulations can lead to severe punishment. Content and service providers may face fines or closure, and users found in violation may face the death penalty for posting materials that is not to the government’s liking.

Furthermore in attempts to filter and block contents on the Internet all Internet traffic is configured to be routed through two major gateways in Beijing and Shanghai, where the communications system is designed to pass through a few key “choke points”, making censorship relatively easy. Working from this system, Chinese authorities have managed to block access to a number of sites and areas on the Internet that they believe offer material unsuitable for its citizens or that run contrary to its rigid culture, including those which express dissident viewpoints from Hong Kong and Taiwan; major media organisations from the US and elsewhere, sexually explicit sites such as Playboy, and politically sensitive sites dealing with Tibetan independence and human rights issues. Additionally, many Usenet groups are not allowed on Chinese Internet host computers.

In practice in addition to government censorship and regulations Internet service and content providers and Internet cafes have set up their own monitors to avoid legal consequences. In Internet cafes, managers have appointed people who patrol the

38 ibid.
monitors checking what material appears on the screen. They have also issued their own sets of guidelines for users. Despite these measures over 2,300 cafes have been closed down between April and July 2001. Several individuals have been detained as a result for posting material on the Internet.39

The government lifted the long-standing blocks during the summit of the Asia-Pacific Economic Co-operation Forum in October 2001 and China’s leaders went to great lengths to demonstrate that they run a modern, cosmopolitan nation ready to play a leading role in global affairs. But as soon as U.S. President Bush and other guests were well on their way home, China’s Internet censors had restored the blocks.40

The success of all these attempts is questionable. The special nature of the Internet is the reason why such efforts to block or filter information are circumvented with regularity. A government can only try to control content within its own jurisdiction. Setting up mirror sites in other countries where the posting of those kinds of content isn’t illegal and transmitting the “forbidden” content back into the country is relatively easy and common practice in the Web community. There is no effective way of counteracting this.41 Web sites can also be reached by determined Internet users sophisticated enough to connect through third-party servers known as proxies.

"The nature of the Internet is such that once it gets in, as long as there’s a human spirit, it will find a way to get around any attempts at blocking, or controlling the

---

39 ibid.
41 supra note 23
content, and it therefore becomes a universal, neutral medium for the transmission of information.”

For the moment, though, the movement of traffic along China’s information superhighway is slowed by official checkpoints and government censorship.

But it is not just in Asia where undemocratic regimes have imposed restrictions on the Internet which impact free expression. With the Internet growing more popular in the Gulf States, those countries’ leaders are attempting to limit access to certain areas of the Internet, too, because the information available might contravene the rules of their strict Islamic societies.

To be sure, it is not only in undemocratic regimes where restrictions have been imposed and censorship is present, even in western democratic countries content control is commonly attempted, although governments here tend to encourage self-rating of content and to urge the industry to develop and deploy tools for blocking inappropriate speech; to avoid direct government censorship and especially after several attempts to “legislate” the Internet have failed:

3.2.3 The United States and the Communications Decency Act (CDA)

The protection of users and especially children online has been a powerful motivating issue for policymakers since the Internet became widely available. Policymakers have found no easy and effective response to the problem of protecting children online.

43 ibid.
Laws directly restricting potentially harmful content online have encountered technical and constitutional difficulties in many countries. The effectiveness of domestic law in the global context of the Internet has been called into question, U.S. courts have struck down the same laws for infringing First Amendment rights of American adults. These difficulties have led to a cycle of legislation, litigation, and court action, but it has provided little in the way of solutions for users seeking to deal with inappropriate content online.45

The CDA was signed into law in 1996 by President Clinton to protect children by prohibiting “indecent” speech or images from being sent via the Internet. It imposed heavy punishments for the transmission of indecent or patently offensive materials over a public computer network to minors or in a manner available to a minor.46

Numerous civil right groups, led by the American Civil Liberties Union (ACLU), decried the law as an unacceptable infringement of the First Amendment of the American Constitution which protects freedom of expression. They argued that the statute was so vague and poorly worded that it “would have criminalized speech that would have never been criminalized before.”47 In July 1997 the Supreme Court unanimously struck down the law, deeming it unconstitutional. One of the reasons was that in the absence of any dependable way of screening users according to age to avoid minors, the CDA was an effective ban on the transmission of indecent materials between adults who have a right to receive and send such material.48 The decision grants Internet speech

---

46 supra note 44, sec. 502, 503
47 Department of Canadian Heritage, Department of Industry and the International Comparative Research Group, “Combating Hate on the Internet: An International Comparative Review of Policy Approaches” (Report) by H. De Santis (January 1998) 33
at least the same amount of protection that the courts have granted to print media under the First Amendment.

The Court, however, did not rule that the government cannot regulate the Internet at all. And while civil rights groups still were celebrating their victory over government Internet censorship, the Congress started a second attempt to censor speech on the Internet in form of the Child Online Protection Act (COPA)\(^49\), passed in 1998, which is not as censorious as the CDA but still imposes severe criminal and civil penalties on speech on the Web that is “harmful to minors” according to “contemporary community standards”.\(^50\)

COPA was first blocked in February 1999 by a federal court in Philadelphia. The court held that the law was invalid because there is no way for Web speakers to prevent minors from harmful material without burdening adults from access to speech protected by the First Amendment.\(^51\) The Third Circuit Court of Appeals affirmed this finding in June 2000, saying that COPA was unconstitutional for an additional reason. “Because of the peculiar geography-free nature of cyberspace, [COPA’s] community standards test would essentially require every web communication to abide by the most restrictive community’s standards.”\(^52\) Web speakers have only limited possibility to determine the characteristics of their audience – whether age or geographic location. Standards aimed at minors may censor adults as well, and what might be illegal in one country might not be illegal in another. In my opinion it can’t be argued that certain community standards of one country have become reasonable constant across the globe. Even in the United States attitudes about providing sex education

\(^{49}\)“Child Online Protection Act” (COPA) 47 U.S.C. §§ 230, 231 (1998); An Act to amend the Communications Act of 1934 (47 U.S.C. 201 et seq.)

\(^{50}\)ibid., §§ 1402, 1403


\(^{52}\)ibid. (“Ashcroft v. ACLU, et al.” [2001] SCT-QL 167 (Order List 533 US Supreme Court 00-1293) online: QL (SCT))
materials to children, or information about sexual orientation, vary widely by region. There might exist a certain worldwide consensus on community standards in some areas, but it would be rather difficult for local courts to determine them. Therefore, while acceptable in narrow circumstances for other media, community standards test should not be applied to the Internet.

Again, ACLU, supported by numerous civil rights groups, filed a legal brief on September 20, 2001 at the Supreme Court. The Court scheduled an argument date for the 14th of February, 2002; a decision will be expected in June 2002. It will have to be seen if the landmark decision of 1997 will be repeated.

At the same time COPA was enacted the Congress established the Commission on Online Child Protection to study “methods to help reduce access by minors to material that is harmful to minors on the Internet”. Congress directed the Commission to evaluate the accessibility, cost, and effectiveness of protective technologies and methods, as well as their possible effects on privacy and law enforcement. The Commission filed a final report to Congress by October 2000. The Commission’s specific recommendations included:

- Public Education: Government and the private sector should undertake a major education campaign to promote public awareness of technologies and methods available to protect children online. They should also promote acceptable use policies.

