The Media Freedom Internet Cookbook

The Representative on
Freedom of the Media

OSCE

VIENNA 2004

OSCE

REPRESENTATIVE ON FREEDOM OF THE MEDIA

The Media Freedom Internet Cookbook

Edited by
Christian Möller and Arnaud Amouroux

Vienna 2004

On the cover is a drawing entitled *Des Schreibers Hand (The Writer's Hand)* by the German author and Nobel prize laureate (1999) Günter Grass. He has kindly let our Office use this as a label for publications of the OSCE Representative on Freedom of the Media.
The drawing was created in the context of Grass's novel *Das Treffen in Telgte*, dealing with literary authors at the time of the Thirty Years War.

The publisher thanks the governments of The Netherlands
and Germany for their financial support to this publication.

Organization for Security and Co-operation in Europe (OSCE)
Office of the Representative on Freedom of the Media
Kärntner Ring 5-7, Top 14, 2. DG,
A-1010 Vienna
Telephone: +43-1 512 21 450
Telefax: +43-1 512 21 459
E-mail: pm-fom@osce.org
www.osce.org/fom

The views expressed in this publication represent those of the authors and contributors and do not necessarily reflect the official position of the OSCE Representative on Freedom of the Media.

Design: WerkstattKrystianBieniek, Vienna
Photo: © Jiri Büller / Hollandse Hoogte

Contents

The Recipes

Legislation & Jurisdiction

Self-regulation, Co-regulation, State Regulation

Hate Speech on the Internet

Education & Developing Internet Literacy

Access to Networks and to Information

Future Challenges of the Information Society

Miklós Haraszti

Preface

Cookbooks usually offer quite a variety of recipes to help in the preparation of a tasty meal. And there are also cookbooks for computer programmers, tongue-in-cheek comparisons between kitchen and communication utensils, containing hundreds of programming recipes.

In the tradition of these guides, *The Media Freedom Internet Cookbook* offers recommendations and best practices, the results from the 2004 Amsterdam Internet Conference of the OSCE Representative on Freedom of the Media.

But our Cookbook's recipes are not the usual "see what you can concoct in your kitchen". Our experts were not asked to explore the infinite possibilities offered by the world's first truly global medium. To all freedom lovers of the Internet – legislators, industry workers, and consumers of the Web – we offer recipes not of how to consume the freedom of the Internet, but how to preserve it.

The assumption that media freedom is valuable for the democracies of the OSCE community, and that it should be preserved, will not surprise you, dear readers.

The surprising feature of this guide may well be the underlying anxiety of our experts that freedom on the Internet needs preservation at all. One of the half-baked wisdoms of our age is the common belief that the Internet is not only qualitatively freer than all previous media forms but also that its freedom is invincible, due to the unique technology and the global character of the Web.

Now, the truth is sobering. The Internet *can* be controlled, conditioned, and curtailed. More than that, it *can* be censored and suppressed. The OSCE democracies, when addressing what their governments or communities see as “bad content” on the Internet, must be aware that they *can* go too far. The experience of China – potentially the biggest Internet market – proves that even the Internet can be fully subjugated to the political needs of the Government.

This guide, the work of cutting-edge experts in modern communication technology, modern media, and modern freedoms, is aware of the real-life dilemmas of the Internet. As our experts point out, the “bad contents” on the Internet are of course very different in nature, impact, or legal and cultural recognition, and therefore all need to be treated differently. But it is beyond doubt that terrorism is real, hate speech is real, and child pornography is real, to mention three of the most-cited types of “bad content”.

The Cookbook is therefore not the fruit of a denial of the challenges posed by the freedom of the Internet. It offers insights into:

- What media freedoms or even media types can get lost in the hands of uninformed or uncaring legislators;
- How good intentions of uninformed or uncaring legislators result only in loss of freedom rather than helping to fight “bad content”;
- What are the unexplored non-regulatory ways of fighting “bad content”, methods that use the potential of the Internet itself and of the communities that create and consume media on the Internet.

I would like to thank the governments of the Netherlands and Germany for all their support to the Amsterdam conferences and this Cookbook. I hope that it will contribute in the OSCE region to the never-ending learning process of living with the free media.

Vienna, November 2004

Christian Möller and Arnaud Amouroux

The Media Freedom Internet Cookbook

Introduction

Media freedom on the Internet first became a concern of this Office in 2002, when Freimut Duve was the OSCE Representative on Freedom of the Media. A first workshop, held that year in Vienna, showed that although the Internet in its decentralized design had so far proved to be a suitable tool to circumvent censorship and to share ideas across borders, this in itself is no safeguard against government (or industry) censorship. Government-imposed blocking and filtering occurs in a number of countries around the world – also in the OSCE region. The Internet can only stay a free place through the active promotion and implementation of good practices.

In 2004, delegations from all OSCE participating States were invited by the Representative to consult Internet experts and together develop the agenda for the 2nd Amsterdam Internet Conference. The aim was to find out more about the needs, concerns and questions of the participating States and to develop tailored answers and solutions.

The 2nd Amsterdam Internet Conference in August 2004 brought together over 80 international experts and 25 speakers. Delegates from the OSCE, the Council of Europe, UNESCO, academia, media, industry and several non-governmental organizations from the whole OSCE region reported on the status quo, discussed possible solutions, collected lessons learned and shared experiences.

The results of the conference are published in this Cookbook. The book combines concrete recommendations – the Recipes – of the OSCE Representative on Freedom of the Media with background papers, grouped in six different chapters. It also acknowledges the results from the *Meeting on the Relationship between Racist, Xenophobic, and anti-Semitic Propaganda on the Internet and Hate Crimes*, which was held in Paris in June 2004, as well as other OSCE Human Dimension conferences to which the Representative contributed with expert side events.

The Recipes in the first part of the book form the 2004 Internet Recommendations of the OSCE Representative on Freedom of the Media and hopefully provide guidelines for OSCE participating States. These recommendations would not have been possible without the valuable input from, and enriching co-operation with, experts from a wide range of institutions, companies and organizations. They also complement the 2003 Amsterdam Recommendations that can be found in the appendix of this publication.

However, the recommendations do not stand alone. The second part of the Cookbook comprises papers by outside experts, which provide background information and insights into current debates about the Internet. These also include lessons learned and examples of successful initiatives and good (or best) practices.

One of the aims of this Cookbook is to find a common terminology that will help people to understand the unique qualities of the Internet. This necessitates explaining, clarifying and differentiating. Eventually, users, governments and other stakeholders will hopefully come to the conclusion that the Internet is not the “evil” black hole some people might think. On the contrary, the potential that the Internet offers to build tolerance and foster mutual understanding has yet to be fully exploited.

The Office would like to thank Christiane Hardy (Vienna) and Karin Spaink (Amsterdam) for their initiatives and co-operation.

An evaluation of the outcomes of this book will take place during the 3rd Amsterdam Internet Conference in 2005.

Vienna, November 2004

The Recipes

Recommendations of the OSCE Representative on Freedom of the Media from the 2004 Amsterdam Internet Conference

A. Legislation & Jurisdiction

- The source for all legislation regarding the Internet should be basic constitutional values, such as freedom of expression and its interpretation in jurisprudence. These values form the foundations for tailor-made and non-restrictive regulation where necessary. New legislation should be limited to instances where it is absolutely unavoidable and then only in the least restrictive way in terms of freedom of expression and users' rights.
- The Internet is not in itself a guarantor of freedom of opinion and expression. The Internet is primarily a technology, a network enabling communications. States and new corporate gatekeepers have increasingly developed policies and technologies of control which go beyond the legitimate. Freedom of expression on the Internet must be protected, as elsewhere, by the rule of law rather than relying on self-regulation or codes of conduct. There must be no prior censorship, arbitrary control or unjustified constraints on content, transmission and dissemination of information. Pluralism of sources of information and media must be safeguarded and promoted including diversity among systems for information retrieval.

- Media presence on the Internet includes websites of traditional media outlets, but it also includes websites of individual desktop publishers who convey information or express their views through their own personal websites. Some of these sites enjoy significant readership; others do not. But when we speak of guaranteeing media freedom, it must be clear that we are not only speaking of freedom for traditional media outlets but also the freedom of the average citizen to voice his or her views through his or her own website.
- All Internet content should be subject to the legislation of the country of its origin (“upload rule”). Any legislation which imposes liability on an author or publisher for content wherever it is downloaded is too restrictive for freedom of expression.
- Most Internet legislation is aimed at the World Wide Web (WWW). Awareness should be raised about the negative impact this can have on different Internet-related communication systems such as chat environments, file transfer protocol servers (ftp) or peer-to-peer networks, Usenet discussion groups, audio and video streams (including live sound and image transmissions), and finally the ubiquitous e-mail communications. WWW content represents only a fraction of the whole of the Internet and different levels of privacy for different forms of communications must be observed. A provider must not be held responsible for the mere conduit or hosting of content.
- Search engines embody the core concept of the Internet: global accessibility and connectivity of content. Filtering or limiting their content searches would betray their basic mission which is to deliver comprehensive and reliable results. Automated search engines should not filter, and must not be held responsible for the content of the results they produce.

B. Self-regulation, Co-regulation, State Regulation

Regulation

- Regulation of the Internet should be limited to fields where it is unavoidable. Preferably the Internet should be seen as a space that works best autonomously and without any intervention. If regulation appears unavoidable, it should be applied according to the principle of subsidiarity, meaning that regulation should be as close to the source of trouble as possible – close both in terms of geography and competence. Within regulatory and co-regulatory bodies, transparency, accountability and the right to appeal should be observed to at least the same degree as in classic media.
- Procedures and patterns of behaviour have evolved among users of the Internet. "Netiquette" was the first informal code of conduct that was not developed by lawmakers or industry representatives but users who wanted to utilize the Net for themselves in a civilized way. This logic should be extended and made popular among all Internet users. It should also serve as a blueprint for other forms of regulation.
- When structures or institutions for Internet regulation are being designed they should follow the multi-stakeholder approach of governance that includes "governors" from different segments of society, geographical regions and genders, representatives from governments, NGOs, industry, users and citizens, etc. No sector should be allowed to dominate and the overall strategy should be based on compromise.

Self-regulation

- Defending values of free expression should become a priority of global public policy. The Internet is based on technical designs that are mostly decided upon by hardware and software companies, not bodies of government or governance. The technical architecture of the Web must reflect values like openness, promotion of progress and knowledge, and easy access. It should also strengthen the intellectual commons and protect the public domain. Protecting these features and developing the courage to counteract any trends that could lead to the monopolization of Internet activities must be central tasks of any regulatory action.
- The Internet is not just threatened by certain state activities; it also faces the danger of "privatized governance". This occurs when a few industrial actors become so powerful that they are able to take over the regulatory process and define the rules. Diversity and pluralism as values do not just refer to the content of the Internet; they are also values of utmost importance in the selection of regulators.
- Industrial "self-regulation" has an ambivalent and tense relationship with freedom of expression. It should be avoided because it tends to be non-transparent and there is also the risk of it being utilized for hidden business purposes. Because self-regulatory institutions are not public bodies, they may be less accountable and there may be less protection of fundamental rights than provided by the rule of law.
- Private bodies must not decide on the legality or illegality of content. This is the duty of courts with transparent mechanisms of appeal and accountability. The right to "put back" content after removal by private bodies should be regarded as a policy issue.

Regulatory Schemes

- Regulatory schemes must be able to command public confidence. There must be a high degree of external consultation and all relevant stakeholders should be involved in the design and operation of schemes. As far as practicable, the operation and control of schemes should be separate from the institutions of the industry.
- Regulatory schemes must be based on clear and intelligible statements of principles and measurable standards – usually in the form of a code – which address real consumer and user concerns. Reasons for interventions must originate from these objectives and intended outcomes should be identified. Schemes must be well publicized, with maximum education and information directed at users and publishers. Schemes must be regularly reviewed and updated in the light of changing circumstances and expectations.

Filtering, Labelling and Blocking

- In a modern democratic and civil society citizens should be allowed to decide for themselves what they want to access on the Internet. The right to disseminate and to receive information is a basic human right. State enforced mechanisms for filtering, labelling or blocking content are not acceptable.
- Unlike in television there is little future in filtering systems based on a rating system. It is highly unlikely that such proposed measures will in the long-term result in a safe Internet environment as the rating and classification of all information on the Internet is not feasible. Even if filtering technology is applied to the WWW, it is not clear what sort of content the regulators intend to rate. In most cases, the targeted

category of Internet content is not illegal and remains well within the limits of legality. At the same time the rating of content is in itself a threat to free expression on the Internet.

- Family-based filtering and blocking software only works well if parents also discuss Internet content and habits with their children and update the filter regularly. If this is not the case, filtering software is not a solution.
- Another downside of relying on such technologies is that these systems are defective and in most cases result in the exclusion of socially useful websites and information. Originally promoted as technological alternatives that would prevent the enactment of national laws regulating Internet speech, filtering and rating systems have been shown to pose their own significant threats to free expression. When closely scrutinized, these systems should be viewed more realistically as fundamental architectural changes that may, in fact, facilitate the suppression of speech far more effectively than national laws alone ever could.
- Rating and filtering systems with blocking capabilities enable preliminary censorship and could allow repressive regimes to block Internet content, or such regimes could make the use of these tools mandatory. Laws or other measures prohibiting speech motivated by racist, xenophobic, anti-Semitic, or other related bias can be enforced in a discriminatory or selective manner or misused as a means of silencing government critics and suppressing political dissent. If the duty of rating were handed to third parties, this would be problematic for freedom of speech. Furthermore, as there are few third-party rating products currently available, the potential for arbitrary censorship increases.

C. Hate Speech on the Internet

- Any definition of hate speech should be narrowly drawn. The differences between different sorts of content (e.g. hate speech and child pornography) should be clarified and differentiated. A precise definition of “hate speech” is a necessary prerequisite for further discussions about this issue on the Internet. At a minimum, it is imperative that speech restrictions, when they must be enacted, be clearly and precisely drawn so that they do not chill lawful speech.
- Words should not be confused with actions. A clear distinction must be maintained between what individuals say and think on the one hand, and what they do on the other. Only then can we have an equitable system of law in which individuals are assumed to be rational legal subjects, who are themselves responsible for their own actions and not some third party.
- Coherent policy cannot be developed on the basis of reacting to individual cases of extreme material. Instead, research and monitoring must form the foundations for any decision-making. Obviously there is distressing material to be found on the Internet. But the fact that something exists online tells you nothing about how widely read or widely accepted it is. There should be an understanding that some hate sites are just too small and insignificant to be prosecuted. They are in fact consigned to oblivion, despite being theoretically accessible to the general audience.
- Since the Internet is a high-tech environment, many battles here can be won through technical means. One good example is adding voluntary disclaimers to search engine results or the establishment of sponsored links to sensible keywords, as was demonstrated in the Paris OSCE *Meeting on the Relationship between Racist, Xenophobic and anti-Semitic Propaganda on the Internet and Hate Crimes* in June 2004.

- A society with confidence in its values and ideals has little to fear from the expression of dissenting views, no matter how repugnant those views may be. Attempts by governments to stifle the exchange of views and the free flow of information in the competition of ideas must be resisted vigorously. Never before has so much information been accessible at the stroke of one's fingertips; never before has it been easier for people around the world to communicate with each other; and never before has it been easier for citizens to participate in public discourse and make their voices heard. Instead of focusing on ways to censor hate speech, we must concentrate on answering such expression with more speech. The battle against intolerance cannot be won through government regulation or mere legislative action. Instead, it is a fight that will be won or lost in the competition of ideas.

D. Education & Developing Internet Literacy

Personal and Parental Responsibility

- Parents and other adults always have a role to play regarding children's access to the Internet. Adults should act responsibly towards children's Internet usage rather than relying on technical solutions that do not fully address problems related to Internet content. Parents and teachers and others who are responsible for children's Internet usage need to be educated in this regard.
- In this borderless media world of VCRs, DVDs, satellite TV, and the Internet, children and young people have increasing access to media products from around the globe. Rating and classification systems, legislation and industry codes and guidelines are no longer enough to protect children. Digital media are forcing a shift in responsibility from statutory regulators toward the individual household. The Internet does

not work on the principles of censorship or control, but rather on principles of responsible decision-making and calculated risk-taking – and those are the kinds of skills the young should develop.

- Librarians and teachers should also have a role to play as far as access to the Internet is provided by public libraries and schools. Any regulatory action intended to protect a certain group of people, such as children, should not take the form of an unconditional and universal prohibition on using the Internet to distribute content that is freely available to adults in other media.
- If "regulation" with an emphasis on self-regulatory or co-regulatory initiatives is addressed, then "self" should mean individuals rather than self-regulation by the Internet industry without the involvement of individuals and Internet users. There should be more emphasis on promoting the Internet as a positive and beneficial medium.

Media Literacy

- Media literacy is a necessary complement to traditional literacy. Young people today need to be able to read, understand and bring critical-thinking skills to information in all forms, including media. Media literacy should involve analysis, evaluation, production of and critical reflection about media products and should stress the positive and creative aspects of media and popular culture.
- Research is critical to understanding how technology is fundamentally transforming young people's lives. Research involves and requires public Internet policy, government policy-setting and responsive national public education strategies on Internet use. Efforts should be made to increase co-operation between OSCE countries in this field.

- Stakeholders in government and industry should be encouraged to support public awareness initiatives to educate parents and other adults not only about the potential risks of the Internet, but also about the opportunities and resources that are available. This support can cover a wide variety of contributions including radio, television, print and Internet advertising, posters and brochures and online resources for parents.

Journalist Training

- There is still a shortage of academic courses for journalists with a special focus on the role of the Internet in journalism. Journalist training needs to be improved to allow students to acquire more specific knowledge and vocational skills on how to utilize the Internet.
- One of the major issues for local media in the OSCE area is Internet literacy for journalists who speak the language of that region. Journalists who can speak English have a distinct advantage over their colleagues in ICT, whereas journalists with other language backgrounds have limited opportunities to gain vocational training on using the Internet because of the lack of special courses and learning programmes in local languages. There is also a shortage of online information in local languages. Special on/off-line Internet training courses need to be arranged and the learning of foreign languages should be promoted.

E. Access to Networks and to Information

Freedom of Information

- Governments should make more information available online. This would increase transparency and allow every citizen to obtain information from any computer connected to the Internet. Governments and intergovernmental organizations should support dissemination of official information online. Projects should be realized that foster citizens' freedom to receive and circulate online information about the activities of governments and state bodies.

- Universal access to information and knowledge, especially information in the public domain, is a prerequisite for broader participation in development processes and civil society. Access to quality education for all is a basic right and is essential for building the necessary skills and capacities for development, progress and social peace in all societies. ICTs provide immense opportunities to increase access to education and information.

Access to Networks

- Universal access to communication services and networks is essential for the realization of communication rights but will not be achieved, within the foreseeable future, by household access to the Internet alone. Access for all to the global communications environment requires investment in public access centres and in traditional communication technologies such as community radio and television. Public investment in communications facilities is one approach. Community-based initiatives should be encouraged and supported including legal and/or regulatory reforms where there are legislative or regulatory barriers.
- Participating States in the OSCE should aim to expand the reach of cyberspace by taking action to foster Internet access both in homes and in schools. They should also implement policies which aim to ensure that the Internet is an open and public forum for the airing of all viewpoints. To achieve this goal, it is imperative that government regulation is kept to a minimum, and the fundamental freedoms of speech, expression, and the press are respected.

- Another prerequisite is to significantly improve electric power supplies in countries in the OSCE region where this is required.

F. Future Challenges of the Information Society

- Access to the public sphere is being rapidly democratized. The Internet, for example, has made it much easier for like-minded individuals to meet, join forces, and raise money in support of their political views. The principle of freedom of expression must apply not only to traditional media but also to new media, including the Internet. It is the basic premise of knowledge societies as laid out in Article 19 of the Universal Declaration of Human Rights. It is important to continue to mobilize energies and efforts to promote freedom of expression and its corollary, freedom of the press, as a basic right indispensable to the exercise of democracy. Freedom of expression is a major avenue through which creativity, innovation and criticism can be developed. The nature of knowledge societies should be conceived as plural, variable and open to choice, and freedom of expression is inseparable from this vision.
- The right to privacy faces new challenges and must be protected. Every person must have the right to decide freely whether and in what manner he or she wishes to receive information or to communicate with others, including the right to communicate anonymously. The collection, retention, processing, use and disclosure of personal data, no matter by whom, should remain under the control of the person concerned. Powers of the private sector and of governments to access personal data risk abuse of privacy and must be kept to a legally acceptable minimum and subject to a framework of public accountability. Encryption techniques and research should be supported.

- The Internet provides enormous scope for the sharing and development of the common pool of human knowledge but this potential is increasingly held back by the reinforcement of private information property regimes in the Internet environment. There is a need for a fundamental review of international regulatory instruments governing copyright, patents and trademarks. The aim is to foster the development of global knowledge, and to safeguard the right of access to information and the right to creative reuse and to adaptation of information, which in turn should accelerate the social and economic benefits of freely available information.
- The fight against terrorism must not be used as an excuse to limit the free flow of information on the Internet. Prosecution of "cybercrime" must only target illegal activities as such and must in no way endanger or limit the technical infrastructure of the Internet.

Legislation & Jurisdiction

Nico van Eijk

Regulating Old Values in the Digital Age

"Nieuwe wijn in oude zakken": New wine in old bags. This Dutch saying, taken from the Bible[1], fully applies to regulating the Internet, the information age, the digital age, the World Wide Web, or whatever term one uses to indicate the fact that electronic communications are at the core of our present society (for practical reasons I will stick to the term "the Internet"). It's new wine in old bags.

What is meant by this? This paper will try to make clear that the Internet is not something that changes fundamental rights such as freedom of information. Freedom of information includes the right to receive and impart information as it has been defined throughout history and – within a European context – has been included in national constitutions and international treaties such as the European Convention on Human Rights. These old values – the old bags – are the foundations of society and should not be called into question because someone is pouring in a new wine called Internet.

The Internet is primarily a technology, a network enabling communications. The Internet is not something that changes the world. It's people who cause change by using technologies. It is quite common to fall into this trap of idolizing technological progress. Just to give an example: there is this book from the 1970s, which is full of beautiful predictions about the benefits of interactive cable television networks: free choice, new services, active participation of citizens, contribution to

[1] Matthew 9:17: "Neither do you put new wine into old wine-skins."

further democratization, and so on. None of these were realized with the creation of cable television networks. Just recently, a huge amount of money was spent in the Netherlands to create a "Kenniswijk" ("Information-rich Neighbourhood").[2] A part of the city of Eindhoven was to get high-speed Internet access (by building a fibre network that reached all the way to individual homes[3]) and strong support for the introduction of new (Internet) services. Introducing fibre turned out not to be a financially viable option and hardly any new service materialized. During a presentation of the project, information was given about one of those so-called innovative services: a babysitter who could watch six children in six different apartments at the same time using web cams. When I asked what would happen if two children got sick at the same time, there was no answer…

The following three examples, rather randomly picked, further illustrate the dilemma. The issues discussed are a) the confusing notion of Internet governance, b) the "evils" of search engines and c) the risk of technology-neutral regulation.

Internet Governance. "Internet governance" is one of the most abused concepts. For some, it relates to the position of ICANN[4], responsible for managing the underlying structure of the Internet, in particular regarding the assignment of domain names. Others see it as a legitimation for extensive governmental influence on the content of the Internet. The recent World Summit on the Information Society conference (WSIS, held in Geneva in December 2003) is a good example of what can go wrong, despite the fact that it ended with a rather balanced Declaration of Principles and Plan of Action.[5] Originally set up by the International Telecommunications Union (ITU) to strengthen its own position, the conference somewhat backfired and produced lengthy political statements, sketching all the dangers and risks of the Internet and aiming for more state control over content – clearly a different interpretation of "Internet governance".

It's surprising to see how much this WSIS "thing" appears to be a replica of discussions that took place in the 1970s and 1980s about satellites. Satellites would change the world and lead to new ways of spreading knowledge, but were also seen as a threat. Borders would disappear, allowing for propaganda from capitalists or communists to indoctrinate innocent citizens. Marshall McLuhan preached his global village and UNESCO published the McBride report *Many Voices, One World,* proclaiming a "New World Information and Communication Order (NWICO)"[6]. In this environment, countries receiving satellite signals wanted prior control over satellite content and nations around the equator were claiming ownership of satellites in orbital positions above their countries.

We should try not to make the same mistake with the Internet. Let's not create unnecessary global involvement or claim new technological developments are reason enough for political intervention. There is little need for global regulation of the Internet. It takes away attention from the real underlying

[2] <www.kenniswijk.nl>

[3] Also called "Fibre to the Home" or FttH.

[4] <www.icann.org>

[5] World Summit on the Information Society, Declaration of Principles, Document WSIS-03/GENEVA/DOC/4-E, Geneva, 12 December 2003; Plan of Action, Document WSIS-03/GENEVA/DOC/4-E, Geneva, 12 December 2003. Documents can be found at <http://www.itu.int/wsis/>

[6] Unesco, *Many Voices, One World* (Paris: Unesco, 1980). On the relationship between the WSIS and the McBride Report, see for example: Claudia Padovani, "Debating communication imbalances: from the MacBride Report to the World Summit on the Information Society, An application of lexical-content analysis for a critical investigation of historical legacies", Social Science Research Council at <http://www.ssrc.org/programs/itic/publications/knowledge_report/memos/Padovanimemo4.pdf>

fundamental problems – the traditional paradigm shift from goals to means – thus creating the risk of ending up with less protection of the freedom of information. And let's not forget: the whole satellite discussion ended with hardly any global regulation. Satellites are mostly dealt with on the national and regional level. There is no specific global jurisdiction on information distributed by satellites. Ultimately the international community was able to handle most issues based on the existing system of fundamental rights. It took some time to realize this, however.

Search Engines. Search engines are a second case that can be used to underline the need for sticking to existing values. The most popular search engine, Google, became a public company.[7] Out of nothing, a 27 billion euro company was created. But with what kind of services does Google intend to make money? Well, its main activity is selling the attention of end-users to advertisers. It does so by showing advertising that matches the searches of its users. It is a good thing that Google is not hiding this: several other search engines prefer not to disclose their commercial approach. However, there is one big question: How does Google's search engine actually work and what happens in the black box that generates search results? This is an important issue, because Google is a dominant gateway to information. Nowadays, electronic content can't be found without using search engines. In a way, they replace library indexes and other existing search facilities.

How exactly search engines make their selection is still a big mystery. Like Microsoft Windows, the source code of Google is not public and we have to rely on what Google tells us about its functions. For example, the brochure of the public offering first mentions the fact that Google gives "relevant and useful information" and that it "only takes the interests of users in mind", but that on the other hand a search might also result in "pertinent, useful commercial information". It is common knowledge that there are ways to get your website on the first search page. Not so long ago Google was manipulated and the words "funny hair" were linked with the web page of the Dutch Prime Minister, Jan Peter Balkenende. There are other examples of these so-called Google bombs. Some time ago typing in the question "Who is more evil than the devil?" would give "Microsoft" as a search result. Google tries to fight these manipulations. One could say that in such a case, Google is manipulating the manipulation. But how Google really works remains a well-kept mystery. The examples cited so far are rather innocent, but what about these two: Google has entered into negotiations with one of the largest scientific publishers, which – if correctly interpreted – might result in a situation where users are directed towards paid publications instead of towards free versions of the same publications (published by the researchers themselves).[8] Secondly, search engines accessible from China are configured to produce politically correct results.[9]

Search engines directly or indirectly influence the freedom to receive and impart information. They facilitate access to information, but at the same time can foreclose the access to information. Search engines can be manipulated by the operator, providers of information and those who retrieve information. Artificial search results can be created and end-users are – for commercial or ideological reasons – directed toward specific information. The users are left in the dark. Fortunately, the impact of search engines is receiving more attention. In Germany,

[7] <http://www.google-ipo.com/> or <http://www.google-watch.org/goo-s1.zip>

[8] "Reed and Google in talks to share revenue", *The Observer*, 19 September 2004.

[9] <http://www.google-watch.org/china.html>

a special non-profit organization has already been created for the promotion of search engine technology and free access to information. In German it sounds even more impressive: “Gemeinnütziger Verein zur Förderung der Suchmaschinen Technologie und des freien Wissenszugangs” (SuMa-eV).[10] This organization wants search engines to be “free, versatile, and non-monopolistic”. Another critical follower of search engines is www.google-watch.org.

To prevent the erosion of access to information as a basic value, the application or modification of existing legislation could be an option. For example, consumer protection regulation might oblige search engines to inform end-users about the way they operate. Or they could be obligated to make the source code public. Moreover, it might be advisable to give the public policy aspects more emphasis by making available transparent public facilities similar to transparent public library indexes or comparable facilities that offer an alternative to the commercially available services. Even the WSIS Action Plan recognizes the importance of this issue when it states the need to “h) Support the creation and development of a digital public library and archive services, adapted to the Information Society, including reviewing national library strategies and legislation, developing a global understanding of the need for ‘hybrid libraries’, and fostering worldwide cooperation between libraries.”[11]

Technology-Neutral Regulation. The third example concerns the notion of technology-neutral regulation as a goal in its own right. A lot of legislation and regulation which attempts to reflect underlying values is based on static technological concepts. Nonetheless, these technological concepts evolve. Old ones sometimes disappear (the telegraph), others get new functions (film), and new ones are added (CD, DVD, the Internet).

Because of this process, legislation often lags behind new developments. Existing legislation no longer works or it creates all kinds of complexities. For example, in some countries the regulation of television depends on whether or not a screen is involved. This automatically makes television regulation applicable to computer screens and therefore to the Internet.

It is often said that in this new information age, we should no longer make a distinction between technologies. In principle, such an approach is good. However, the question then arises: What kind of regulation should apply to the Internet? For example, should the "telecom model" (known for the absence of content control) be used or are we better served with the "broadcasting model" (known for its content regulation)? If this is the real question, the outcome is clear: with the increasing importance of the Internet as an information resource, one may expect that more and more elements of the broadcasting model will enter the arena of Internet regulation, certainly when the Internet becomes a substitute for traditional broadcasting reception. However, this question is based on a false proposition. A technologically neutral approach should be based on the catalogue of fundamental rights. This could mean that regulation will not always be technologically neutral, but will partly depend on the technology used. This is nothing new. For example, take the jurisprudence of the European Court for Human Rights. It gives more freedom to certain types of expression in a closed, private environment such as a theatre or gallery than to expressions that are located in areas without restrictions and accessible to an undefined audience. In such a case, the regulation is not technology-neutral, but the underlying fundamental right is.

[10] <http://www.suma-ev.de>

[11] Page 4.

Conclusion. Many more examples can be given. In a rather fragmented way, this paper has tried to illustrate that there are a lot of questions and tensions surrounding the regulation of the Internet.

First of all, most of these derive from the fact that often things are turned upside down. We think the Internet is something special and make it our point of departure for regulatory intervention or non-intervention. It should be done the other way around. The source of inspiration should be basic constitutional values, such as the freedom of information and its interpretation in jurisprudence. These values are a "living instrument" allowing us to interact with the factual circumstances, resulting in tailor-made regulation where necessary.

Secondly, the Internet has grown up and lost its innocence. The old idea of the Internet being a (or even "the") place for free exchange of ideas and opinions should be looked at in a more realistic way. This has been illustrated with the example of search engines. These gateways to the information available on the Internet are not neutral or objective, but can be a source of serious manipulation. The borders between use and abuse are seriously blurred. Regulation can be an adequate instrument to increase transparency.

Thirdly, the rather unregulated environment of the Internet also has led to a "control vacuum", which has translated into a substantial "governance" issue, where powers are being claimed that do not match with the basic constitutional values. However, lessons can be learned from the past where new technologies (satellites) were seen as a legitimation for the introduction of new governmental control over content. These attempts largely failed. There are no reasons to make the same mistakes again with the Internet.