- Consumer Empowerment Efforts: Resources should be allocated for the independent evaluation of child protection technologies and to provide reports to the public about the capabilities of these technologies.

---

54 supra note 45
55 ibid.
Industry Action: The online commercial adult industry should voluntarily take steps to restrict minors’ ready access to adult content. ISPs should voluntarily undertake “best practices” to protect minors.\(^{56}\)

But despite the COPA Commission’s experts’ advice Congress passed in the year 2000 as part of a massive budget bill a law called the Children’s Internet Protection Act (CIPA), the latest in a long line of attempts to regulate Web content in the U.S. which forces schools and libraries that receive government funding to block Web images deemed harmful to minors. CIPA represents a more tailored attempt at regulating content. Unlike the two previous acts, it restricts only visual depictions, affects only schools and libraries, and ties restrictions to federal funds.\(^{57}\)

It is also facing legal challenges from groups including ACLU and the American Library Association (ALA)\(^{58}\). They argue that the bill not only violates the First Amendment by restricting content in libraries, furthermore the bill accelerates the digital divide by forcing people who don’t have a computer at home to surf a filtered Web.\(^{59}\)

Although the cases concern U.S. legislation, a number of crucial points of general interest for Internet regulation were raised:

- The censoring of content potentially harmful to minors will ultimately always lead to censorship of material that would be legally available to adults because of the impossibility to differentiate users by age.

\(^{56}\) ibid.
\(^{58}\) "Multnomah County Public Library et al. v. United States Federal Communications Commission et al." [2001] PA-QL 438 (E.D.PA No. 01-1322) online: QL (PA)
\(^{59}\) CIPA also presents a technical challenge, partly because it requires the blocking only of visual depictions. Developers of filtering software warn that the technology for such narrow laws maybe can’t be delivered at present time.
The ultimate decision what the user wants to see on the Net should stay with the user, and should not be regulated by government. Those responsible for minors should undertake the primary obligation to prevent their exposure to harmful material.

The Internet raises the question as to what community standards it has to be judged by. Given the global structure of the Internet, where information travels around the world, the application of community standards simply made in USA or elsewhere is not acceptable.

In my opinion there is a wide span between censorship and total government control and providing a legal framework to keep up a certain level of "culture" on the Net. Most countries agree that the Internet is not operating in a legal vacuum: existing laws concerning freedom of expression, media regulation and so on are perceived to be applicable to Internet content, too. Therefore, new Internet-specific legislation is not generally seen as necessary to address problems of Internet content. Some countries fine-tune existing laws to make them more applicable and enforceable in the changing world of global networks. Considering the major difficulties and opposition from various sides countries that attempted to create new legislation have experienced, the tendency at least in democratic countries is to educate the public and promote the awareness that existing law applies to computer mediated communications, encourage the development and adoption of voluntary codes of conduct of the Internet industry, promote research and development of technical tools that protect users against offensive content on the Internet, and assist law enforcement.

They also do so, not only because they want to protect the freedom of speech, highly valued and guarded in democratic societies, but also because censorship on government level has many pitfalls which can be observed in reality in diverse
countries like China; but there are also many studies that point out the problems. But how effective are all those measures?

First of all, while a number of technologies exist that can be applied toward the regulation of the users' access to Internet content, none of these technological approaches will effectively and entirely prevent users from accessing content that violates pre-defined rules of acceptability. Blocking and filtering technologies are of limited accuracy, because there are a number of technical means to circumvent those systems. Even the most sophisticated software that makes it possible to block content and track people based on their physical location is far from foolproof. 60

Second, even in a relative small environment such as a corporate Intranet, blocking and filtering of content are expensive to implement and to maintain and they impose delays and inefficiencies in network performance. On the national scale such measures have enormous cost and performance implications. The Internet of a country would become uncompetitive with the rest of the world and that would result in economic disadvantages.

Therefore it can be said that it may be possible for a country to control Internet content within its borders to some extent, but only if it is prepared to accept considerable costs in terms of technological infrastructure, human resources, enforcement mechanisms, and social, economic, and legal consequences.

The solution seemed to be self-rating schemes and Internet filtering software available for ISPs and users, applied on their own servers and in their own homes, on their own

60 "Yahoo in Frankreich verurteilt" (ORF ON Futurezone 2000) : A panel of three technical experts advising the French court in the Yahoo case concluded that IP address tracking could spot only about 70 percent of the portal's users in France. online: ORF ON Futurezone Homepage <http://futurezone.orf.at/futurezone.orf?read=detail&view=bw&id=52427&tmp=24436> (date accessed: 10 October 2001)
computers to make government censorship unnecessary. Even free speech activists saw that software as providing the answer to the dilemma of government regulation of Internet content. Indeed, some of the strongest supporters of blocking software were free speech activists who sharply opposed direct government censorship of the Net. But their initial enthusiasm has turned into concern or even opposition of self-rating schemes and blocking software. The reasons why will be explained in the following section.

3.3 Self-rating Schemes and Filtering and Blocking Software

The use of rating systems as well as filter and blocking software has been considered as an alternative to other measures in order to control the presence and accessibility on the Internet of content deemed illegal or harmful or objectionable by governments or others.

There are basically two technological approaches to restricting access to content on the Internet:

a) blocking requests for identified unacceptable content using a list of prohibited sites, and

b) filtering of content by identifying prohibited text strings on the basis of partial or full-text searches or, by detecting rating labels attached to the content.

Filtering and blocking of content can take place on several levels in the structure of the Internet:

Exercised by national governments as a means of political control and censorship over their citizens.

by ISPs (on behalf of governments or on their own behalf)

by the users themselves

Most rating systems today follow the PICS specifications. The PICS specification enables labels to be associated with Internet content. It was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing and privacy. The PICS platform is one on which other rating services and filtering software have been built. PICS is a rating standard that establishes a consistent way to rate and block online content, it is not a rating system in itself. PICS was developed by the World Wide Web Consortium, the body responsible for developing common protocols and reference codes for the evolution of the Web and the participation of major Internet industry leaders. In theory, PICS does not incorporate or endorse any particular rating system – the technology is an empty vessel into which different rating systems can be poured. The ratings can be assigned by the content creators themselves, or by third parties, or by the creators of filtering or blocking software. Varying groups can seek to establish ratings that reflect their own values.

The particular approaches of rating systems differ:

First, there are those systems where the author himself rates the content he created (self-rating systems), like the one of the Internet Content Rating Association (ICRA).

---

63 Platform for Internet Content Selection [hereinafter PICS], for more detailed information visit online: W3C World Wide Web Consortium <http://www.w3.org/PICS/> (date accessed: 19 December 2001)
65 online: Internet Content Rating Association <http://www.icra.org/> (date accessed: 19 December 2001)
which is an international, independent organisation. There are two elements to the system: Web authors fill in an online questionnaire describing the content of their site, simply in terms of what is and isn't present. ICRA then generates a content label (a short piece of computer code) which the author adds to his/her site. Users can then set their internet browser to allow or disallow access to web sites based on the objective information declared in the label and the subjective preferences of the user. A key point is that ICRA (or any other self-rating system like it) does not rate internet content itself - the content providers do that, using the ICRA system. ICRA does not promote any filtering software of its own, but filtering software can be developed by the industry based on the ICRA labels.