Morris Lipson

In the Name of Protecting Freedom of Expression: Rejecting the Wrong Rule for Liability for Internet Content

It might be thought that publishing content over the Internet is pretty much like publishing material in a newspaper. As this paper explains, courts in particular have been tempted to think so. However, this fact, in combination with the fact that restrictions on the publication of content vary widely from jurisdiction to jurisdiction, yields the result, probably unintended, of a very significant threat to freedom of expression. This paper describes that threat, and recommends a way of avoiding it.

A Range of Content Restrictions. Different national and subnational legal regimes, often supported by international instruments, have content restrictions on publication (not to say, expression more generally) which may differ quite considerably. The consequence is that the publication of material in one jurisdiction, perfectly legal and non-actionable there, may well be subject to criminal or civil liability in other jurisdictions. For the purposes of what follows, I will restrict my attention to variations in restrictions on hate speech and defamation, though the points made in this paper apply with equal force to other (varying) content restrictions: on obscenity or pornography, blasphemy or sedition, among others.

Take hate speech first. In the United States, it is well settled that the publication of racially vilificatory material is protected under the First Amendment of the United States Constitution unless it is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.[1] This is a very high threshold: publications which cast clear and vulgar aspersions on racial groups, which express the strong desire that certain groups be deported or eliminated altogether, are protected unless it can be shown that they are intended to produce violence and in fact are likely to produce such violence imminently. In the United Kingdom, the test for restricting certain racial content is the substantially weaker one of whether the challenged speech is intended to stir up racial hatred and "is likely" to stir it up. By the terms of the applicable statute, at least, no showing needs be made of the *imminence* of any allegedly likely violence, or indeed of any likely *violence* at all.[2] Again, jurisdictions including Austria, France and Germany have blanket restrictions on Holocaust denial. Finally, broad and potentially far-reaching bans are common: to take one example, Article 156 of the Criminal Code of Uzbekistan prohibits the premeditated "insulting [of] citizens' feelings … committed with the purpose of … agitating … intolerance or separation between groups [which are distinguished racially or ethnically]".[3]

It must be said that international instruments reflect a far from consistent approach to what sort of expression may be prohibited as hate speech. Article 20(2) of the International Covenant on Civil and Political Rights requires the enactment of national legislation which prohibits only the advocacy of racial hatred "that constitutes incitement to discrimination, hostility or violence". In contrast, Article 4(a) of the International Convention on the Elimination of All Forms of Racial Discrimination prohibits not only the incitement of racial discrimination, but also the dissemination of "ideas based on racial superiority or racial hatred". The Additional Protocol to the Convention on Cybercrime goes even further, in both directions so to speak, in that it invites Parties to enact prohibitions which can be very broad (for example, on the mere "distribution" of racist material through a computer system [Article 3], or on the public insulting of persons "for the reason that they belong" to a racial or ethnic group [Article 5]); but it also permits Parties to opt out of these provisions (or effectively to do so). The effect is explicitly to recognize and mandate substantial differences in restrictions on hate speech.[4]

Similar, and similarly dramatic, variations in criminal defamation laws exist across jurisdictions. In Azerbaijan, for instance, you can be imprisoned for as much as two years if you defame someone, and you can go to prison for as much as six months just for insulting them.[5] Many countries have special, and particularly objectionable from the point of view of freedom of expression, criminal penalties for insulting the President or other heads of state, or for insulting public institutions or even national flags; enhanced criminal penalties are often a part of such regimes.[6] In many countries, prosecutions

[1] *Brandenburg v. Ohio*, 395 US 444 (1969).

[2] 1986 Public Order Act, Section 18.

[3] The European Court of Human Rights has found on numerous occasions that a similarly broadly-worded provision in the Turkish Criminal Code has been employed to restrict expression which is protected under Article 10 of the European Convention on Human Rights. See e.g., *Okcuoglu v. Turkey* (8 July 1999, Application No. 24246/94); *Karatas v. Turkey* (8 July 1999, Application No. 23168/94).

[4] It is perhaps worth noting that, at the time of writing, there are 23 signatories to the Additional Protocol, but there have been no ratifications.

[5] Articles 147 and 148, respectively, of the Criminal Code of 2000.

[6] For instance, the Criminal Code of Albania prohibits intentionally insulting: "an official acting in the execution of a state duty or public service, because of his state activity or service" (Article 239); "an official acting in the execution of a state duty or public service, because of his state activity or service" (Article 240); "the President of the Republic" (Article 241); "a judge or other members of trial panel, the prosecutor, the defence lawyer, the experts, or every arbitrator assigned to a case because of their activity" (Article 318); "prime ministers, cabinet members, parliamentarians of foreign states, diplomatic representatives, or [representatives] of recognized international bodies who are officially in the Republic of Albania" (Article 227); and "the flag, emblems or national anthem of foreign countries and international organizations" (Article 229). It is well to point out that this sort of enhanced coverage is precisely the opposite of what international law requires, recognizing as that law does that public officials should be required to accept more, rather than less, criticism. See e.g., *Lingens v. Austria* (8 July 1986, Application No. 9815/82) para. 43; *Thoma v. Luxembourg* (29 March 2001, Application No. 38432/97) para. 47.

under such laws occur with alarming frequency. On the other hand, however, some jurisdictions, such as Bosnia and Georgia, have actually abolished criminal defamation provisions altogether. And other countries which have criminal defamation on the books have not seen prosecutions under such provisions for many years.[7]

To repeat the principal point thus far: A racial comment, or a critical comment about a public official, may be fully protected in one jurisdiction, while at the same time sanctionable by the criminal regimes (or actionable in the civil regimes) of other jurisdictions. Indeed, some jurisdictions support the punishment, either criminal or civil, for expression which is almost certainly protected under the international law of freedom of expression.

The Newspaper Rule for Assessing Liability in Foreign Jurisdictions. Consider the situation of a newspaper publisher, facing the fact that content in his or her newspaper may not constitute illegal or civilly actionable expression in the jurisdiction where the newspaper is typically read, but would be punishable or civilly actionable in other jurisdictions. To set the stage for the special problem posed for Internet publishers by the variation of content restrictions across jurisdictions, let us ask the following: *Would the newspaper or the editor be legally liable in the event that the article in question finds its way into one of the latter jurisdictions?*

The answer is: it depends. Note, first, that publishers, particularly those whose newspapers cross national frontiers, have well-established distribution networks. Newspapers are shipped throughout the newspaper's home country, and abroad as well, to vendors who have sales arrangements with the newspaper, and to individual subscribers.

In these cases, it is highly foreseeable to the publisher that copies of the newspaper will find their way to these foreign vendors and subscribers and will be read in those jurisdictions. Indeed, it is not only foreseeable – the publisher fully intends that copies of the newspaper be sent to and read in those jurisdictions. Under these circumstances, it is appropriate, and courts and other tribunals have not hesitated in concluding, that if the newspaper contains material falling under a hate speech ban, or if it is defamatory, in one of the jurisdictions to which copies are sent, the newspaper and publisher (and perhaps others affiliated with the newspaper) will be liable for that content in that jurisdiction.[8]

This situation, which makes reasonable sense, is to be sharply distinguished from the situation in which a newspaper with certain problematic content finds its way by accident, so to speak, into a jurisdiction in which such content is illegal, notwithstanding that the content is legal in all the jurisdictions of the paper's distribution network. For example, a tourist from Uzbekistan purchases a newspaper published in the United States at LaGuardia Airport in New York. It contains racially vilificatory material relating to an ethnic community in Uzbekistan. The tourist drops the newspaper on a seat in the arrivals lounge at Tashkent airport where it is picked up by an airport employee who takes it home with her and reads it there. The newspaper has no subscribers or vendors in Uzbekistan. The reader finds the material offensive, takes it to the authorities who determine that it is illegal racist content under Article 156 of the Criminal Code, and they prosecute the publisher.

[7] A similar variation can be seen in civil defamation regimes.

[8] See e.g., *Shevill v. Presse Alliance S.A.*, Case C-68/93 (1995) 2 A.C. 18; *Berezovksy v. Michael* (2000) 2 All ER 986 (both relating to defamation, but usefully illustrating the general principle).

It is quite clear that in this circumstance, the publisher should not be held liable, and in most jurisdictions would not be so held. Why? Because it was not reasonably foreseeable by the publisher that the newspaper would be read in Tashkent; the publisher took no steps at all to get the newspaper to that jurisdiction and had no control over the fact that it would end up there. Under these circumstances, courts would hold that, in fact, the newspaper *was not published* in that jurisdiction; and on that basis would not impose liability on it there.

This hypothetical situation illustrates what I would like to call the "newspaper rule" for liability for newspaper content. According to this rule, a publisher is legally liable for content deemed illegal or otherwise actionable by a given jurisdiction as long as two conditions are met: (1) a copy of the newspaper actually reaches the jurisdiction and is read there; and (2) the publisher had reason to know that the newspaper would probably be read there – because, most prominently, the jurisdiction is in the distribution network of the newspaper. This liability rule, most crucially, imposes liability in every place in the newspaper's distribution network *where the newspaper is read, regardless of where it is produced or where the content was written.*

Applying the Newspaper Rule to Internet Publications.

Publication on the Internet is fundamentally different from publication by newspaper, in ways directly relevant to the newspaper rule. Suppose someone writes an article with racial content. It is written in the United Kingdom, uploaded and stored there on the author's website. The author knows, or should know, that the moment that the material is posted on his website, it is instantly accessible by virtually any person virtually anywhere in the world.[9] To put it another way: fundamentally unlike the typical newspaper, the Internet makes virtually every person with Internet access *within the distribution network* of any Internet publisher. And, equally crucially, this is a fact which virtually every Internet user knows, or should know.

What, therefore, if we employ the newspaper rule for fixing liability for materials posted on the Internet? It's simple really: (1) since the newspaper rule subjects a newspaper to potential liability for any content actionable in any jurisdiction within its distribution network, (2) since virtually every place with a computer connected to the Internet is within the distribution network of every website, then (3) application of the newspaper rule to Internet publication subjects an Internet publisher to liability *in virtually every jurisdiction in the world.*

As we have already seen, however, different jurisdictions have radically different content restrictive regimes; some have restrictions on allegedly defamatory material, or on allegedly racist material, which go far beyond what is permissible in one's home jurisdiction. Some, indeed, have restrictions which are not mandated by the international law of freedom of expression. Yet, if the newspaper rule is also the rule for Internet publication, the Internet publisher would be "legitimately" liable for content which is legal and protected in his or her home jurisdiction (and which might also be protected by international law), as long as (1) it is prohibited in a jurisdiction which has Internet access and (2) someone actually downloads it there.

[9] I say "virtually" for two different but related reasons. First, if I have sophisticated technical skills and some software, I can restrict access to my website, for example, only to persons who have taken out a subscription. In that case, only persons of whom I have knowledge (or should have) will have access to the site. At the other end, there may be some form of sophisticated blocking or shielding software employed by a particular server which would prevent access to my website, or to the particular content in my article on that website, for any would-be user attempting to gain access employing that server. These, however, are relatively exceptional situations.

Some Cases. Surprisingly, to some at least, it would appear that the trend has indeed been to apply the newspaper rule to Internet publication. There is, for example, the attempted prosecution of Frederick Toben, who had posted material denying the Holocaust on a website in Australia. Toben was arrested in 1999 on a visit to Germany and was tried there, in part for inciting racial hatred. That part of the prosecution was based on the fact that the materials on his website had been downloaded in Germany. The trial court had dismissed the charge because the offending materials "existed" outside Germany, but the *Bundesgerichtshof* reversed, holding that German laws prohibiting the glorification of the Nazi party could be applied to materials situated outside Germany as long as they were downloaded within the jurisdiction.[10]

A defamation case brought in Australia applied similar reasoning. *Dow Jones & Company Inc. v. Gutnick*[11] concerned the uploading by the *Wall Street Journal* of a story which made critical comments about Gutnick, an Australian businessman. The story was written in the United States, and was uploaded and stored on a computer there. Gutnick downloaded the story in Australia, read it there, took offence and sued the *Wall Street Journal* for defamation in Australia. It is highly likely that the material in question would not have been found to be defamatory in the United States, but could well have been so found under the defamation laws of the Australian state where the download occurred. Again, the *Wall Street Journal* argued that publication occurred in the United States, where the material was uploaded and stored; Gutnick disagreed, arguing that publication occurred where download occurred – in Australia. At a crucial point in its reasoning, the court wrote that "those who post information on the World Wide Web do so knowing that the information they make available is available to all and sundry without any geographic restriction". The court's point appears to be that in this respect the same applies to Internet and newspaper publishers. As newspaper publishers know about and control their distribution networks and have full knowledge of where the content of their newspapers is likely to be read, it is appropriate to impose liability on them for any content found problematic anywhere in their distribution networks. In the same way Internet publishers have full knowledge that the reach of the materials they publish is everywhere (that is, the whole world is in their distribution network), and therefore imposing liability in any jurisdiction in which the material is downloaded is entirely proper. On this basis, the court took the case.

Conclusion. Applying the newspaper rule to Internet publication subjects Internet publishers to the content restrictions of virtually every country on earth, regardless of whether such content restrictions exist in the jurisdictions where such publishers live,[12] and regardless of whether the foreign restrictions comply with the international freedom of expression standards. Application of the newspaper rule will subject persons living in regimes whose laws fully protect freedom of expression to the laws of regimes which regularly censor, and whose public officials otherwise keep a stranglehold over the press

[10] See "German Hate Law: No Denying It", available at <www.wired.com/news/politics/0,1283,40669,00.html>. Another case of the same ilk involved Yahoo!, Inc., which operated an automated online auction site from the United States. Nazi memorabilia were offered for sale on the site – perfectly legally in the United States, but illegal in France. Persons in France were able to access the site. The French Union of Jewish Students brought suit against Yahoo! for violating France's prohibition on Holocaust denial. The French court found a basis for taking jurisdiction of the case based on the fact of the availability of the materials, by download, in France.

[11] (2002) HCA 56.

[12] As often as not, of course, Internet publishers are individuals, writing and working from their own homes and uploading their materials on their home personal computers.

and others by the use and abuse of content-restrictive laws. Of course, this may not be a particularly fearsome prospect for those Internet publishers who do not expect ever to find themselves in jurisdictions far from home where they may be subject to suit. On the other hand, it may well cause a great many persons to think twice before uploading material protected "at home" because of what may happen to them when they travel abroad.[13] The potential for the chilling of expression, in other words, is considerable.

A full respect for freedom of expression requires a different treatment for Internet publication. The Internet, as has often been noted, is a liberating tool, a tool with which ordinary individuals can reach out across the globe to communicate with others on matters of concern to them. It is a means of transcending borders and differences. Yet, a rule which catapults the unknown laws of unknown places into the communication space of persons living in freedom-protecting countries has precisely the opposite effect: of stifling expression for fear of legal – often criminal – liability abroad.

It may not be perfectly clear what the precisely right liability rule for Internet publication is. Perhaps it is to impose liability only where material uploaded is actionable in the jurisdiction of upload. Perhaps it is to impose liability in those jurisdictions where materials are downloaded provided that the author is "substantially connected" to the download jurisdiction. But what is certain is that, in the name of freedom of expression at least, *the newspaper rule must not be the rule of liability for Internet publishers.*

[13] Not to mention the simple fact that many Internet publishers will not wish to face the possibility of having criminal convictions or civil judgements entered against them in foreign jurisdictions even if they have no intention of travelling there, and even if such judgments would not be enforceable in their home jurisdictions.