This may sound like the perfect solution; one might figure, if authors evaluate their own sites, they could hardly disagree with the ratings they chose. In reality, that matter, though, is not so clear. When an author rates his site with any PICS-compliant rating service, he must follow the algorithms and rules of that service, weather he likes them or not.66 It is a matter of fact that no rating system can classify documents in a perfectly satisfactory and objective manner, and this theoretical inadequacy has important real world consequences concerning the accuracy of self-rating schemes and filtering software.67

All rating system designers face the same dilemma. To create a rating system they can rely either on rules or on standards. Legal thought teaches that both, rules and standards, each have their disadvantages. Standards allow evaluators to consider more factors, in a more situational specific manner, and to capture the essence of a site; but they will only work within a community of shared values, so that the evaluators can draw on the same norms and assumptions in applying the value judgements

67 supra note 61
embedded in the standards. The system will allow more flexibility, but will lack consistency and predictability.\textsuperscript{68}

Rules become increasingly necessary as the number of content evaluated grows, and evaluators are less able to rely on shared culture and values as a guide to applying standards in a relatively consistent and coherent way. They have to use simple, hard-edged categories, relying on a few, easily ascertainable characteristics of each site to achieve fairness and consistency in the rating system. Those categories, however, will probably not reflect the diversity of content on-line and most users won’t find them very useful in rating their content. They also won’t empower users to decide according to their own values what speech should or should not be blocked.\textsuperscript{69}

It seems even worse, if not the author himself rates his content, but third-party labelling services such as Cyber Patrol\textsuperscript{70} or CYBERSitter\textsuperscript{71} do so. Authors complaints about ratings of their content are magnified; and almost no third-party rating service takes steps to inform content providers of the ratings it assigns to their pages, in fact, their ratings are trade secrets and not disclosed.\textsuperscript{72} The list of blocked sites is sometimes surprising and alarming.\textsuperscript{73} Cyber Patrol, for example, blocked the Web site of the League for Programming Freedom (a group opposing software patents), the Electronic Frontier Foundation’s censorship archive, the National Organisation of Women Web site, or animal-rights web pages because of images of animal abuse.\textsuperscript{74} Content providers can discover their ratings only by buying the various blocking software and searching for their own sites. Depending on the software users have either no or just

\textsuperscript{68} ibid.
\textsuperscript{69} ibid.
\textsuperscript{70} See online: Cyber Patrol Homepage <http://www.cyberpatrol.com/> (date accessed: 19 December 2001)
\textsuperscript{71} See online: Cybersitter Homepage <http://www.cybersitter.com/> (date accessed: 19 December 2001)
\textsuperscript{72} supra note 61
\textsuperscript{73} For more details see, for example, online: National Coalition against Censorship Homepage <http://www.ncac.org/issues/internetfilters.html> (date accessed: 10 April 2002)
\textsuperscript{74} ibid.
little choice of what content will be blocked. One of the consequences of buying off-the-shelf blocking software is that the values of the rating services are reflected in the ratings and the users should make sure that they are at least in basic agreement with those values.

A main problem of blocking and filtering software is that it only can work if all sites are rated. Otherwise, the software must either exclude all unrated sites, barring innocuous speech, or allow unrated sites, letting in speech that the user would prefer to exclude. Considering the huge amount of new pages that come on-line every day and that the content associated with any given page can constantly change, no rating scheme could be big enough to rate the entire Web. The other option is to simply block all unrated sites. Industry members seem to contemplate this as the necessary solution. Microsoft, for example, cautions Internet content providers that "[for] a rating system to be useful, the browser application must deny access to sites that are unrated." 

The result: To make sure that their content won't be blocked in the first place content providers have either to self-rate their sites, even if they don't like the idea, or leave the rating up to a third-party rating service and hope for the best.

Therefore the consequences of rating are far from neutral. The ratings themselves are all pejorative by definition, and they result in certain speech being blocked. While in the "real world" publishers of books and magazines don't have to rate each and every article or story they publish, or every person engaged in a streetcorner conversation has to rate his or her comments, any kind of speech that appears online will be subject to the rating schemes, because, as mentioned above, if content providers for whatsoever reason decide not to rate their sites, they will be blocked anyway, even if they don't provide illegal or harmful content; and while the same material in print form

75 ibid.
could be distributed on any streetcorner or in any bookstore without worrying about rating it, on the Internet it would be blocked from reaching a large portion of audience, before the users even know that it exists.

And what happens if somebody decides to mis-rate his/her site in order to reach a wider audience and to penetrate the existing filters and blocking software? Who will be in charge to hold those content providers liable? In the end, it will have to be the government that has to impose penalties for mis-rated content, because without a penalty system for mis-rating, the entire concept of self-rating schemes breaks down; and only the state has the coercive means to enforce penalties for mis-rating.

It gets even more difficult with conversation. Many Internet users don’t run web pages, but millions of people send messages to chat rooms, news groups or mailing lists every day. A rating requirement for these areas could be compared with the requirement to rate all our telephone or dinner party or street conversations. People will stop using the Internet to exchange and discuss information on topics that may be controversial or unpopular.

In the end the Internet will turn into a homogenised medium dominated by large commercial speakers, because for those who have the money to hire legal counsel and staff to apply the necessary ratings to reach the widest audience possible, rating systems will impose only minimal burdens. Smaller commercial and individual speakers may neither have the money nor the time or will to rate their content and their speech will disappear. While it is today still just as easy to find the Disney site as it is to find the Critical Path AIDS web site, it may easily be that the Internet will turn into a bland, homogenised medium dominated by powerful corporate speakers.

76 supra note 64
77 ibid.
It also has to be pointed out that most of the available filtering and blocking software as well as labelled sites are mainly in English. Due to that fact access to content in other languages, which is either not labelled or would be considered as unrated by filtering software in English, would be denied. Although English can be considered as the main language used on the Internet, still, probably at least half of all Internet speech is not in English. Imagine the wide variety of speech totally appropriate and valuable for anybody being blocked just because it is not in the "right" language. The fundamental cultural diversity of the Internet will be distorted.

Although most blocking and filtering schemes are intended to restrict children's access to questionable sites, it will affect what adults see on the Net, too. This can be seen in a variety of contexts:

In the home, parents may have set up filters to protect their children from entering material, which they consider inappropriate for them, but which may be completely appropriate to see for adults. But will those filters always be disabled for their own use? There is a variety of reasons I doubt that. For example, you just want to have a quick look at the news and don't want to bother resetting your browsers, or you forgot that the filters are on at all. You might also have subscribed to an ISP that filters out material at the server level, even without letting you know about it. Rating and filtering systems enable invisible "upstream" filtering by ISPs or other entities.


79 So-called "Stealth blocking": ISPs intentionally block their customers from accessing certain Web sites or sending e-mail to users at certain other ISPs. The blocking is done undetectably, so users only see a browser error saying that a Web site is down or an e-mail error saying that the destination mail server could not be reached. Over 99% of end users never discover that any intentional blocking is being done. Of course, this does not include ISPs that advertise a filtering service the customer is aware of, even if he might not know about all sites being blocked.
A lot of people get Internet access through public places, like libraries, or through their employers at their work place. Library computers may be blocked for reasons of politics or to avoid legal consequences, if, for example, somebody enters illegal content like child pornography via a library computer. Corporations may put stringent filters in place in order to avoid the risk of wasted work time and profit loss. In sum, large amounts of content may end up off-limits to a substantial number of adults.

Last, but not least, how long will it take before governments again make use of an Internet already configured to accommodate massive censorship? As mentioned above, PICS is just an empty technological vessel, in which any rating system by whoever can be poured. If the use of PICS becomes universal, it provides a uniform method for content rating around the globe. At the moment only very few rating systems dominate the market and they can de facto become standard for the Internet. Those systems can be built into every Internet software as an automatic default. Unrated speech is effectively blocked by these defaults. The existence of a standardised rating system for Internet content allows governments to mandate the use of such a regime. By requiring compliance with an existing rating system, a state could avoid the burdensome task of creating a new content classification system while defending the ratings protocol as voluntarily and approved by private industry. With PICS built in their network infrastructure, it is much easier for governments to selectively choose which information to let in and which to keep out their country's borders.

---

80 supra note 64; Microsoft's Internet Explorer adopted the PICS standard for its built-in content advisor, and now working PICS implementations are running on millions of desktops connected to the Internet world wide.

81 Australia, for example, has already enacted legislation which mandates blocking of Internet content based on existing national film and video classification guidelines. (Broadcasting Services Amendment (Online Services) Act 1999)

82 Global Internet Liberty Campaign Member Statement on international ratings & filters submitted to the Internet Content Summit, Munich, Germany, 9-11 September 1999, online: Global Internet Liberty Campaign (GILC) <http://www.gilc.org/speech/ratings/gilc-munich.html> (date accessed: 27 December 2001)
Furthermore, as mentioned above, the imposition of civil or criminal penalties for misrating Internet content is likely to follow any widespread deployment of a rating and blocking regime. A state-imposed penalty system that effectively deters misrepresentation would likely be proposed to facilitate effective “self-regulation”. Therefore filtering and blocking pose a great threat to freedom of speech on the Internet. While it is easy to understand the acclaim of parents for filtering software to protect their children from entering material on the Web which they do not wish them to see, everybody has to be aware that filtering comes at a cost. People whose image of the Internet is mediated through blocking software will miss out on worthwhile speech that makes the Internet a unique medium of mass communication. Controversial speech may still exist, but will be only visible to those with the tools and know-how to penetrate filters and blocking software. While dedicated dissidents will be prepared to go through all this trouble, many Internet users won’t have the time nor the will to do so.

Although harder to reach, sex, hate speech and other controversial matters will still be available and governments, frustrated by this fact, will want to implement even stronger legislation or censorship in form of filtering and blocking schemes to combat illegal or harmful content or just to determine what their citizens should be allowed to see. The libertarian ethos of the Internet will become a myth and geographical borders are proving surprisingly resilient, despite the “borderless flow of information”.

In my opinion the Internet user knows best. The primary responsibility for determining what speech to access should remain with the individual Internet user; parents should take the primary obligation for determining what their children should access. If they decide to use blocking software on their home computers, they should be made aware

---

83 ibid.
of the consequences by the producers of this software. The lists of blocked speech should be made available to consumers and industry should develop products that provide maximum user control.

I strongly oppose indirect government coercion or censorship by imposing mandatory Internet self-rating schemes (or from coercing industry to develop them) and mandating public entities or ISPs the use of user-based blocking software, because all these actions take the control out of the user's hands and will destroy the unique character of the Internet.

3.4 Liability of Internet Service Providers (ISPs)

Another pivotal issue in the context of Internet regulation is the liability for content transmitted over the Internet. Many countries have been eager to pass written rules on the subject matter and as we all know, a society's values find an expression in its legal system, therefore the results have been varying in different countries due to differing local values.

Since the Internet makes the world wide distribution and reception of information for the private citizen much easier than it was the case with traditional means of communication, countries also encounter the problem of how to hold the person who creates and distributes such content liable for their actions.84

The primary focus of discussion about content and freedom of expression is of course first on the person engaging in the expression: the author, the filmmaker, the artist etc. Second, if attention goes beyond this point, the focus is on the person receiving the

expression. But especially with regard to the Internet a third actor comes into play, an intermediary who moves the information from the expressing person to the listener.

These intermediaries often have interests in the expression that are considerably different from those of the expressing person. While the manager of an art gallery, for example, may have almost as much interest in the content of the exhibits as the artist, the typical owner of a video rental store will have little or no concern for the content of all the films made available, seeing them only as inventory to be marketed. Along with reduced interest comes reduced knowledge. A bookseller who sells a huge number of different books may never even look beyond their covers.  

Yet if the content of the expression engages civil or criminal liability, the intermediary may find itself put in the same position as the speaker. Such legal responsibility may very well act as a strong disincentive to the intermediary who will act to limit his liability in a way which inhibits the free flow of expression and information. This liability of the intermediary has even more significance on the Internet, because of the anonymity it offers to users and its borderless flow of information. It is very difficult to locate the originator of any particular piece of information, and enforcing laws against that originator if he or she is in a different jurisdiction from the regulator. Given these difficulties, it is tempting for a regulator to turn its attention away from the originator to the intermediary. Internet Service Providers are visible and accessible, unlike the users.

Another central issue in the discussion is not only the civil and criminal liability of ISPs, but also the legal position of the intermediary in the communication process. It has to

86 ibid.
be differentiated between mere access providers, so-called host providers and content providers. These are all third persons who contribute to the distribution of third party content and to confuse the situation even more, some companies perform several or all of these functions simultaneously.\textsuperscript{87}

The situation for mere access providers and content providers is quite clear:\textsuperscript{88}

Access providers only provide the technical infrastructure for connections to the Internet, and do not have influence on the content transported through their lines. They are comparable to the postal service, which also has no knowledge about the contents of the letters it transports. Thus, the access provider is immune from any liability according to the legal situation in many countries.\textsuperscript{89} On the other hand content providers are fully responsible for their own content.

The problem arises in the case of the so-called host providers, who store third party content for use by third persons, either free of charge or against payment, in the form of web space or bulletin boards. In general, they have no influence on the content put up on its servers by the content provider. However, they can also moderate newsgroups and thereby be involved in the process in putting the content together. These frequently changing roles make it very difficult to place host providers in a certain category. Are they located in the same category as content providers and therefore fully responsible for all content they provide; or are they in the same category as access providers who are not held responsible for content at all?

\textsuperscript{87} AOL, for instance, is at the same time a content provider with its own or purchased content on its own pages, an access provider by providing dial-up access to the Internet to its members, and a host provider by giving its members the possibility to store their homepages on its servers for access by third parties.