Lee Hibbard

Internet with a Human Face – A Common Responsibility[*]

Introduction

- The right to freedom of expression for the purposes of Article 10 of the European Convention on Human Rights (ECHR) is a fundamental guarantee for media freedom. This freedom is "technology neutral" and therefore remains unchanged by the Internet as an important tool in informing and shaping public opinion by providing information which has been gathered and processed in accordance with professional standards in order to scrutinize public authorities and other power holders in society.
- The Council of Europe considers that "independent, professional journalism adhering to ethical standards will not be less important in the Information Society than before. The provision of relevant, timely and well-researched information by media professionals will continue to be essential in laying the foundations of an informed public debate about current affairs and public policy."[1]
- The Internet has, however, brought about greater media speed and greater volumes of information to the public via the media and has also multiplied the number of Internet (new media) actors which can be argued to threaten both

[*] This paper reflects the views of the author and not necessarily those of the Council of Europe.

[1] Paragraph 14, "Democracy, human rights and the rule of law in the Information Society" – Contribution by the Council of Europe to the second Preparatory Committee for the WSIS (February 2003).

the quality of information by the Internet and, as a corollary, the future of traditional and electronic media. Both the speed and the volume of information on the Internet and the arguable lack of transparency in decisions made regarding Internet content call for particular care to be taken by (media) content producers and disseminators, notably in order not to harm human dignity and the rights of individuals, especially minors.

Freedom of Communication on the Internet and the Media

- The Council of Europe is particularly concerned about the right to freedom of information and to receive and impart information and ideas without interference by public authorities for the purposes of Article 10 ECHR. The Organisation believes therefore that attempts to limit public access to communication on the Internet for political reasons or other motives are contrary to democratic principles.
- In the 2003 Declaration on the freedom of communication on the Internet, the Council of Europe member States made several important declarations which positively affect media freedom on the Internet *inter alia*:

  a. member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery (Principle 1),

  b. self-regulation and co-regulation is encouraged (Principle 2),

  c. public authorities should not – through general blocking or filtering measures – deny access by the public to information, regardless of frontiers (Principle 3),

d. fostering access to the Internet and the active participation of the public on the Internet is important (Principle 4),

e. freedom to provide services via the Internet (Principle 5) should not be restricted,

f. the importance of limits on the obligations (liabilities) of service providers for Internet content, coupled with the introduction of co-responsibility (Principle 6),

g. the principle of anonymity *inter alia* in order to enhance freedom of expression (Principle 7).

- These principles, adopted by Council of Europe member States, reinforce the importance of freedom of expression and information while at the same time stressing a more limited role for member States in controlling such (media) freedoms on the Internet. These principles empower the (new) media in regulating themselves on the Internet and should inspire them to take an active and participatory role in promoting the wider democratic participation of individuals in public life with the help of interactive new technologies.

Council of Europe Legal and Political Instruments

- The Council of Europe has developed a series of international legally binding instruments directly and indirectly concerning the Internet. These include the Convention on Cybercrime (CETS 185) and its Additional Protocol[2], Convention for the protection of individuals with regard to automatic processing of data (CETS 108) and its Additional

[2] Convention on Cybercrime (CETS 185) which *inter alia* criminalizes new types of crime using information communication technologies, and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189) which is a reaction to highly offensive material that undermines human dignity (thereby displaying a zero tolerance attitude to such content).

Protocol[3], all of which reflect the belief that cyberspace is not a lawless area in which member States have an obligation to uphold the law, using their national laws, in order to protect individual rights and freedoms.

- This is reinforced by a series of politically binding instruments[4] positively regulating the media environment with regard to the media and violence, the media and video games (games being considered as a form of "mass media") and, more recently, regarding new media and the right to reply which is currently under preparation as a Council of Europe Recommendation.
- Moreover, the Council of Europe has produced a series of political (non-legally binding) statements[5], and more recently has consolidated its position with regard to the Information Society for the purposes of the World Summit on the Information Society (WSIS) by underlining *inter alia*:
  a. respect the rule of law on the Internet: "the Rule of Law will be a reality when state regulation, co-regulation and self-regulation work together under national legislation and international standards to build a clear regulatory framework in full respect of Human Rights";[6]
  b. the importance of quality information on the Internet as barriers fall and "public authorities try to support citizens in reaching for reliable and comprehensive information through all media";[7]
  c. the vital role of the traditional media, including local and community radio, in programming, producing, and distributing diverse, high-quality content in the Information Society and providing moderated platforms for public debate.[8]

- These legal instruments and political statements impact directly and indirectly on media freedom on the Internet and provide clear proof of the commitment of Council of Europe member States to promoting all media, including new media, as responsible, professional and independent.

[3] Convention for the protection of individuals with regard to automatic processing of data (CETS 108) and its Additional Protocol regarding supervisory authorities and transborder data flows (CETS 181) which calls for *inter alia* national data protection laws that strike a fair balance between respect for privacy of individuals and the free flow of information between peoples.

[4] Recommendation (97)19 concerning the (determination of responsibilities for the) portrayal of violence in electronic media; Recommendation (92)19 on video games as mass media which concerns a review of member States' legislation regarding video games – as a form of mass media – containing racist content, discrimination, hatred and violence in order to protect young people; Recommendation (89) 7 of principles on the distribution (as well as regulation of systems of classification and control) of videograms having a violent, brutal or pornographic content which also includes references to various dissuasive measures and the application of criminal law; Recommendation (2001) 8 on self-regulation concerning cyber-content (self-regulation and user protection against illegal or harmful content on new communications and information services) which promotes the development of content descriptors, content selection tools, content complaints systems etc., in order to raise the levels on information and awareness of content.

[5] Political Message from the Committee of Ministers of the Council of Europe to the World Summit on the Information Society (WSIS) (Geneva, 10–12 December 2003); 1999 Committee of Ministers Declaration on European policy for new information communication technologies which encouraged self-regulation and development of technical standards and systems codes of conduct; 1997 Council of Europe Summit called for "a European policy for the application of new information communication technologies with a view to ensuring respect for human rights (…) fostering freedom of expression and information (…)"; 1997 5th Ministerial Conference on Mass Media Policy on "the Information Society: a challenge for Europe", and its Action Plan encouraged *inter alia* self-regulation by providers and operators of new information communication technologies (e.g. codes of conduct etc.), the study of misuse of new information communication technologies in spreading ideology and activities contrary to human rights and thereby to formulate proposals or other (legal) action to combat such misuse, the examination of the opportunity and feasibility of establishing warning, co-operation and assistance procedures, and the study of practical and legal difficulties in combating dissemination of hate speech, violence and pornography.

[6] Paragraph 13 of the Political Message from the Committee of Ministers of the Council of Europe to the World Summit on the Information Society (WSIS) (Geneva, 10–12 December 2003).

[7] Idem, paragraph 4.

[8] Idem, paragraph 5.

European Forum on "Internet with a Human Face – A Common Responsibility" (Warsaw, 26–27 March 2004)

- The title of my presentation bears the same title as the recent European Forum that was organized by the Council of Europe and the Safe Borders Consortium that was co-sponsored by the European Commission through its Safer Internet Action Plan – "Internet with a Human Face – A Common Responsibility" – which took place in Warsaw on 26 and 27 March 2004. This title evokes, in my opinion, the important need to visualize and to understand the Internet better in order for us all – including the media – to take greater responsibility for it.
- This Forum was one of the latest activities of the Council of Europe to address some of the challenges posed by the Internet, in particular as regards the protection of vulnerable groups such as minors regarding harmful content. The Forum concluded *inter alia* that cyberspace should not be a lawless area and that member States have an obligation to uphold the law in this field as well as others in order to protect individual rights and human dignity. Both national and international law are therefore of particular importance as is self-regulation and co-regulation of the media profession.
- The Forum was unable to resolve the quagmire regarding legal responsibility and jurisdiction for Internet content, and such legal uncertainty does not help to strengthen media freedom when faced with defamation proceedings. Instead, the Forum encouraged international co-operation across governments, other agencies, industry and advocacy groups, and emphasized the need for greater awareness raising, media literacy and a better understanding of (harmful) content. All of this underlines the fact that the Internet is a com-

mon and shared responsibility requiring a co-ordinated and strategic approach by embracing all Internet actors with the participation of all relevant media.

7th European Ministerial Conference on Mass Media Policy (Kiev, 10–11 March 2005)

- European media policy will be examined and developed in the light of the forthcoming European Ministerial Conference on Mass Media Policy, to be held in Kiev in March 2005, which will address *inter alia* human rights and regulation of the media and new communication services in the Information Society. On this occasion, it is quite clear that the results of the European Forum will be taken into consideration by the European Ministers in particular as regards the roles and (ethical) responsibilities of different Internet actors including the media and the (media) freedom of communication on the Internet.
- At the same time, the Organisation is aware of the potential of the Internet and the media and is currently addressing the impact[9] of the Information Society on the interpretation of human rights and their protection using the Internet and other means of electronic communication as part of the Council of Europe's contribution to the 2005 Tunis World Summit on the Information Society.

[9] In considering any such impact, one member State is interested to know: (i) whether the right to freedom of expression applies equally to the old media as to new media operating on the Internet, (ii) whether regulation aimed at protecting minors from violent films applies equally to films broadcast on television as to films broadcast on the Internet, and, more broadly speaking, (iii) how should fundamental human rights, such as the right to respect for private life and the right to freedom of expression, be interpreted in a world that is becoming more and more digital?

Conclusions

- It is clear that the Council of Europe is a bastion of media professionalism and independence in Europe and that the 46 member States of the Organisation are committed to preserving and promoting the right to freedom of expression and information for the purposes of the "technology neutral" Article 10 ECHR.
- On the occasion of the 7th European Ministerial Conference on Mass Media Policy in Kiev in 2005 the media will (hopefully) reflect and reassert media freedom on the Internet. At the same time however, the media are independent and they must assert and (re⸮)position themselves to accommodate the growth in the number of media appearing on the Internet landscape.

The Media Freedom Internet Cookbook

- In the light of what I have considered in this report, my recommendations for *The Media Freedom Internet Cookbook* are quite straightforward:

  a. Promote media freedom (on the Internet) emanating from Article 10 ECHR and the case-law of the European Court of Human Rights as well as from relevant Council of Europe legal instruments and political declarations;

  b. Promote media integrity and professionalism on the Internet; this could be achieved indirectly by using the media to actively promote the public's use of interactive technologies and its participation in political life,

  c. Actively lobbying the WSIS process to promote professional media on the Internet,

d. Follow, endorse and, where possible, participate in the Council of Europe's ongoing work in the media, in particular as regards its intergovernmental work to be carried by its Group of Specialists provisionally entitled Group of Specialists on Human Rights in the Information Society (MM-S-IS),

e. Encourage self-regulation and co-regulation initiatives regarding the media and the Internet.

Self-regulation, Co-regulation, State Regulation

Hans J. Kleinsteuber

The Internet between Regulation and Governance

Fresh Thinking and the Internet. Government actors in many countries attempted to react to the Internet using conventional means of the state apparatus, like passing laws in parliament or having courts judge over access to unlawful content. In most cases this proved to be fruitless; in fact it demonstrated the weakness of the traditional nation-state in attempts to regulate the Internet. Just to give a few examples: since 1997 there has been a law on digital signature (the oldest in the world) in Germany, but after seven years there is still no practical way to sign a contract on the Net. In several countries, courts have attempted to punish Internet service providers (ISPs), which allowed access to hate speech or child pornography for example, usually without any success. True, there are governments like Singapore or China that censor content on the Net, but the effect is limited as the fluidity of the Net often means that filtering programs can be circumvented.

This paper is about the obvious weakness of the traditional nation-state and its instruments *vis-à-vis* the Internet and new ways of coping with the problem. It is often the State itself that encourages unconventional action as this releases it from difficulties in fulfilling its obligations. A Council of Europe Recommendation of 5 September 2001 encourages self-regulatory organizations, especially in the field of media regulation. Innovative concepts of regulation and governance are being tested and decision-making procedures in a global environment are being addressed. This requires new ways of thinking:

- Firstly, it is necessary to assess existing concepts of regulation and governance (from pre-Internet times) and consider how they may be applied in the Internet age.
- Secondly, recent and encouraging developments can be observed that might lead to a new era of global Internet governance.
- Finally, ten rules of Good Internet Governance will be proposed that define trends and values for the emerging structure of global Internet regulation.

State Regulation and Self-regulation. Regulation in the original sense refers to an arbitrary process under the rule of the State, usually centred in a (more or less) independent regulatory body. This body makes decisions in situations where there are conflicting interests. The idea is that decision-making is so complex that a specialized body of independent experts is better equipped to do this than state bureaucrats. The term "regulation" is already mentioned in the US Constitution, dating back to the late eighteenth century. Regulatory bodies are also not new. The first "watchdog agencies" were established in the US in the second half of the nineteenth century for the private railroad industry.

One field that is regulated by the State is broadcasting. More precisely, this means that the State issues radio and television licences and supervises the industry. Again this first emerged in the US in the 1930s (FCC 1934) in the context of commercial broadcasting. Europe did not experiment with regulatory bodies until the 1980s. Today examples of these are Ofcom that was recently established in Britain, the Conseil Supérieur de l'Audiovisuel Français in France or equivalent bodies in the German *Länder* or States. Bodies of this type are usually constructed like a court, with collective decision-making somehow reflecting the work of a "jury". They have to handle applications from different interests and may also adjudicate between the interests of the broadcasting industry and the public. Their main task is to hammer out a lasting compromise, not to decide what is legal or unlawful. One obvious problem is that these authorities are potentially weak and vulnerable to being "taken over" by the industries that (mis)use them for their own interests, for example to keep newcomers away from the market or to increase tariffs (e.g. for cable fees).

This traditional version of regulation contains – especially in the European perspective – "the idea of control by a superior; it has a directive function"[1]. As matters of broadcasting regulation tend to be very complex, these bodies are soon overloaded with work and usually encourage self-regulation of the industry. This means that the actors are urged to solve problems among themselves, before turning to the state regulator. As it usually reflects the interests of the industry to keep the State out of its affairs, it accepts this obligation. Therefore state regulation is usually accompanied by self-regulation. This type of self-regulation is done under the "shadow of the State", meaning that all sides act under the threat that the State may intervene if no compromise is found or public interests are seriously threatened.

If the State and the private regulators co-operate in joint institutions, this is called "co-regulation". If this type of self-regulation is structured by the State but the State is not involved the appropriate term is "regulated self-regulation"[2]. This type of regulation was first developed in Australia.

[1] A. Ogus, *Regulation. Legal Form and Economic Theory* (Oxford: Calderon Press, 1994), 2.

[2] Wolfgang Hoffmann-Riem, *Modernisierung in Recht und Kultur* (Frankfurt: Suhrkamp, 2001).

But self-regulation may also be found where there is no state regulation. One might say that self-regulation looks back over a long tradition, especially in environments where no state authority was available. It was quite well developed in early networks of long-distance traders, e.g. in the Mediterranean region (Lex Mercatoria, eleventh century) or in the Hanseatic League, covering the North and Baltic Seas.[3]

Modern self-regulation again started in the US with industry associations that defined their own code of conduct. And only those who adhered to these self-defined moral rules were entitled to become members. Whoever did not follow the rules voluntarily, could not be formally punished, but there were sanctions like being excluded from the association and/or making public the accusations. The first organizations that followed these procedures were associations of newspaper publishers and editors in the 1920s.

The best known fields for this type of self-regulation in Europe are the press councils that may be found in a majority of EU member countries today.[4] The press council movement started in the 1950s in Britain and later in Germany. The first step was usually taken by the State, which planned to intervene in the matters of the industry with a law. The press industry retaliated by offering to build an autonomous structure for complaints that would be handled before independent bodies, constituted and financed by them. Decisions are made based on a Code of Ethics for Journalists that is then applied to individual complaints. In a similar way to a court, the case is considered by a jury. However, this jury consists of representatives from the industry, possibly of active journalists and media professionals and perhaps also laypeople. They consider the case together and issue a ruling that is made public. If a publication is being criticized, it is expected to publish the criticism, but it cannot be sanctioned if it does not.