\textsuperscript{88} supra note 84

\textsuperscript{89} See for example: E-commerce directive of the EU para. 13 (infra note 87), Chapter III, 3.4 Liability of ISPs at 100
Different countries, different solutions:

In the US, for example, there is no civil liability (e.g. defamation) or criminal liability due to CDA Section 230 and its interpretation by the courts. Liability of providers for third party content is completely ruled out. This immunity applies, no matter if the provider knew or did not know about the presence of a third party’s content on its servers, if it paid the third party for its services or if it was aware of the illegality of the content.\(^90\)

In Europe the situation is different: Art. 14 of the E-Commerce Directive of the EU states that host providers have civil liability if the provider knows that the activity is illegal, or if he is aware of circumstances from which illegal activity is apparent. They have criminal liability if there is actual knowledge of the illegality. There is no criminal nor civil liability if the provider, upon obtaining knowledge of illegal activity, acts expeditiously to remove or disable access to the information.\(^91\) There is no obligation for ISPs to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.\(^92\)

Which solution is the “better” one? There are pros and cons that can be argued with both of them. On the one hand, the American solution creates a very clear situation for host ISPs: They are not liable, even if they know about illegal content and leave it on their servers. That far reaching immunity is caused by the very important position of the basic right of freedom of expression in the American legal system and it encourages the free flow of information and freedom of expression, because ISPs need not to be afraid of being liable for anything posted on their servers. It also plays an important role in the expansion of the “Information Highway” and e-commerce,

\(^90\) supra note 84
\(^92\) ibid., para. 15
which is being pushed particularly by the American Internet industry world wide. These economic realities are one reason to avoid limitations on the economic freedom of Internet companies or other providers, wherever possible. Criminal liability of host providers certainly leads to economically unpleasant limitations for those who run such companies.

In Europe, on the other hand, if a host provider has knowledge of certain specific illegal content and it can reasonably be expected to block or delete this content, the host provider must take this action, otherwise it renders itself liable. This is not such an uncommon thing: In many countries world wide, according to their penal codes, you have criminal liability if you know about illegal activities or crimes committed by a third party and you don’t react or try to prevent them, for example by notifying the police. Why should this be different on the Internet?

Therefore even in the Somm-case European critique of the first verdict was more focused on the fact that the prosecution was unwilling to accept that an absolute ban on child pornography on the Internet is not possible by just enforcing German laws; and not so much against the principle of liability of host providers in general. I think that a majority of people would not see a problem with expecting a host provider to permanently block a newsgroup that provides a forum for child pornography, because they see their tolerance end when it comes to this subject.

Such clashes of legal positions will become more and more frequent in a business world where operations are increasingly global. To further illustrate the problem I have included the following case-study:

93 See: Chapter III, Somm case at 64
3.4.1. Yahoo Case

In November 2000 a French judge broke new legal ground when he ordered Yahoo! to erect a "virtual wall" around France, preventing French inhabitants’ access to a US based Web site offering Nazi memorabilia for sale. The case arose when two French groups sued Yahoo! under a French law that makes it illegal to engage in speech related to Nazism, including the display and possession of Nazi memorabilia. The French court imposed the verdict over Yahoo’s objections that it could not selectively deny access to French users and despite the fact that the Internet servers for Yahoo’s auction sites are based wholly in the United States. The French daughter company of Yahoo! Yahoo France was not involved in the auctions. The ruling demanded that Yahoo! shields French eyes from "any other site or service that my be construed as an apology for Nazism" and if Yahoo! won’t comply, fines up to CAD 20,000 per day would have to be paid.

Although Yahoo! now restricts sales of Nazi merchandise on its auction sites, the Internet portal asked an U.S. court to issue a declaratory judgement supporting its view that a French court has no authority over the content carried on its U.S. based Web servers. On November 8th 2001, a federal judge of the US District Court for the Northern District of California said that American courts would not enforce the French court’s order because Yahoo! is protected by the First Amendment of the U.S. Constitution protecting free speech and the American constitutional freedom is beyond the reach of foreign governments to control. The judge wrote that “Although France has the sovereign right to regulate what speech is permissible in France, this court may not enforce a foreign order that violates the protections of the United States

94 Yahoo! is a global Internet consumer and business services company. For further information visit online: Yahoo <http://docs.yahoo.com/info/pr/> (date accessed: 12 November 2001)
96 Yahoo!, Inc. v. La Ligue Contre Le Racisme, 169 F. Supp. 2d 1181, 1189 (N.D. Cal. 2001)
Constitution by chilling protected speech that occurs simultaneously within our borders."

The Yahoo!-France dispute has been closely watched by the Internet industry, free speech advocates, and scholars of international law around the world. The ruling could have broad implications involving free speech on the Internet as well as regarding the growing problem of regulating the Internet globally. It has been viewed as a major test of how the Internet's global reach can be reconciled with conflicting laws intended to be applied within national borders. Therefore reactions after the ruling have been very contrary.

Internet companies and civil liberties groups applauded the decision. "This is a very good ruling for both free expression and commerce online," said Alan Davidson, associate director of the Center for Democracy and Technology, a civil liberties group based in Washington. "The ruling sends a very powerful message to governments around the world. Those countries who seek to reach out beyond their borders to punish Internet users simply because they publish Web sites have now been put on notice that their rulings won’t be enforced in the United States." It was pointed out that each nation has its own conception of what legitimate speech is and while countries should have the power to regulate speech within their borders, they should not have the power to reach out and silence speech elsewhere.

Internet companies further argue that location technology is far from perfect and it is very difficult to determine where a person is when logging on to the Web. Restrictive technology would hinder their businesses and contents arbitrarily blocked could hinder

---

97 L. Guernsay, "Court Says France Can’t Censor Yahoo Site", The New York Times, Technology (9 November, 2001)
users from viewing information that would be available to them under the law of their country.

On the other side it was pointed out that the ruling, if upheld, will give total impunity to all those who seek technological asylum in the United States. If a racist organisation establishes a Web site aimed at influencing audience world wide, situating it in the United States solely to take refuge behind the First Amendment, it would be protected.

The ruling also sends out the signal that the Internet itself with its global reach is still more or less a "no-law-land" and one just has to find the country with the most favourable set of rules for his business to reach the global community.

Therefore the promotion of understanding differences between legal systems gains great significance. It is also the reason why many countries don't believe in legislation imposed on ISP's by the government. They try to find new strategies of combating illegal and offensive content on the Internet by working together with the Internet industry in finding new solutions. They have recognised their common interest in the prevention of illegal content and the need for support in order to be successful.

3.5 Voluntary Codes of Conduct

Self-regulation is increasingly perceived as an effective way to address issues of public concern. It refers generally to standardised, industry led measures that industry sectors use to establish good practices throughout the industry. Central to self-regulation in many industries are voluntary codes of conduct. They can strengthen business and consumer confidence by assuring that the industry is working to meet the challenges posed by conducting business. Although it is not completely clear how
effective those codes of conduct really are\textsuperscript{98}, they certainly help to improve many areas such as labour practices, health and safety standards or environmental management. In addition other organisations – business associations, inter-governmental organisations and NGOs – have developed standards and guidelines industry can rely on.

After facing the dilemma that the Internet is not conducive to traditional forms of content control such as broadcasting regulations and that attempts to regulate the flow of Internet content at a national level have a lot of pitfalls and are easily circumvented governments started to encourage self-regulation to deal with illegal and offensive content on the Internet. Since ISPs provide the interface between users and the Internet, they can perform an important role in combating illegal and offensive content. Other organisations, such as electronic commerce companies, can also play a key role, as can community access sites and other providers of public access to the Internet. Governments work in co-operation with these organisations and experts to encourage effective self-regulation.

Government regulation cannot be flexible enough to keep up with the fast pace at which the character of networks and technology changes. Voluntary industry initiatives have been and will continue to develop from experience and they will be context driven. It is a fact that each industry sector best understands its security needs and its customers’ needs. And since those sectors cross national and regional borders, they are more likely to drive harmonisation and arrive at a common basis. Industry also has a high self interest in maintaining and increasing the confidence of users in using the Internet, and therefore will certainly continue to drive improvements to self-regulation. Representatives of the commercial online adult content industry, for example, have

articulated their willingness to take voluntary steps to reduce ready access to online commercial adult content by children.\textsuperscript{99}

In Canada the Canadian Association of Internet Providers (CAIP)\textsuperscript{100} developed a code of conduct for its membership in 1996. Their Fair Practices initiative\textsuperscript{101} launched in the year 2000 builds on this code of conduct. It covers areas such as responsible delivery of service, customer communications, and addressing customer complaints about content and spam. CAIP members also pledge to comply with all applicable laws and that they will co-operate with government officials, international organisations and law enforcement authorities. They also promise not to knowingly host illegal content on their servers and to share information about illegal content. CAIP offers a protection portal which connects users to organisations that combat illegal and offensive content on the Internet.

Similar initiatives can be found all around the world\textsuperscript{102}. In Europe EurolSPA\textsuperscript{103}, the pan-European association of the Internet services providers associations of the countries of the European Union provides a platform for European ISPs. The association was established when a number of such ISP associations signed the EurolSPA Memorandum of Understanding on 6 August 1997 in Brussels. EurolSPA helps their members to establish and implement codes of conduct in harmonisation with European Union law and national law, and to increase effectiveness by co-ordination of national initiatives.

\textsuperscript{99} supra note 45; They would provide public front pages which would not contain explicit graphics or text, but be limited to material sufficient to make clear that the site contains sexual material, teaser pages would be located only beyond the front, public page.

\textsuperscript{100} for more information visit online: Canadian Association of Internet Providers (CAIP) <http://www.caip.ca/> (date accessed: 26 January 2002)

\textsuperscript{101} CAIP’s Fair Practices initiative, online: CAIP <http://www.caip.ca/issueset.htm> (date accessed: 26 January 2002)

\textsuperscript{102} See for example: online: <http://www.iiia.net.au/> (Australian ISPs) <http://www.ecom-lac.org/> (ISPs of South America) <http://www.apia.org> (Asia and Pacific Internet Association)

\textsuperscript{103} For more information visit online: European Internet Services Providers Association (Euroispa) <http://www.euroispa.org> (date accessed: 26 January 2002)
Although international co-operation is an essential part in the development of codes of conduct there should not be a single code of conduct to regulate all ISPs around the world. Some have argued for the establishment of such a single, global document, but an attempt to draft such a code would remove the flexibility of the industry, hinder context-specific development and interfere with cultural diversity. Considering the advantages of self-regulation for the industry and the fact that industry and governments already co-operate in various ways, it is very unlikely that such an approach, where a single document promulgates mandatory rules or guidelines for ISPs, would be accepted and add value in terms of trust and confidence to the scene.

While the efforts of the Internet industry in providing responsible approaches to effective self-regulation of their joint interests to further promote the confidence, security and trust of their customers are welcomed, it is essential that those private entities do not take on the role of content censors. They should assist law enforcement in investigating criminal activities and to combat illegal content, but not become the police or prosecutor. ISPs have been targeted by the governments of many countries to act as censors because of the crucial role they play for access to the Internet.  

The danger lies in the fact that what is often promoted as Internet self-regulation is rather privatised censorship, where a formerly direct government function is turned over to administration by a private agency. The backing is still state power and government threat, but the actual implementation and mechanics of the suppression of material is delegated to a trade group.  

---

104 See also Chapter III, 3.4 Liability of ISPs at 100
Governments should not force ISPs to self-regulate certain classes of content in exchange for some limit on legal liability for that content. The overwhelming pressure will be to censor even more material, rather than less, in an effort by ISPs to be certain that they have removed any material that might be illegal. Content will be removed in advance of legal judgement to satisfy government demands and that will lead to an inappropriate suppression of speech that might be legal and protected, though possibly controversial. That goes far beyond the limited category of illegal content and such a regime would severely interfere with the right to freedom of expression. It should not be forgotten that the prime responsibility for content lies with the authors and content providers. ISPs should have the right to take action in good faith to restrict the availability of material that violates best practices but without government pressure.

3.6 Hotlines

To restrict the circulation of illegal material a network of hotlines which allow users to report content which they come across in the course of their use of the Internet and which they consider to be illegal can be set up. Hotlines can be operated by a variety of people such as ISPs, telecom operators or national hotline operators.

Internet users or providers contact the hotline when they encounter Internet content they believe to be illegal. The hotline investigates the complaint and, when it deems the content in question to be potentially illegal, notifies the content provider and appropriate law enforcement officials.

Hotlines have their benefits: Rather than depending on active monitoring or depending on filtering and blocking content right from the start by governments or ISPs, hotlines rely on complaints from Internet users to uncover illegal content. Hotlines do not remove content, they just report illegal content to law enforcement authorities and they
have to take further action. By screening complaints hotlines sort out illegal from legal, though maybe offensive, content which is protected by the right to freedom of expression and therefore “allowed” to stay online.

Hotlines can also help to increase trust and confidence of users. Studies\textsuperscript{106} have found that users don’t often complain about objectionable material they find on the Internet, even if they want to, because they don’t know where to file their complaints. Setting up a network of hotlines can address this issue and provide users with a communications system and a link between users, content providers and law enforcement authorities.

Hotlines are operated in several countries, such as Australia, Austria, France, Germany, Ireland, the Netherlands, Norway, the UK and the U.S. To be effective Internet users have to be aware of the existence of these hotlines. Therefore they need to be promoted not only by the Internet industry but also by governments, because in the end everybody benefits from their existence by taking off the burden of ISPs to censor content and still giving government the possibility to combat illegal material without censorship.

3.7 Educate and Empower Users

Although there are laws that apply to cyberspace we have to recognise that legislation alone won’t solve the problem of illegal and offensive content on the Internet. Legislative reform is important, but to address the issue of illegal and offensive content a broad approach is necessary. This is also important, because approaches to addressing inappropriate Internet content must balance the need to protect users with

the need to respect democratic rights and freedoms such as the freedom of expression.

Therefore governments and international organisations around the world have realised the importance of the support of initiatives that educate and empower users and give them the tools for a safe use of the Internet.\footnote{See for example: EC, Council Decision 276/99 of 25 January 1999 “Multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks”, (1999), O.J. L. 33/1} It is important to raise the awareness of the potential pitfalls of the Internet. Awareness actions contribute to the trust and confidence of parents and teachers in safer use of the Internet by children. This is also important because in some cases, despite its legal status, content may be considered harmful to children. This content can include sexually explicit material, graphic violence, or content may be considered offensive on social, religious, cultural or moral grounds. Both governments and the private sector play important roles in raising awareness and educate and empower users.