The advantage of this type of self-regulation is that representatives from the profession and not regular judges pass judgement on complicated matters of journalistic reporting and decide what is acceptable and what crosses the borderlines. This adheres to the idea of a peer review. Most European countries have press councils although these differ very much in the way they work. Even though press councils usually date back to pre-Internet times, they have extended their activities and are today responsible for online publications as long as they are of a journalistic nature. There are other fields of pre-Internet self-regulation, the most prominent being the classification of films and movies, which is mandatory in most European States.[5]

Both variations of regulation – by the State and by the industry itself – are highly relevant for the development of Internet regulations. Practically all European regulatory bodies in broadcasting started with a limited range of activities. But with the convergence of broadcasting, telecommunications and information technology, they have to widen their regulatory responsibilities or merge with institutions that regulate telecommunications. The American Federal Communications Commission (FCC) has covered all communication sectors since it was founded in 1934 (www.fcc.gov). As a result it only had to co-ordinate and merge its internal handlings. In Britain, Ofcom was established in 2004 incorporating the work of five former agencies that had been performed independently before (www.ofcom.gov.uk). In other countries, like Germany,

[3] Michael Latzer et al., *Selbst- und Ko-Regulierung im Mediamatiksektor. Alternative Regulierungsformen zwischen Staat und Markt* (Wiesbaden: Westdeuscher Verlag, 2002), 9.

[4] Danilo A. Leornardi, *Self-Regulation and the Print Media: Codes and Analysis of Codes in Use by Press Councils in Countries of the EU*, 2004.

[5] Oxford University, Programme on Comparative Media Law and Policy, *Self-Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis* (Oxford, 30 April 2004), 57–60.

the convergence of regulatory structures has not even started. It remains to be seen to what extent the logic of "old" regulatory action will be able to cope with the Internet.

A new field of industry self-regulation has emerged in relation to the Internet. This is based on codes of practice that regulate issues like respect for privacy, public decency, protection of minors, accuracy or the application of filtering software. An important part is played here by Internet service providers (ISPs) and their respective industry associations. A recent study identified self-regulatory activities in most EU countries although there were considerable differences between them. The study comes to the general conclusion that the "most successful self-regulatory activity has taken place where there is a key legal basis; e.g. in relation to complaints about illegal content."[6] Regulation was less successful when public policy objectives are not clear or consensus is difficult to build. Often the codes of practice are little known and insufficient transparency and accountability in the process of code production and application were mentioned. Other fields of self-regulation of the Internet and digital media include Internet content, the electronic game industry and mobile Internet services.[7]

The distinctive feature of these regulations is that they were removed from traditional state bureaucracy, which was unable to handle the details of Internet communication. Problems arise when bodies are "captured" by private interests. Regulation and self-regulation in Europe reflect the thinking of a corporate age in which co-operation between industry and professional associations, rather than the State, is seen as a move away from "big government".

These "old" procedures of regulation were devised at a time when citizens and the civil society were not yet seen as autonomous actors with independent competence and expertise. Therefore in these regulatory schemes there is no room for the participation of the "public", or representatives of non-governmental organizations (NGOs) and citizen action groups. As a consequence, regulation was left to the experts, mostly in the industry but sometimes in co-operation with professional organizations. Laypeople are rarely involved. The one exception is the traditional idea of the "ombudsman", a well-accepted person who represents the interests of "ordinary" people. The lack of citizens' representation certainly has to do with the fact that the civil society was not involved in the "old" media, so no need was felt to include citizens or their associations in the regulatory process.

The concept of governance is more recent and reflects the fact that over the past decades civil society organizations were increasingly voicing their concerns about many issues (including environment, gender, unemployment etc.). This certainly affects new forms of communication and the Internet.

Governance. Even before the "discovery" of governance it had become a common insight that conventional political decision-making is no longer appropriate to solve many of the complex challenges. It might be more effective to have decision-making organized in policy networks – informal structures of different actors with mixed public and private backgrounds. In EU schemes the search was for a "third way" between supranationalism and intergovernmentalism and the solution was seen in forms of self-regulation as well as European "multi-

[6] Oxford University, Programme on Comparative Media Law and Policy, *Internet Self-Regulation: An Overview*, 2004 <www.selfregulation.info/iapcoda/03029-selfreg-global-report.htm>, 2.

[7] Oxford University, Programme on Comparative Media Law and Policy, *Self-Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis* (Oxford, 30 April 2004), 37–57, 61–70.

level" governance.[8] Other spectators saw the need for "self-organizing, interorganizational networks" that they called governance.[9]

Governance was first developed in the 1980s as a concept to introduce good behaviour in companies, with the intention to improve relations with the public and make decisions more transparent.[10] The term was then introduced in the analysis of international relations, reflecting the fact that in the absence of global government, successful decision-making becomes a highly complex procedure between national governments, global organizations like the UN, economic actors and NGOs.[11] Civil society representatives were closely involved in global UN Conferences on Environment, Women, Health etc., which started in the early 1990s. These conferences can therefore be seen as good examples of emerging governance. Certainly the two-stage World Summit on the Information Society (WSIS), with its first meeting in Geneva (2003) and the final conference in Tunis (2005), follows this tradition and serves as a good example of Internet governance.

Modern governance has different meanings. A rather general definition describes it as government that interacts with society, applying interactions "with a 'co'-public-private character, offset against a 'do-it-alone' government perspective".[12] According to the Dutch scholar Jan Koosman, governance describes a mix of all kinds of social responses to changing government demands, based on the idea that governance is made up of both public and private "governors". In contrast to concepts of self-regulation, which were primarily developed in law and reflect legal thinking, governance is a "socio-political" term and is based predominantly on social and political science analysis. A crucial aspect is the idea that political decision-making should go beyond the strict boundaries of state apparatus and should seek to involve interested and competent partners in the economy and civil society. It is especially the inclusion of the civil society and its representatives, old associations and new non-governmental groups, allowing new forms of public interest advocacy, that is typical for concepts of governance.

The logic of governance existed before the Internet and has been successfully practised in various situations. One might recall the "round tables" at the time of the transformation of politics in many former communist countries. Representatives from all layers of politics, economics and society, including former Communists and members of the opposition, sat together to find viable solutions. Including representatives of all "socially relevant groups" on the broadcasting boards of public service radio and television stations in Germany, as has been the practice since the late 1940s, also points in this direction.

Whereas self-regulation works best under the "shadow of the State", which provides a "safety net" if self-regulation fails, governance calls for collaboration with the State. Governance makes the decisions instead of the State and expects the State to respect these. Of course, governance is a concept that is in an experimental phase and still has to prove its usefulness in a global context.

[8] Michael Latzer et al., *Selbst- und Ko-Regulierung im Mediamatiksektor. Alternative Regulierungsformen zwischen Staat und Markt* (Wiesbaden: Westdeuscher Verlag, 2002), 35.

[9] R.A.W. Rhodes, *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability* (Buckingham/Philadelphia: Open University Press, 1997), 46.

[10] Arthur Benz, "Governance- Modebegriff oder nützliches sozialwissenschaftliches Konzept?", in Benz (ed.), *Governance - Regieren in komplexen Regelsystemen. Eine Einführung* (Wiesbaden: Westdeutscher Verlag, 2004), 12–28.

[11] Maria Behrens, "Global Governance", in Benz (ed.), *Governance - Regieren in komplexen Regelsystemen. Eine Einführung* (Wiesbaden: Westdeutscher Verlag, 2004), 104–24.

[12] Jan Koosman, *Governing as Governance* (London: Sage, 2003), 3.

Beginnings of Global Internet Governance. In order to cope with global issues relating to the Internet, including the future of the Internet Corporation of Assigned Names and Numbers (ICANN), the World Summit on the Information Society (WSIS) in Geneva in December 2003 called for action. On 11 November 2004 the Secretary General of the United Nations Kofi Annan announced the establishment of a new Working Group on Internet Governance (WGIG). Some of its obligations are:

- to define Internet governance;
- to identify public policy issues that are relevant to Internet governance;
- to develop a common understanding of the respective roles and responsibilities of governments, international organizations and other forums, as well as the private sector and civil society from both developing and developed countries.[13]

The 40-member Working Group is chaired by Nitin Desai, Special Adviser to Annan for the WSIS. The Swiss diplomat Markus Kummer was appointed Executive Coordinator of the WGIG's Secretariat. The UN emphasized that it will provide for an "open and inclusive" process and "a mechanism for the full and active participation of governments, the private sector and civil society from both developing and developed countries, involving relevant intergovernmental and international organizations and forums."[14] The members of the first, governmental bank consist of representatives of national governments, usually from the Telecommunications Ministries (in the case of the European Commission the Information Society Director-General). A second bank, mainly of economists, includes personalities from different industrial sectors and their trade associations. Activists from the civil society side showed satisfaction that nine of their ten proposals had been accepted.

Karen Banks, Director of the London-based organization GreenNet, Association for Progressive Communications, is one of the members of this third bank. Another representative is Wolfgang Kleinwächter, Professor for International Communication Policy and Regulation at Aarhus University. It seems that because of the plurality and diversity of competence the WGIG is well prepared to do its job. The same applies to the regional distribution of the members, which – projected on the globe – would look like a graphic version of a "policy network" that includes all major spaces of the world.

The WGIG is expected to submit its report to the Secretary General by July 2005. Issues that should be addressed include the management of Internet resources, network security, cybercrime, spam and multilingualism.[15]

The WGIG is so far the most striking example of the incorporation of governance structures into the future of the Internet. On the other hand, the Working Group does not follow all the principles of fully fledged governance that have been devised in academic research. For example, the members have been appointed, the body is not self-organizing and it may only supply proposals instead of making binding decisions. In spite of this it may serve as a role model for the establishment of future regulatory bodies on Internet issues.

Thinking about the Future of Internet Governance. The introduction of the Internet – in complete contrast to earlier technologies of communication – was accompanied by procedures and patterns of behaviour that have evolved among users of the Internet. This could very well be described as practical self-regulation. "Netiquette" was the first informal code of conduct

[13] UN Press Release, "United Nations establishes Working Group on Internet Governance", 2004 <www.un.org/News/Press/docs/2004/pi1620.doc.htm>

14 and 15 Ibid.

that was not developed by industry representatives but users who wanted to utilize the Net for themselves in a civilized way. This logic should be extended and made popular among all Net users. It should also serve as a blueprint for other forms of regulation.

It has become clear that coping with the Internet requires innovative and new ways of thinking. The conventional law-making process centred around a nation-state, its lawmaker, bureaucracy and court system proved unsuccessful in most cases. There are two reasons for this: firstly laws cannot regulate the Internet in many cases, and secondly the Internet as a global medium cannot be caged in by nation-states. Instead new concepts are required and, as Lawrence Lessig demands, "code instead of laws" are needed.

Regulation of the Internet is complicated and should be limited to fields where it is unavoidable. Preferably the Web should be seen as a space that works best autonomously and without any intervention. If regulation appears unavoidable though, it should be applied according to the principle of subsidiarity, meaning that regulation should be as close to the source of trouble as possible – close both in terms of geography and competence. Regulated self-regulation is here a preferable option to a regulatory authority. The best model though is that of governance as it includes all relevant stakeholders.

Successful regulation of the Internet requires a high level of competence and expertise. The knowledge of how it can best be achieved is distributed across different segments of society and includes representatives of governments, industry, the users themselves and citizen action groups. Without their joint involvement, no regulation of the Internet will ever be successful. When structures or institutions for Internet regulation are being designed they should follow the multi-stakeholder approach of governance that includes "governors" from different segments of society, geographical regions and genders etc. No sector should be allowed to dominate and the overall strategy should be based on compromise.

A crucial element of governance procedures is transparency, both in the selection of "governors" and in conducting its day-to-day work. The emphasis on transparency follows the principle that any regulatory action should be proposed, openly and widely disputed and finally executed in public, with an openness that clearly expresses responsibilities for decisions. At the same time transparency reduces mistrust against those who are in charge. A perfect means for achieving this transparency is the Net itself. For example, meetings of the regulators should be held in public and be made available worldwide via video stream. The Net should be utilized to collect proposals and statements from interested users. Negotiations should be accompanied by Net-based mediation and presentation. The results of regulatory work should be made available on the Net.

An important element of governance is trust and legitimacy. Governments receive legitimacy through general elections and parliamentary action. Participants in governance processes have to bridge a trust gap. Until now members of governance bodies have been appointed, which means that there is little legitimacy. But self-organization and the selection of representatives by the respective constituencies and stakeholders are certainly possible. The best way is to base their legitimacy on new Net-based votes, including Net-based elections of representatives and referenda or opinion polls about options proposed by the regulators. Thinking through the concept of governance to take it one step further, one could combine the WGIG logic with that of other Internet experiences.

ICANN is at present a company that cannot act independently from the Commerce Department of the US Government.[16] Network administration by ICANN could in the future follow the self-regulatory logic of global governance, i.e. as an international corporation under UN authority with a board of globally selected governors. These governors could be elected in different world regions in Internet-based elections of a kind that have already been practised by ICANN. During the ICANN elections of 2000 it was demonstrated that votes are possible outside the structure of the nation-state and this should be used as a role model.[17] As a result ICANN could be a very good starting point for establishing a role model for an international Internet regime that follows the logic of governance.

Freedom, diversity and pluralism must be predominant values in the work of governance bodies. Freedom primarily refers to the rules of freedom of expression and information as stated in democratic constitutions and international conventions on human rights. But it also applies to the interaction between the States and their citizens. Government bodies should only intervene in matters of the Internet if this is unavoidable and there is no other possible solution. Censorship, filtering and other repressive measures should not be tolerated. But the Internet is not just threatened by state activities, it also faces the danger of "privatized governance". This occurs when a few industrial actors become so powerful that they are able to take over the regulatory process and define the rules. Diversity and pluralism as values do not just refer to the content of the Internet, they are also values of utmost importance in the selection of regulators. Global public policy should become a champion defending these values. Part of the working mechanisms of Internet governance bodies could be complaint procedures. Those who feel threatened by any kind of restrictions on their freedom could appeal to the body that could act as a form of jury and decide how to proceed.

A cautious form of regulation and governance cannot, of course, solve all problems posed by the Internet. It is based on technical designs that are mostly decided upon by hardware and software companies, not bodies of government or governance. The technical architecture of the Web must reflect values like openness, competition and easy access. It must be a central task of regulatory action to protect these features and to develop the courage to counteract any trends that could lead to the monopolization of Internet activities. As the freedom of the Internet will not happen automatically and there will always be the danger of deterioration, a competent and knowledgeable global network of "governors", following the logic of governance, that keeps careful watch is probably the best guarantee for a promising future.

[16] Monika Ermert, "ICANN, WSIS und die Selbständigkeit der Internet-Verwaltung", *Heise-Online-Newsticker*, 20 July 2004 <www. heise.de/newsticker/meldung/49236>

[17] Ingrid Hamm and Marcel Machill (eds.), *Wer regiert das Internet? ICANN als Fallbeispiel für Global Internet Governance* (Gütersloh: Verlag Bertelsmann Stiftung, 2001).

Christopher T. Marsden

Co- and Self-regulation in European Media and Internet Sectors: The Results of Oxford University's Study www.selfregulation.info*

1. Introduction: Co-regulation of the Media in Europe

PCMLP (Programme on Comparative Media Law and Policy) recently completed a two-and-a-half year empirical investigation into regulatory change with its final report for DG Information Society, the IAPCODE (Internet Action Plan Codes of Conduct) study of May 2004.[1] This article outlines the main findings and research questions answered and explored by the report. PCMLP adopted an overtly empirical and applied methodology to the IAPCODE project, recognizing that co- and self-regulation result from institutional settlements and negotiations between various stakeholders (corporate, government and viewers/consumers). By tunnelling down from legislation and regulation into self-regulatory codes of conduct voluntarily agreed by industry, and supervised by user groups and regulators, PCMLP was able to build a substantial capacity for analysis of such codes, and therefore the real commitments agreed to by actors. After the policy debates, and consequent concrete codes agreed to, PCMLP recognized a vital further empirical investigative stage – into codes in action, the

* This article is based on the executive summary of the final report delivered to the Directorate General Information Society of the European Commission, in May 2004. My thanks to Damian Tambini, Danilo Leonardi and Marcus Alexander at Oxford, and Richard Swetenham at the Commission, for help and advice. All errors and omissions remain my own.

real enforcement behaviour of self-regulated actors. It was here, in the development of the practice and culture of compliance with voluntary self-regulation by actors, that the real differences between shades of regulation were seen. Over the period from 2002 to 2004, across media sectors and national borders, the PCMLP investigation uncovered huge variety in regulatory effectiveness and real-life examples of regulation that varied from more-or-less state-sanctioned and required regulation, which was closer to command-and-control than even co-regulation, across varieties of co-regulation, to an almost pure form of self-regulation.