A very good example of how these strategies can work is in my opinion the initiative of the Canadian government to promote safe, wise and responsible Internet use.\footnote{online: Government of Canada <http://www.connect.gc.ca/cyberwise> (date accessed: 30 January 2002)} In its guide it refers users to organisations and programs that equip parents and teachers with tools to help youth develop skills they require to become safe, wise and responsible users of the Internet.

The Media Awareness Network (MNet) is a non-government, not-for-profit Canadian organisation that supports media education in Canadian homes, schools and communities. Its national, bilingual, Internet education program “Web Awareness” provides parents, teachers, public librarians and all other users with information on
how to find children's sites, do effective online searches, track where children go while on-line and protect children from online predators.  

The Canadian Library Association is developing a similar program in co-operation with MNet to deliver Internet education in public libraries across Canada. It will provide professional development for library staff, who in turn will raise awareness of Internet issues among those accessing the Internet from public libraries.

The Canadian Association of Internet Providers established an Internet Protection Portal, an online window to resources users can use to safeguard their Internet experience. The Portal provides information on addressing online hate propaganda, the use of the Internet to lure children, and consumer issues.

---

109 for more information visit online: Media awareness network <http://www.media-awareness.ca> (date accessed: 30 January 2002)
Chapter IV  Conclusion

When I first started to write my thesis I was convinced that to protect human rights on the Internet a new piece of international legislation would be necessary. Due to the character of the Internet as a transnational medium and its borderless flow of information this seemed to be the obvious solution. The nation state won’t be able to effectively regulate the Internet within its borders and it has to accept its loss of sovereignty in the digital age. Only the international community by working together could face the challenges of the new medium and create new legislation to protect and enforce human rights on the Internet.

I never believed in no regulation at all. The myth of cyberspace as a “no-law-land” and the idea that the Internet was impossible to regulate might have been true in its early days when its architecture was far simpler and its use limited. At that time, it was widely believed that the Internet would help to undermine authoritarian regimes, promote democracy, and circumvent all kinds of local or international regulation. American cyber-libertarians hoped that the Internet would spread their free speech gospel around the world and therefore further promote the right to freedom of expression. The Internet was seen as a parallel world, an exciting new frontier where a lawless freedom prevailed.

But to me this always seemed to be a glorious illusion. New technologies have always presented opportunities and risks. With the rapid growth of the Internet in the 1990’s and its extended commercial use new challenges arose. As in the real world not only “good and law obeying society” had discovered the great potential the Internet offers. Cheats and criminals, hate mongers, distributors of child pornography, terrorists, and so on also appeared in cyberspace, threatening the dignity and security of users. And
while, as in the real world, the Internet is not primarily concerned with such negative activities, we still have to face the fact that they exist and that they pose a threat to privacy and freedom of expression on the Internet.

I do not doubt the benefits, the Internet has which I have shown in my thesis. I believe that the Internet has a high potential to further promote human rights in the world, especially the right to freedom of expression, to raise awareness of human rights violations and to show people around the world how governments still violate human rights despite their international commitments and multiple international agreements and treaties that exist. The Internet can make a difference in authoritarian regimes by providing a possibility for people to reach an audience outside the countries borders who could have never been reached before to report human rights violations.

The Internet has made it easier for many organisations to take advantage of the global network, to establish online presence, to exchange information and ideas on a far greater base than ever before. Educational institutions, cultural associations, scientific societies and others have all benefited from the wide reach of the Internet and the growth of network communications. The Web has also made possible the rapid development of new commercial applications that include both business to business services and business to consumer services. The rise of e-commerce is boosting the economy of many countries.

New technologies provide a high level of security and privacy. They can enable anonymous transactions over the Internet so that individuals can obtain access to information and purchase products without disclosing their actual identity. They enable the secure transfer of credit card numbers or other personal data. Filtering software can
protect users, and in particular children who use the Net, from illegal or offensive content they might come across while surfing in cyberspace.

But the same technologies also make possible a widespread surveillance of private activity by governments and law enforcement agencies. Huge amounts of private data can be collected and stored. Without strong laws in place to protect privacy and personal data the use of this information is uncertain and poses a threat to important human rights guarantees. \(^1\) Filtering and blocking restrict access to information that was freely available before and therefore limiting the right to freedom of expression on the Internet.

Recent developments pose additional challenges to the protection of human rights on the Internet. Concerns about cybercrime and the fight against terrorism have led to increased government regulation and police investigation of the Internet. Well established human rights suddenly appear to be threatened not only in authoritarian regimes but also in democratic countries. While there is a clear need to protect public safety and investigate and prosecute criminal activities, it is also vitally important that public concerns do not lead to expansive new police powers that diminish human rights established for a long time.

With e-commerce and the expansion of the global economy international organisations, such as the World Trade Organisation and the World Intellectual Property Organisation have gained greater prominence in setting public policy for the digital age. These organisations tend to emphasise commercial interests and do not generally recognise the broader values of cultural, social, political, or artistic activities. Individuals may also face the specific threat that rights accorded under national laws may not be recognised by these international organisations.

\(^1\) See also: Chapter III, 3.2.1 Convention on Cybercrime at 69
While a complete lack of regulation gives a free hand to criminals and will lead to a decrease of trust and increased insecurity of users, it is also unrealistic to expect that countries with different cultural values will agree upon a single set of rules for the whole world, even a set of lowest-common-denominators. International harmonisation strategies are clearly an important response to the jurisdictional difficulties of Internet regulation, but they usually come at the cost of local values and national differences, and international legislation is often not easy to achieve. It is hard to determine whether the gains from harmonisation outweigh the costs. Many harmonisation efforts reflect coercion of powerful nations rather than truly fair or efficient regulatory improvements. A prominent example of this may be seen in the Convention on Cybercrime, where an additional protocol had to be added to eliminate racist and hateful web sites from the Internet, because in particular the United States strongly opposed their ban. So the issue was dropped from the Convention itself to ensure that the U.S. would at least agree upon the rest of the Convention.

International harmonisation of law does not always have to take place in the "hard" form of treaties that either establish a uniform international standard, or an international anti-discrimination regime, or an international choice-of-law regime. It can take "softer" forms like information sharing among enforcement agencies or informally agreed upon regulatory targets. But the problems of "single" international solutions remain the same, which form they may take.

We should keep in mind that there are good reasons for regulatory differences among nations. Nations have different regulatory commitments because of, among other things, differences in endowment, technological capacities, and preferences. A primary virtue of decentralised law making by nation states (as opposed to uniform international rules) is that it allows populations to implement policies that reflect these differences. When regulatory differences reflect important local values, harmonisation is very
difficult to achieve because of domestic political opposition. This is why almost all international regulatory regimes are littered with mandatory or local public policy exceptions.²

Harmonisation of Internet regulation will likely be easiest to achieve in those contexts where nations' interests converge and the gains from co-operation are high and where every nation has an incentive to adhere to adopted standards, like many aspects of criminal law enforcement. In other areas, such as issues concerning privacy or freedom of expression and social issues, it is more likely to see harmonisation through informal means and "soft" harmonisation strategies.

Therefore a single international document cannot be the solution. To protect human rights on the Internet a combination of many different approaches has to be the goal. Governments, international organisations, NGOs and users have to work together to achieve this goal.