Legal and regulatory certainty is a prerequisite for a vibrant, innovative and economically strong EU multimedia industry.[2] Effective content regulation is necessary to protect the public interest in cultural and linguistic diversity, rights to information, minors, human dignity and, in areas like advertising and telesales, to protect consumers. The European Commission recognizes that co-regulation can be used as a means to implement objectives set by directives and has outlined in the White Paper on European Governance[3] a set of conditions under which it will consider the use of co-regulation. Co-regulation is a pragmatic response to the common perception that regulatory frameworks must quickly adapt and continually be optimized

[1] See Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors OJ L 33, 6.2.1999, p.1 as amended by Decision No. 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 OJ L 162, 1.7.2003.

[2] See L. Woods and A. Scheuer, (2004) "Advertising Frequency and the Television Without Frontiers Directive", 29(3) *European Law Review* at 366–384, analysing in particular Case C-245/01 *RTL Television GmbH v. Niedersächsische Landesmedienanstalt für privaten Rundfunk*, judgment 23 October 2003, nyr (see http://curia.eu.int). See further in context, L. Woods, *Free Movement of Goods and Services* (Ashgate Publishing, 2004).

[3] Com (2001) 428 Final, European Governance – A White Paper, at p. 21, see <http://europa.eu.int/eurlex/en/com/cnc/2001/com2001_0428en01.pdf>

to maintain relevance and effectiveness in rapidly evolving markets. This is particularly evident in the media sector which is generally regarded as the engine for creating and exploiting content.

European debate[4] led to a co-regulatory Recommendation in 1998 that continues to serve as the Commission's policy towards content regulation.[5] Further Commission legal instruments, including the E-Commerce Directive of 2000, have maintained the co-regulatory approach to new media regulation laid out in the 1998 Recommendation.[6] The European Commission expresses some of the pitfalls of new media consumption compared with traditional means: "Whereas in traditional broadcasting (analogue or digital) the individual broadcaster is easily identifiable, it is difficult and sometimes impossible to identify the source of content on the Internet. Access to harmful and illegal content is easy and can even occur without intent. In addition, the volume of information in the Internet is massive in comparison to broadcasting."[7] End-user tools such as filtering or the famous "V-chip", imposing rules on children's use of computer games and the World Wide Web, and reporting inappropriate or illegal content to hotlines established by Internet companies have had only limited success.

There are markets for regional and/or national television, radio, newspapers, telecoms, satellite and cable pay TV, all recognized in case law.[8] The use of data compression and increases in cost-effective bandwidth such as Digital Subscriber Lines (DSL) allow more and better point-to-point delivery.[9] In this environment flexibility of regulatory frameworks will be of paramount importance to ensure that regulators meet the current and future needs of the marketplace and maintain the confidence of consumers through the protection of public interests. Commission consultations have shown that a wide range of co-regulatory and self-regulatory approaches have been used within the Member States, particularly in areas such as advertising and protection of minors. However, such is the dynamic development of the sector and its regulatory landscape, that there remains insufficient clarity as to the nature of the co-regulatory/self-regulatory approaches taken, the areas within the media sector where they are applied, their consistency with public interest objectives, their impact on fragmentation of the single market and ultimately, their effectiveness in achieving the intended regulatory objectives.

[4] See European Commission (1996) Green Paper on the protection of minors and human dignity in audiovisual and information services on 16 October 1996; Council resolution on illegal and harmful content on the Internet of 17 February 1997 OJ C 70, 6.3.1997; Economic and Social Committee Opinion OJ C 214, 10.7.1998; European Parliament Opinion OJ C 339, 10.11.1997; Economic and Social Committee Opinion OJ C 287, 22.9.1997; Committee of the Regions Opinion OJ C 215, 16.7.1997.

[5] Green Paper on the protection of minors and human dignity in audiovisual and information services, COM (96) 483, 16.10.97; Communication on Illegal and Harmful content on the Internet, COM(97) 487, 16.10.97; Council Recommendation 98/560/EC on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity OJ L 270, 7.10.1998.

[6] See further Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications OJ L 201, 31.7.2002; Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L 178, 17.7.2000.

[7] See Second Evaluation Report From The Commission To The Council And The European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity COM(2003) 776 final of 12 December at <http://europa.eu.int/comm/avpolicy/legis/reports/com2003_776final_en.pdf> at 6.

[8] See A. Harcourt, (1998) "Regulation of European Media Markets: Approaches of the European Court of Justice and the Commission's Merger Task Force", 9 *Utilities Law Review* 6 at 276–291; P. Larouche, (1998) EC Competition law and the convergence of the telecommunications and broadcasting sectors 22 Telecommunications Policy 3.

[9] See C. Marsden, "Video over IP: the challenges of standardization – towards the next generation Internet", [2003] chapter 8 in Eli M. Noam, Jo Groebel and Darcy Gerbarg (eds.), *Internet Television*; C. Marsden, "The Start of End-to-End? Internet Protocol Television" [2001] 29 *Intermedia* at 4–8.

2. Theoretical and Methodical Framework – What is Co-regulation?

The European Commission has readdressed co-regulation of the media in 2004[10]:

> The Recommendation on the protection of minors has a **cross-media approach** and emphasises the **cross-border exchange of best practices** and the development of **co-regulatory and self-regulatory mechanisms.** (emphasis in original)

It explains how best to achieve the regulatory goals:

> A co-regulatory approach may be more flexible, adaptable and effective than straightforward regulation and legislation. With regard to the protection of minors, where many sensibilities have to be taken into account, co-regulation can often better achieve the given aims. Co-regulation implies however, from the Commission's point of view, an appropriate level of involvement by the public authorities.

Co-regulation expresses a dialogue process between stakeholders, which results in a form of regulation which is neither state command-and-control regulation in its bureaucratic central or IRA (Independent Regulatory Agency) specialized functions[11], but is also not "pure" self-regulation as observed in industry-led standard setting in Internet infrastructure.[12] The State and stakeholder groups, including consumers, form part of the institutional setting for regulation. Co-regulation constitutes multiple stakeholders, and this inclusiveness results in greater legitimacy for claims. However, direct government involvement including sanctioning powers may result in the gains of reflexive regulation – speed of response, dynamism, international co-operation between ISPs and others – being lost. It is clearly a finely balanced concept, a middle way between state regulation and "pure" industry self-regulation.

Craig cautions that:

> Regulation is often informal, characterized by negotiation, persuasion and cajoling ... The potential economic advantage of informal regulation in achieving a cost-effective level of regulation must be weighed against the danger of regulation becoming *ad hoc* and circumventing procedural safeguards in legislation.[13]

An economist's notion of regulation "in its widest conception is state intervention in the economic decisions of companies."[14] A broader sociological definition "considers all mechanisms of social control" to be forms of regulation, which encompasses self-regulatory models, the role of firms and social norms. This enables the consideration of non-legal norms, and the interaction of firm, civil society and State. Ayres and Braithwaite state[15]:

> by working more creatively with the interplay between private and public regulation, government and citizens

[10] European Commission (2004) Second Evaluation Report, ibid. It continues: "It should consist of cooperation between the public authorities, industry and the other interested parties, such as consumers. This is the approach laid out in the Recommendation. In order to promote national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, the Recommendation enumerates different objectives to be fulfilled by (i) the Member States, (ii) the industries and parties concerned and (iii) the Commission."

[11] R. Baldwin et al., (1998) *Socio-Legal Reader on Regulation*, at 3 explain that "At its simplest, regulation refers to the promulgation of an authoritative set of rules, accompanied by some mechanism, typically a public agency, for monitoring and promoting compliance with these rules." They explain that recent regulatory design has generally separated rule-making from enforcement/monitoring activities, the former remaining in parliamentary competence, the latter delegated to IRAs.

[12] See a summary of de Cockborne's Montreux speech in Adam Watson Brown (1999), Industry Consortia and the Changing Roles of Standards Bodies and Regulators, 35 Inst. Prospective Tech. Stud., June 1999, available at <http://www.jrc.es/pages/f-report.en.html>

[13] P.P. Craig at 197 in R. Baldwin and C. McCrudden, (1987) *Regulation and Public Law*.

[14] C.D. Foster, *Privatization, Public Ownership and the Regulation of Natural Monopoly* (Oxford: Blackwell, 1992), 186.

[15] Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: Oxford University Press, 1992), 4.

> can design better policy solutions ... administrative and regulatory practice is in a state of flux in which responsive regulatory innovations are politically feasible.

Responsive regulation reflects a more complex, dynamic interaction of state and market, a break with more stable previous arrangements.[16] This applies to other globalizing phenomena than digital TV and the Internet, for instance financial and environmental law[17], where initial European public reaction to the Internet resembled that associated with environmental pollution.[18] In advertising protection of minors and consideration of broadcast regulation's extension to new media including the Internet and 3G/UMTS mobile phones[19], co-regulation is a vitally important concept.

A common understanding of the concept of co-regulation, its importance for regulators, and the perspective with which to assess its impact are among the most important threshold issues to address, before it is possible to consider specific regulatory responses.[20] The difference with the Internet is that government regulation has only taken place in special circumstances, with co-regulation being the norm. Price and Verhulst assert the limits of both government and private action in this sphere, and affirm the interdependence of both – there is little purity in self-regulation without at least a lurking government threat to intervene where market actors prove unable to agree. They draw on regulatory theory and empirical studies of advertising and newspaper regulation, demonstrating that in areas of speech, the Internet included, government preference in liberal democracies is for self-regulation.[21] Ayres and Braithwaite state: "Practical people who are concerned with outcomes seek to understand the intricacies of interplays between state regulation and private orderings." [22]

The term "co-regulation" encompasses a range of different regulatory phenomena, a complex interaction of general legislation and a self-regulatory body. The following table illustrates the range of possible co-regulatory architectures, and therefore the potential complexity involved.

Table: Possible Co-regulatory Architectures

Example of code	**Demand for code from**	**Code drafters**	**Code enforcers**	**Sanctions**
Video Standards Council (UK)	Industry/ public	Industry with public representation	Industry board with public involvement	Civil penalties for improper video rental
ICSTIS – UK Independent Committee for Standards in Telephony and Information Services	Industry/ public	Industry	Industry/public board with recourse to Ofcom	Fines, with backup powers via Ofcom to telecoms providers
Italian Internet Service Providers Association	Industry/ Government	Government	Industry	Industry (exclusion from industry association)

[16] G. Teubner, "The Transformation of Law in the Welfare State", in G. Teubner (ed.), *Dilemmas of Law in the Welfare State* (Berlin: W. de Gruyter, 1986), at 8: European conceptions of law as "moving away from the idea of direct societal guidance through a politically instrumentalised law … Instead, reflexive law tends to rely on procedural norms that regulate processes, organisation, and the distribution of rights and competencies."

[17] See for instance Sanford E. Gaines and Cliona Kimber, (2001) Redirecting Self-Regulation Env. Law 13(157).

[18] See Phillip Whitehead, (1997) Draft Report on the Commission Green Paper on The Protection of Minors and Human Dignity in Audiovisual and Information Services (COM[96]0483 - C4-0621/96) PE 221.804 of 24 April 1997.

[19] C. Ahlert, M. Alexander, and D. Tambini, (2003) European 3G Mobile Industry Self-Regulation, IAPCODE Background Paper for World Telemedia Conference at 2: <http://www.selfregulation.info/iapcoda/031106-mobiles-revised-bckgrd.pdf>

[20] See also Goldberg, Prosser and Verhulst, *Regulating the Changing Media* (Oxford: Clarendon Press, 1998).

[21] Price, Monroe and Stefaan Verhulst, (2000) "In search of the self: charting the course of self-regulation on the Internet in a global environment", chapter 3 in C. Marsden (ed.), *Regulating the Global Information Society*; M. Price, *Television, The Public Sphere and National Identity* (Oxford: Oxford University Press, 1995).

[22] Ian and John Braithwaite, (1992) *Responsive Regulation: Transcending the Deregulation Debate* at 3.

In analysing various media sectors, it is vital to recognize the different points at which some form of regulation is necessary, both for content and for economic protection of the consumer. The varying interests of actors result in different incentives to co-operate or attempt unilateral actions at the various points of the value chain. Without sensible analysis of the sectors from film to video to cable, satellite and terrestrial television, to distribution over broadband and mobile phones, it is impossible to rationally assess actors' individual motives and therefore their incentives to pursue regulatory options of various types. Without regulation responsive to both the single European market[23] and the need for constitutional protection of freedom of expression and protection of minors at national levels, co- and self-regulatory measures cannot be sufficiently responsive to economic and cultural environments to be self-sustaining.

3. What can we learn from existing studies in analysing co-regulation?

3.1. Regulated Self-regulation and European Concepts of Co-regulation

There have been many studies of self- and co-regulation in the media sector in the past 15 years since Boddewyn's pioneering 1988 study of advertising[24], notably those of PCMLP[25]; of PCMLP faculty and associates, both independently[26] and with collaborators[27]; of Braithwaite and collaborators in Australia and the United States[28]; and of others[29], with shorter country- or sector-specific contributions[30].

Schulz and Held have investigated co-regulation in the German context, specifically in the case of protection of minors.[31] In their view, self-regulation in Anglo-American debate is concerned with "reconciliation of private interests" whereas their formulation – regulated self-regulation[32] – is indirect state regulation based on constitutional principles. It is the combination of "intentional self-regulation" – the actions of market actors, whether in social or economic settings – with the state

[23] A communitaire legal justification for national application of EC competition law under the Treaty of Rome is provided in J. Temple-Lang, (1998) "The Duty of National Authorities under Community Constitutional Law" 23 *European Law Review* 109 at 119.

[24] J. J. Boddewyn, (1988) *Advertising Self-regulation and Outside Participation*. See also Lee C. Bollinger, (1976) "Freedom of the Press and Public Access: Toward a Theory of Partial Regulation", 75 *Michigan Law Review* 1.

[25] (www.selfregulation.info) PCMLP has conducted three surveys into self-regulation and co-regulation of the media for the Commission, for DG Media Culture and for DG Information Society:
(undated, 1999) Parental Control of Television Broadcasting, A Report;
2000: Internet Codes of Conduct: An Analytic Report on Current Developments
2004: Self-Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis.

[26] M. Price and S. Verhulst, (2004) *Self-Regulation and the Internet*; Pierre Larouche (2001) "Communications convergence and public service broadcasting", at <http://infolab.kub.nl/uvtweb/bin.php3?id=00011353&mime=application/pdf&file=/tilec/publications/larouche2.pdf>

[27] C. Marsden (ed.), (2001) *Regulating the Global Information Society*; C. Marsden and S. Verhulst (eds.) *Convergence in European Digital TV Regulation* (1999). See also Peter J. Humphreys, (1996) *Mass media and media policy in Western Europe*; A. Harcourt, (2004) *European Institutions and Regulation of the Media Industry*.

[28] Ian Ayres and John Braithwaite, (1992) *Responsive Regulation: Transcending the Deregulation Debate*; Braithwaite and P. Drahos, (2000) *Global Business Regulation*, both contextualizing media co-regulation within the broader regulatory debate. On broader debates, see R. Baldwin, C. Scott, and C. Hood, (1998) *A Reader on Regulation*.

[29] C. Marsden, (1999) Pluralism In The Multi-Channel Market: Suggestions For Regulatory Scrutiny, Council of Europe Human Rights Commission, Mass Media Directorate, MM-S-PL [99] 12 Def 2.