First, it is necessary to reaffirm the support for the existing international and regional human rights agreements, such as the Universal Declaration, the ICCPR or the European Convention, which can be applied to the Internet as shown in Chapter II. Further efforts should be made to promote public awareness of the protections granted in these agreements. The international community should take more efforts to ensure the enforcement of these agreements and to raise compliance of signatory states. Public awareness can definitely help to achieve these goals.

If international treaties of Internet regulation, such as the CCC, are established their application and implementation has to be watched carefully to ensure that fundamental human rights and the free flow of information on the Internet are protected. As mentioned above, these higher level rules will be necessary to govern cross-border transactions, to set international standards, and to combat cybercrime. For more controversial matters it will be better to regulate them locally or regionally, because agreement at a regional level is easier to achieve if States have more shared common values and interests.

Second, the development of new technologies to enhance the protection of privacy and personal data should be encouraged. But their development has to be critically assessed to determine whether in fact they protect the interests of users in the digital age. Research should go forward on techniques that minimise or eliminate the collection of personally identifiable information but still allow for secure and verifiable transactions. In this context it is important to address the concern of unlawful police surveillance that takes place around the world. The development of these new technologies has to be accompanied by the implementation of strong legislation to protect privacy and personal data to ensure that those technologies won't be used by governments to set up an “orwellian” style surveillance system to control their citizens.

Efforts by governments to restrict access to information on the Internet or to limit the distribution of information on the Internet, particularly information that is political, cultural or artistic should be opposed. As examples show the diffusion of the Internet does not necessarily spell the demise of authoritarian rule. By “firewalling” whole countries, governments are able to stifle the Internet’s supposedly democratising influence. Old-style geographical borders are proving surprisingly resilient with the development of new technologies.
Standard setting organisations should promote open, non-proprietary standards that enable competition and the development of a variety of products instead of creating uniform, single standards that encourage the development of "bottlenecks" in the communications infrastructure. The decision to choose filtering and blocking to limit access to certain information should stay with the individual user. The use of such techniques at a network level is a direct threat to freedom of expression on the Internet.

Last, but not least, the strengthening of the public voice and the active participation of civil society are central to the protection of human rights on the Internet. The growth of the Internet has also encouraged the growth of NGOs that are independent of governments and business organisations. They focus on the social issues arising from the impact of the new information technologies, such as privacy and free expression, but they also use the Internet to educate the public and to take action. Users become empowered through education and awareness of their rights.

The work of these NGOs should be encouraged. These organisations are already involved in decision making processes by national governments, and international organisations, such as the OECD, the UN, or the EU. They bring a public voice to emerging digital age issues based on international human rights norms. Their influence on Internet policy should not be underestimated. In my opinion successful policies for the Internet must include the voices of its users in order to be most effective.

In the end the rules governing the Internet will be the same like those governing the physical world. In some ways this might be considered a shame, in others not. It is certainly a pity that the Internet has not really turned out to be quite the force of freedom that it once promised to be. But that was only to be expected. After all the Internet is part of the real world, although it is inspiring to think it could have been a lawless datasphere, unregulated and free of "real-world" consequences.
Bibliography

I. Legislation

1.1 International


*Universal Declaration of Human Rights*, (10 December 1948), U.N.GA Res. 217 A (III)
Vienna Convention on the law of treaties, (23 May 1969), 1155 U.N.T.S. 331

1.2 Europe

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe (CoE), [28 January 1981], Eur. T.S. 108
Multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks Council Decision 276/99/EC of 25 January 1999, O.J. L. 33/1

1.3 Canada

Bill C-36, An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to
enact measures respecting the registration of charities, in order to combat terrorism, 1st session, 37th Parl., 2001 (assented to 18 December 2001 S.C. 2001, c. 41)

1.4 United States


II. Jurisprudence

2.1 Europe


*John Murray v. the United Kingdom* (1996), 1996-I EHRR 49
Saunders v. the United Kingdom (1996), 1996-VI EHRR 2064
Serves v. France (1997), 1997-VI EHRR.

2.2 United States

Ashcroft v. ACLU, et al. [2001] SCT-QL167 (Order List 533 US Supreme Court 00-1293) QL (SCT)
Doe v United States (1988), 487 US 201, 219,
Multnomah County Public Library et al. v. United States Federal Communications Commission, et al. [2001] PA-QL438 (E.D. PA No. 01-1322) QL (PA)
Reno vs. ACLU, 117 U.S. 2329 (1997)
Schenk v. United States, 259 U.S. 47 (1919)
Yahoo!, Inc. v. La Ligue Contre Le Racisme, 169 F. Supp. 2d 1181, 1189 (N.D. Cal. 2001)
III. Secondary Materials

3.1 Books


Davies, S., "Big Brother: Britain's Web of Surveillance and the New Technological Order" (Pan, London 1996)


Everard, J., "Virtual States, The Internet and the boundaries of the nation-state", (London: Routledge, 2000)


**Articles**

"China to Speed up Internet", People's Daily (11 July 2001)

Agence France Presse, "Jiang Renews Warning Against "Pernicious" Internet", July 11, 2001

Barber, B.R., "Which technology for which democracy? Which democracy for which technology?" (Winter 2000/2001) 6 International Journal of Communications Law and Policy

Chandler, "China Again Censoring Web", Washington Post Foreign Service (23 October 2001) E01

Guernsay, L., "Court Says France Can't Censor Yahoo Site", The New York Times, Technology (9 November, 2001)

Hogan, K., "Will Spyware Work?" (December 2001) MIT Technology Review


Reitinger, P.R., "Compelled Production of Plaintext and Keys", The University of Chicago, 1996 U Chi Legal F 171


2.3 Reports


De Santis, H., "Combating Hate on the Internet: An International Comparative Review of Policy Approaches" (1998), Report for the Department of Canadian Heritage, the Department of Industry and the International Comparative Research Group

Department of Justice Canada,


<http://www2.epic.org/reports/crypto2000/overview.html#Heading2> (date accessed: 4 April 2002)


Miller, G. et al., , “Regulation of the Internet, A Technological Perspective” (1999), Report for Industry Canada


2.4 Addresses at Conferences


Global Internet Liberty Campaign Member Statement on international ratings & filters submitted to the Internet Content Summit, Munich, Germany, 9-11 September 1999

2.5 Online Documents

Banisar, D. et al., Comments of the American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International on Draft 27 of the Proposed CoE Convention on Cybercrime (2001), online: Privacy International

Barlow, J.P., "Declaration of Independence of Cyberspace" (1996) online: Electronic Frontier Foundation

Berman, J. & Bruening, P., "Is Privacy Still Possible in the Twenty-first Century?" (2001) (Social Research for the Center for Democracy & Technology) at "Threats to Privacy", online: Center for Democracy & Technology

Cacas, M., "Efforts to Censor 'Net in Asia Doomed" (1998), online: Freedom Forum

Global Internet Liberty Campaign (GILC), "Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on the Global Internet", online: GILC

Holznagel, B., "Responsibility for Harmful and Illegal Content as well as Free Speech on the Internet in the United States of America and Germany" online: Max Planck Project Group “Common Goods: Law, Politics and Economics” Homepage


UNDP Agenda for Action, "Driving Information and Communications Technology for Development" (2000-2001) online:
Yahoo in Frankreich verurteilt (ORF ON Futurezone 2000) online: ORF ON Futurezone Homepage