[30] See special issues of IRIS in 2002-3, notably IRIS Special (2003) *Co-Regulation of the Media in Europe*, Strasbourg, Council of Europe at <http://www.obs.coe.int/oea_publ/iris_special/2003.html.en>; M. Benassi, "New Self-Regulatory Code of Conduct on Television and Minors", IRIS 2003-4:10/21; Andrea Schneider, "Child Protection on German Television – The Voluntary Television Review Body (FSF)", IRIS 1995-3:7/13; M. Capello, "Comparative Advertising Allowed by the Self-regulatory Advertising Code", IRIS 1999-6: 13/25; K. Mastowska, "Television Self-Regulation", IRIS 1999-5:13/16

[31] Schulz and Held, (2001) *Regulated Self-Regulation as a Form of Modern Government.*

[32] See Wolfgang Hoffman Reim, (1996) *Regulating Media*.

sanction in reserve which results in self-regulation which is "regulated" by the possibility of state intervention. At the Birmingham "Audiovisual Assizes" in 1998, the formulation used was: "Self-regulation that fits in with a legal framework or has a basis laid down in law".[33]

The term "co-regulation" also gives a sense of the joint responsibilities of market actors and the State, short of outright command-and-control, in the activity under investigation. It has been used by the UK's telecom regulator to suggest a state role in setting objectives which market actors must then organize to achieve – with the threat of statutory powers invoked in the absence of market self-regulation.[34] However, co-regulation is used in such a wide variety of circumstances that its specific meaning must be seen in the national, sectoral and temporal context in which it is used.[35]

Schulz and Held suggest that "regulated self-regulation" can be any of these categories: co-regulation, intentional self-regulation, or a third category – "audited self-regulation". Independent audit of self-regulation is a US concept of using an independent standard or professional body to audit a self-regulatory organization or individual company according to preset standards. In the case of ISPs, audited self-regulation might involve a standard being set against which an audit firm could certify organizations (or at least that organizations could self-certify reporting requirements), but could involve the setting of an international standard, as increasingly occurs in accountancy, for instance. At a minimum, dedicated budgetary and personnel resources, with activity reports, would be required to demonstrate regulatory commitment. The German concept of regulated self-regulation gives the State a role when basic constitutional rights need to be upheld: "The extent of possible delegation [to self-regulation] depends … on the relevance … in terms of basic rights".[36]

3.2. A Typology of Co-regulation

Co-regulation in the European context must also be proportional to the aims of the legal instrument, as well as conforming to the competition law of the European Union. Enforcement is the ultimate responsibility ("the safety net") of the State. In Schulz and Held's case study, Australia, practical self-regulation is illustrated in the application of the 1997 Telecoms Act and 1992 Broadcasting Services Act, where four types of regulatory scheme can be identified.[37]

Regulatory type	**State role**
1. Intentional or "pure" self-regulation	No state IRA involvement
2. Industry codes	Registered with the state IRA
3. Industry standards	Mandatory codes set in the absence of pan-industry code agreement
4. Command-and-control	Set by state IRA pre-empting attempts at self-regulatory action

The vital lessons from co-regulatory studies, upon which the final www.selfregulation.info report draws, are several:

- Consistency of methodology is vital for comparative data capture to be accurate, between sectors as well as national examples.

[33] See typologies and quotation at 7 in Schulz and Held supra n.35.

[34] See Richard Thomas's report to the National Consumer Council (UK) "Better business practice: how to make self-regulation work for consumers and business" at <http://www.ncc.org.uk/pubs/pdf/self-regulation_gpg.pdf> and OFCOM (2004) Consultation Document "Criteria for Transferring Functions to co-Regulatory Bodies" <http://www.ofcom.org.uk/consultations/past/co-reg/?a=87101>

[35] Schulz and Held detail different meanings used in the UK, Australia and France, at 7,14, supra n.35.

[36] Schulz and Held (2001) at 8, supra n.35.

[37] See J. Reidenberg, (2004) States and Law Enforcement, 1 Uni.Ottawa L.& Tech.J. summarizing J. Reidenberg, (2002) Yahoo and democracy on the Internet, 42 Jurimetrics 261.

- Iterating and modifying the template can only be conducted prior to the study, by taking test cases to pilot the methodology.
- Co-regulation is a moving target – the national and sectoral templates for co-regulation have to be modified following each survey in order to encompass the different and dynamic practices of co-regulation in each geography and sector examined.
- It is essential in surveys to conduct field research in as short a time as possible, for the reasons outlined above.

4. Does co-regulation deliver the expected results?

As outlined above, the PCMLP project has conducted research in the 15 pre-2004 Member States in the following areas: broadcast co- and self-regulation; mobile telephony and child protection; Internet self-regulation; computer games and video cassette ratings schema; print news media self-regulation. Based on the www.selfregulation.info report and other prior work, we can offer some tentative initial hypotheses. PCMLP refers to its conclusions, final chapter and executive summary for the IAPCODE project, which contain detailed options for co-regulation in the media including specifications for regulatory audit. Three options suggest themselves:

1. Adopting best practice in self-regulatory approaches taken from US and possibly UK models;
2. Developing and extending a sophisticated version of co-regulation such as that found in Australia or Germany, with a pan-sectoral focus;
3. Extending practice to a pan-European role, as in the Internet sector, where INHOPE, EuroISPA or ISFE have adopted a successful model (for details see main IAPCODE report).

However, the role of free speech, cultural diversity and the enforceability of such regimes remain problematic.

These three options are in addition to nation-specific and sector-specific status quo options, which one might term Option 0.

In considering the range of self-regulatory solutions across Europe, it is necessary to reflect on exactly why there is a range of responses, and whether it is possible to conceive of a European model of media self-regulation:

- What is the most important national factor with regard to self-regulation, and what are the barriers to international co-operation?
- Is it legal and constitutional and the implications for self-regulation or rather the differences in cultural content standards?
- Is it rather a more complex set of factors relating to institutional political economy?

To place our media self-regulation survey in the context of country-level differences and EU-wide changes that impact on Member States in contrasting ways, the level of analysis must be useful for:

- Understanding self-regulation on the national level;
- For policymaking that is concerned with co-ordinating national media approaches across sectors, and
- For evaluating prospects for convergence in practices on the EU level.

Our approach also entails difficulties in assessing changing political cultures. Cultural as well as economically rational motivations differentiate state and market actors. Pan-European options present further complexity: multilateral solutions may therefore be theoretical solutions to intractable real-world problems. Yet, when self-regulation is put into practice this is often first done on the national level, and here attention to economic governance, political culture, civil society and institutions in general may make a crucial distinction in assessing which self-regulatory schemes succeed and which fail.

Codes of conduct, in order to be legitimate, credible, transparent and effective need to include clear and workable procedures for review and amendment of the code. Ideally this should include some input from the adjudication body. The most effective and skilled code operators take the following issues into account when revising their codes:

- The convergence of national, regulatory and corporate cultures;
- The changing nature of the relationship between government and industry;
- The evolving technological architecture that underwrites self-regulation;
- The further development of standards, codes, and rules;
- The growth and change of cultural norms and of public understanding surrounding self-regulation; and
- Third party consultation or audit.

5. Recommendations from the IAPCODE Study

Our recommendations can help the effective development of media codes of conduct and co-regulation of Internet content in specific ways. Our key finding is that technological progress brings about change and that self-regulation can respond more rapidly and efficiently than state regulation. There is no universally acceptable recipe for successful self-regulation, as regimes must be adjusted to the needs of each sector and different circumstances (technological changes, changes in policy in response, a country's legal system, case law of European courts, and so on). To illustrate, broadcasting is an area in which technological progress resulted in complexity and the increase of self-regulation responds in part to policy changes prompted by those technological changes. The European monopolistic broadcasting model which developed with radio, and was maintained for television, was first challenged by commercial terrestrial services. Further pluralism brought about first by cable and satellite, and then digital technologies including the Internet, forced changes in the regulatory environment and public authorities increasingly delegated the power to regulate to market actors. The trend is towards continued delegation (with regulatory authority audit of the resources, procedures, transparency, stakeholder participation and market effect of the self-regulatory scheme).

Key Recommendation. Adequate resourcing is the key to successful self-regulation. Policy on self-regulation must take into account a broader view of the sustainability, effectiveness and impact on free speech of self-regulatory codes and institutions. We recommend applying an auditing procedure for establishing self-regulatory institutions and codes. Notwithstanding the centrality of speech freedoms in constitutions, we hold that this regulatory audit burden is a minimal price to pay for effective self-regulation in the public interest.

Convergence, the Single Market and Future Trends in Co-regulation. Significant economies of scale are likely to be realized through functional integration of certain key aspects of the content regulation value chain horizontally across sectors and across EU Member States. The rating of computer games has illustrated the potential for developing a common pan-European ratings structure. Germany and the Netherlands operate a cross-media rating and labelling scheme. In a situation of increasing cross border trade within the EU, this trend is set to continue. An important use of the Internet is to access news. Journalistic ethics online, often an extension of systems developed for the print media over decades, has the potential for a pan-European structure. Online news services, online versions of newspapers, news aggregators, as well as self-regulatory mechanisms to which they may belong could soon acquire relevance beyond national borders. Readership may start seeking access to self-regulatory bodies and complaint mechanisms located outside national jurisdictions.

Although the *legislative* role of the European institutions is currently limited (prior to any EU constitutional settlement), several recommendations have been made as cited below. And it is likely that in a single market context, there will be significant self-interest on the part of industry in self-regulation. More research and development, benchmarking and technical assistance in disseminating best practice between Member States is clearly essential to assist industry bodies in the exploitation of economies of scale and scope in self-regulation across the various converging media sectors in the single market, and to ensure greater effectiveness of self-regulation.

The general trend is towards an expansion of scope of co-regulation, often at the expense of statutory regulation. Many IRAs are exploring the possibility of "sunsetting" particular regulations in the event that co-regulatory alternatives can be found.

Funding and Sustainability of Media Co-regulatory Regimes. Where there is a clear industry interest in self-regulation to improve market penetration, or to head off threats of statutory regulation, there are adequate market incentives for resources to be allocated to self-regulatory activities. However, the enlightened self interest required is vulnerable to changing personnel and market structures. Self-regulatory institutions, where they do not have access to compulsory funding, will not enjoy the funding necessary to meet standards of transparency, accountability and due process.

A wide variety of models of self-regulatory tools exist. Some of these are based on adequate standards of transparency, inclusion, due process, resources and so forth, and some clearly are not. As a result there is some concern with the development of codes that insufficient standards apply to both law enforcement/child protection and protection of freedom of expression rights. If these mechanisms are improperly structured we can expect public harm to result in the medium term. The European Commission and Council of Europe should develop and publish clear benchmarks for acceptable levels of transparency, accountability and due process and appeal, particularly with regard to communications regulation that may impact upon freedom of expression. Self-regulatory institutions should follow the guidelines for transparency and access to information that are followed by public and government bodies according to international best practice. At the very least self-regulators should provide summaries of complaints by clause of code of conduct, numbers of adjudications, and findings of adjudications on their website. Failure to conform to these baseline standards of transparency should be viewed as a failure of self-regulation.

Co-regulation and Freedom of Expression. Self-regulation has an ambivalent and tense relationship with fundamental rights to freedom of expression. At one level this depends on definitions. In some cases, and particularly in the US, case law tends to favour a view of freedom of expression as a negative right: i.e. it exists where there is an absence of state interference with communication. In other traditions, freedom of expression is equally endangered by private bodies such as corporations. In the former case, self-regulation is likely to be viewed favourably in terms of its impact on freedom of expression because, by definition, freedom of expression is not endangered by non-state entities. However, this does not mean that positive rights to free speech are protected by self-regulatory institutions. On the contrary, because self-regulatory institutions are not public bodies they may be less accountable. Self-regulation could be used instead of government regulation to avoid constitutional free speech issues when regulating more stringently: for example, broadcasting pre-publication control as carried out by the *Freiwillige Selbstkontrolle Fernsehen (FSF)* in Germany and similar bodies in other countries. Self-regulation offers a complaints procedure and alternative dispute resolution. However, there may be less protection for rights than with the protection offered by the law. For example, injunctions, fines and sanctions may be unavailable within a self-regulatory regime. Similarly victims may not be able to access financial compensation if complaints are resolved by self-regulation rather than in court.

Stakeholder Participation in Co-regulation. A key lesson is that it is essential to achieve a balance between industry representatives and non-industry members on boards. This combination strengthens its legitimacy. This, in turn, may lead to a virtuous circle in which the enlightened self-interest of the industry can help the media to willingly fund the mechanism of code implementation, and abide by decisions. Industry professionals should constitute a minority on boards of content self-regulatory bodies. Measures should be adopted to ensure that bodies that are 100 per cent funded by their industry are not captured by it. These measures could include: fixed tenure for board members, dismantling separate “funding boards” (who may attempt to hold regulatory boards to ransom), replacing them with a compulsory levy on industry participants, as currently applies to premium telephony in for instance the UK. This transparent and guaranteed funding then permits industry participants to play a much greater expert role in advising the regulator, with less conflict of interest. Despite recent progress, consumer groups often lack the technical and legal knowledge of the application of media self-regulation to the Internet, especially in new capabilities of mobile and broadband.

Internet Co-regulation. The following twelve recommendations are directed to those public and private institutions engaged in Internet regulation. The response to the extensive surveys conducted by IAPCODE has been exceptionally meagre, demonstrating a lack of resources devoted to self-regulation within Internet service providers. In part, this may be because self-regulation in the sector is of such recent vintage compared to the other sectors studied. We recommend a significant role in inculcating a regulatory culture by the IRAs in each country. The several countries conforming to best practice may find the co-regulatory audit concept, in particular, a relatively low hurdle to cross. Nevertheless, we believe that co-regulation will encourage publicity for those best practice schemes, and therefore better public awareness of their work. For the other under-resourced market actors and their schemes, co-regulatory audit will act as a much-needed reality check on the resources required for effective self-regulation in sectors where freedom of speech concerns are so critical. We begin with four recommendations on strengthening the relationship between industry self-regulatory codes and user-based solutions: holistic thinking and media literacy, filtering, hotlines and trustmark accreditation.

Inappropriate and harmful content is becoming a massive problem – unsolicited adult content is part of a larger content category including unsolicited commercial communication (spam) and unsolicited code (including malicious code – viruses and spyware). It threatens trust in the medium as a whole, including e-commerce and even e-mail. Legislation is dealing with some of these issues, such as spam. Self-regulation arrangements should take account of these new initiatives and any changes to their role that may result. There is insufficient "joined up" thinking at national and regional level about the interrelationship between different layers of the Internet: content, physical and software protocols. We cannot regulate adult content alone without consideration for other content type regulation, such as spam blocking, and their effect on other layers.

Filtering and Hotlines. Where filtering rules and self-regulatory hotlines have been instituted, there has been a heroic assumption that users will install technical solutions and be aware of hotlines, and that the 10 billion web pages will be self-classified or policed effectively. This is becoming increasingly unlikely. Technical enthusiasts or global user communities without real self-interest cannot achieve the co-ordination necessary. Future studies of filters and hotlines should continue to focus not only on the technical capabilities of filtering technology or police co-operation, but also on the skills of users, parents, children and others and awareness of these technologies.

End-user software, for instance filters and search engines, raise significant problems for freedom of expression. For example, popular search engines may have rules for search that prioritize content inappropriately for specific cultures: by language, content type or software format. It is essential that studies of filters be instituted that examine the freedom of speech implications of commercial ranking of sites, pages, content types, languages. ISP or portal judgements of speech freedoms must be subjected to national law.

Notice and Take Down: "Put Back" in the E-Commerce Directive. The opacity of self-regulatory regimes is also a cause for concern in the Notice and Take Down regime for ISPs. Where an ISP substitutes its own judgement of harmful or potentially illegal content, with or without trained legal advice, it does so "in the shadow of the law". This privatized enforcement of freedom of expression is a continued cause for concern. Where there is even a suspicion that Notice and Takedown procedures are not being adhered to, the legitimacy of self-regulation and the ISP industry suffers. Presently ISPs appear to be substituting their view of illegal, harmful (and copyright infringing) content without effective legal procedures for content producers to respond and appeal. This is a direct infringement of freedom of expression on the Internet, which is unchecked by current legislation. We recommend that "put back" be seriously considered as a policy option when the E-commerce Directive is reviewed.

Co-regulation: Resource Audit Role of IRAs. Generally, there is a lack of credibility in Internet co-regulatory forums. This is in part due to lack of technical and regulatory expertise, but also due to insufficient co-operation in the industry. It is particularly difficult for regulatory staff in smaller and medium-sized media businesses to make the internal business case to release resource, especially legal resource, for self-regulatory solutions. ISPs often do not have the resources necessary to meet high standards of transparency, accountability and due process in self-regulation. Decisions to take part in self-regulatory schemes are often taken without sufficient knowledge of the longer term cost implications.

- **Industry** must take active part in co-regulatory initiatives. Whereas large multinationals (such as Microsoft, AOL, and ISP subsidiaries of national telcos) and voluntary actors (typically from research or educational backgrounds) are active participants, proactive measures need to be taken to fully engage with user groups, and smaller for-profit content and access providers.

- **IRAs** should convene a **co-regulatory forum** on a quarterly basis located at their offices, with minutes and participants published on the IRA website. This will introduce much-needed transparency into the co-regulatory process, to ensure all commercial operators take content co-regulation seriously. Effective co-regulatory schemes will find this no extra burden; indeed it will act as a stimulus for new members and be educational for the consumer.
- **Accrediting** co-regulatory codes of conduct and behaviour can only be carried out under the auspices of IRAs, who have the regulatory resource, stakeholder participation and competition law exclusion to effectively institute a voluntary kite-marking scheme. IRAs may choose to subcontract the scheme's functioning to a third party.
- **IRA audit** of self-regulatory activity, incorporating assessment of market structure and interests in self-regulation and an assessment of impact on fundamental rights, must take place within a dynamic and pragmatic framework which encourages rather than discourages self-regulatory activity where it is appropriate. We also recommend a "national resource audit of ISP and content sectors" – to answer essential questions of effective and sustainable ISP self-regulation:
  - Who is engaged in the Notice and Take Down regime?
  - What is the dedicated legal resource in each ISP?
  - Are the crucial code writing and adjudication functions sufficiently independent from industry?
  - Who performs the freedom of expression function in each ISP?

- Does the self-regulatory industry scheme, as well as individual ISPs, have sufficient resource “ringfenced” away from industry participant control, to operate efficiently, transparently and fairly?

6. Benchmarking and Research for a Forward-Looking Agenda

Accession States to the EU have substantial need of technical assistance in formulating co-regulatory schemes. Such assistance is needed in legislative and technical areas as much as in co-regulation itself. In particular, stakeholder/consumer groups require assistance in playing an effective role in co-regulatory discussions. The European Commission and OSCE are urged to establish expert groups in these areas. It is therefore suggested that a Technical Advisory Board be established for co-regulatory schemes, best practice and policy research. The TAB can take composition from national experts (in the manner of the moribund DGInfoSoc Legal Advisory Board). It requires an active secretariat and a willingness to consult at short notice where issues of content regulation arise. Its members must be appropriately qualified.

- The TAB would need to advise on achieving a progressive, forward-looking agenda, actively engaging industry and stakeholder interests (including technical stakeholders) through partnerships with, for instance, the spam forum now established by the OECD.
- Co-regulatory practice needs to take account of rapidly developing technologies and content types in [a] broadband; and [b] mobile Internet networks.
- The TAB would be required to engage with other advanced Internet stakeholders from East Asia, North America, and

from sectors including software, content and hardware developers. Without these inputs, its work would be limited in scale and scope to a regional and narrow view of the Internet

- The TAB would be required to pursue an active engagement with stakeholders from across the many media and communication sectors, and from multinational stakeholders active in European markets, as well as representatives from European media industries and other national and regional stakeholders.

Yaman Akdeniz

Who Watches the Watchmen? The Role of Filtering Software in Internet Content Regulation

Introduction. There have been many initiatives to deal specifically with the existence of illegal and harmful content over the Internet. These include an emphasis on self-regulation by the Internet industry with the creation of Internet hotlines for reporting illegal Internet content to assist law enforcement agencies, and the development of filtering and rating systems to deal with children's access to content which may be deemed harmful. These two issues are different in nature and should be addressed separately. Confusion between the two different problems seems to delay the appropriate policy initiatives to tackle them. But as far as the debate on "harmful content" is concerned, it should be stressed from the beginning that what may not be appropriate for children may certainly be legal for, and therefore accessible by, willing adults.

This paper will try to provide a broad overview of Internet content regulation and related policy initiatives and will argue that there is too much unwarranted anxiety about what is and what is not available over the Internet. Furthermore, the specific technical solutions offered within different forums for the availability of harmful Internet content may not be the right solutions to pursue as these can have serious consequences for freedom of speech in cyberspace.

Identifying the Problems. The decentralized nature of the Internet means that there is no unique solution for effective regulation at the national level. However, it would be wrong to dismiss the role that may be played by governments, especially in creating laws, maintaining the policing of the State and co-ordinating and aligning national policy with initiatives and policies at both supranational and international levels of Internet governance. Since October 1996, the European Commission has drawn a distinction between illegal and harmful content.[1] In its Communication on Illegal and Harmful Content on the Internet the Commission stated that:

> These different categories of content pose radically different issues of principle, and call for very different legal and technological responses. It would be dangerous to amalgamate separate issues such as children accessing pornographic content for adults, and adults accessing pornography about children.[2]

Although the Commission's Action Plan for the European Union for a safer use of the Internet[3] (which followed from the above-mentioned Communication paper) suggests that "harmful content needs to be treated differently from illegal content",[4] these categories have never been clearly defined by the Commission in its original Action Plan or by regulators elsewhere. The Action Plan states that illegal content is related to a wide variety of issues such as instructions on bomb-making (national security),[5] pornography (protection of minors),[6] incitement to racial hatred (protection of human dignity) and libel (protection of reputation). But none of these categories provided by the European Commission are necessarily "illegal content" and are not even considered "harmful content" (probably undefinable in a global context) by many European countries.

Illegal Content. It is wrong to consider the Internet a "lawless place"[7] and therefore the law of the land also applies to the Internet in theory. This is also true regarding the availability of illegal content over the Internet. The most common and most frequently cited example of illegal content is the availability of child pornography over the Internet.[8] Consequently, the whole issue of illegal content and how to deal with this

Child Pornography	**Hate Speech**	**Pornography**
• Society sees it as a problem. • Child pornography is not a new problem. • Digital child pornography is not a new problem – it can be traced back to the mid-1980s. • Clear cut example of "illegal content". • Criminalized by the CoE Cybercrime Convention, the UN Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, and the EU Council Framework Decision on combating the sexual exploitation of children and child pornography (not adopted yet). **• UN Optional Protocol: 108 signatories, 71 parties as of February 2004.**	• Society sees it as a problem. • Racism and xenophobia are not new problems. • Digital hate is not a new problem – it can be traced back to the mid-1980s. • Difficult to categorize: Depending upon its nature and the laws of a specific State it could be considered illegal or harmful/offensive (BUT legal). • Harm criteria are different in different European States. • CoE Additional Protocol to the Cybercrime Convention on the criminalisation of acts of a racist and xenophobic nature committed through computer systems: **23 signatories so far but no ratifications.** ¿	• Society does NOT always see it as a problem. • Pornography is certainly NOT new. • Difficult to categorize: Depending upon its nature and the laws of a specific State it could be considered illegal or harmful/offensive (BUT legal). • Harm criteria are different in different European States. • UK approach is rather different to the German or Scandinavian approaches to sexually explicit content. **• NO international attempt to regulate "sexually explicit content".**
Illegal ←——	————	——→ **Legal**

Table 1: Note that categorization of content is not straightforward and is often problematic.

[1] See European Commission Communication, Illegal and Harmful Content on the Internet, Com (96) 487, Brussels, 16 October 1996; and European Commission Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, Brussels, 16 October 1996.

[2] Ibid., p. 10.

[3] Decision No. /98/EC of the European Parliament and of the Council of adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, December 1998. See further C. Walker and Y. Akdeniz, "The governance of the Internet in Europe with special reference to illegal and harmful content", [1998] *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the Internet, 5–19.

[4] Ibid.

[5] Next stop is bookshops as a book named *Anarchist's Cookbook* is available through well-known bookshops such as Waterstone's and Dillons in the UK.

[6] See Y. Akdeniz, *Sex on the Net? The Dilemma of Policing Cyberspace* (Reading: South Street Press, 1999).

[7] See J.R. Reidenberg, "Governing Networks and Cyberspace Rule-Making", [1996] *Emory Law Journal* 45.

[8] See generally Y. Akdeniz, "Child Pornography", in Y. Akdeniz, C. Walker and D. Wall (eds.), *The Internet, Law and Society* (Addison Wesley Longman, 2000).

has revolved around child pornography, even though child pornography and paedophilia are not necessarily Internet-specific problems. Another concern for content-related criminal activity by law enforcement agencies is the possibility of using the Internet for harassment and threats. As Table 1 illustrates, it is not always easy to categorize certain types of content as illegal even though these may sometimes be regarded as objectionable or harmful.

It should also be noted that law enforcement bodies remain concerned about the incidental use of the Internet for existing crimes such as fraud,[9] and the emergence of specific cybercrimes[10] such as unauthorized access (hacking) to computer networks,[11] distribution of computer viruses such as the "ILOVEYOU" or the Melissa viruses,[12] and the denial-of-service attacks to computer networks. However, as these issues are not content-related they will not be discussed further in this paper.

Harmful Content. The difference between illegal and harmful content is that the former is criminalized by national laws, while the latter is considered offensive, objectionable, unwanted, or disgusting by some people but is generally not criminalized by national laws. Internet content that may be labelled "harmful" includes sexually explicit material, political opinions, religious beliefs, views on racial matters, and sexuality. But it should be noted that in the *Handyside*[13] case the European Court of Human Rights confirmed that freedom of expression extends not only to ideas and information generally regarded as inoffensive but even to those that might offend, shock, or disturb,[14] and this sort of information legally exists over the Internet as well as in other media.

The governance of this sort of Internet content may differ from country to country. This is certainly the case within

Europe where there are different approaches to sexually explicit content, hate speech, or Holocaust denial.[15] For example, under the Obscene Publications Act, in the UK it is illegal to publish and distribute obscene publications. Yet possessing or browsing through sexually explicit and obscene content on the Internet is not an illegal activity for consenting adults. Furthermore, there are no UK laws making it illegal for a child to view such content in a magazine or on the Internet. The laws normally deal with the provision of such content to children.

Therefore, harm is a criterion which depends upon cultural differences and this is accepted within the jurisprudence of the European Court of Human Rights.[16] Nevertheless, the availability of harmful Internet content is a politically sensitive area and a cause for concern for European regulators.

Approaches to Harmful Content. "Internet users are concerned about protecting children and vulnerable people from illegal or immoral material. A May 1999 survey of US parents showed

[9] See D. Davis, "Criminal Law and the Internet: The Investigator's Perspective", [1998] *Criminal Law Review*, December Special Edition, 48–61.

[10] See D. Wall, "Policing and the Regulation of the Internet", *Criminal Law Review*, December Special Edition (1998), 79–90.

[11] See Y. Akdeniz, "Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!", [1996] 3 *Web Journal of Current Legal Issues*.

[12] The Melissa virus first appeared on the Internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It is estimated that the virus caused $80 million in damages to computers worldwide. David Smith pleaded guilty on 9 December 1999 to state and federal charges associated with his creation of the Melissa virus. See *United States of America v. David Smith*, Criminal No. 99-18 U.S.C.§ 1030(a)(5)(A) information, United States District Court District of New Jersey.

[13] See *Handyside v. UK*, App. no. no. 5493/72, Ser A vol.24, (1976) 1 EHRR 737.

[14] See further *Castells v. Spain,* App. no.11798/85, Ser. A vol.236, (1992) 14 EHRR 445.

[15] See further Y. Akdeniz, "Case Review: League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v. Yahoo! Inc. (USA), Yahoo France", [2001] *Electronic Business Law Reports*, 1(3), 110–120 at <http://www.cyber-rights.org/documents/yahoo_ya.pdf>

[16] See for example *Handyside v. UK*, App. no. no. 5493/72, Ser A vol.24, (1976) 1 EHRR 737.

that 78% have concerns about the content of Internet material to which their children have access. … Control of content for consumers is thus a serious, and growing issue and a problem that must be solved."[17]

At a supranational level, the European Union Action Plan on the safer use of the Internet[18] encourages self-regulatory initiatives to deal with harmful content such as the creation of a European network of hotlines for Internet users to report illegal content like child pornography; the development of self-regulatory and content-monitoring schemes by access and content providers; and the development of internationally compatible and interoperable rating and filtering schemes to protect users. Furthermore, it advocates measures to increase awareness of available possibilities among parents, teachers, children and other consumers to help these groups to use the networks whilst choosing the appropriate content and exercising a reasonable amount of parental control.

Development of Rating and Filtering Systems. To deal with harmful Internet content, the European Union encourages the development of rating and filtering systems. Rating systems, such as the Platform for Internet Content Selections (PICS)[19], work by embedding electronic labels in web documents to vet their content before the computer displays them.[20] The vetting system could include political, religious, advertising or commercial topics. These can be added by the publisher of the material, or by a third party (e.g. by an ISP, or by an independent vetting body). Filtering software is also available and is intended to respond to the wishes of parents who are making decisions for their children. There are currently around 50 filtering products (mainly US-based),[21] and these do not necessarily reflect the cultural differences in a global environment such as the Internet. The type of harmful/offensive/disturbing/shocking/unwanted or undesirable content that is blocked by various filtering software usually include the following:

- Sexually explicit material
- Graphically violent material
- Content advocating hate
- Content advocating illegal activity, such as drug use, bomb-making, or underage drinking and gambling

In addition to these general categories, GetNetWise.Org identified tools that also limit access to information relating to abortion advocacy, advertising, alternative journals, art, lifestyles, humour, leisure activities, politics, religion and many others which would not be categorized or deemed either "harmful" or "offensive".[22] It is also difficult to categorize this content as "shocking"; in fact the only terms that could possibly apply are "unwanted" or "undesirable". There may well be parents out there who do not want their children to access art-related or humorous web pages or, for that matter, political websites such as that of George W. Bush.[23] But such categorization, and what is blocked as a result by producers of filtering software,

[17] Paragraph 10.13 of the Cabinet Office report *e-commerce@its.best.uk.*

[18] Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, December 1998.

[19] Note also the ICRA (Internet Content Rating Association) system which follows from the RSACi system. See <http://www.icra.org/> for further information.

[20] See Computer Professionals for Social Responsibility, "Filtering FAQ" <http://quark.cpsr.org/~harryh/faq.html>. Note that most filtering systems based on third-party rating, such as CyberPatrol, are compliant with the PICS labelling system.

[21] See <http://kids.getnetwise.org/tools/index.php>

[22] See <http://kids.getnetwise.org/tools/blockother>

[23] See BBC News, "Attack prompts Bush website block" 28 October 2004, at <http://news.bbc.co.uk/1/hi/technology/3961557.stm>

remains dubious. Even if parents do not want their children to access political websites, they will not know what other websites have been blocked by the product maker.

Yet self-rating and filtering systems are promoted as empowering user choice by the industry,[24] governments and international organizations. Bertelsmann Foundation's Memorandum in 1999 argued that "used wisely, this technology can help shift control of and responsibility for harmful content from governments, regulatory agencies, and supervisory bodies to individuals."[25] The memorandum urged that there should be an "independent organization to provide a basic vocabulary for rating and to oversee updates to the system at periodic intervals."

A Critique of Rating and Filtering Systems. It is important to show the whole picture concerning rating and filtering systems, including the limitations and criticisms about their use and development – aspects that are usually not considered by government representatives, the European Commission and industry bodies.[26]

> Originally promoted as technological alternatives that would prevent the enactment of national laws regulating Internet speech, filtering and rating systems have been shown to pose their own significant threats to free expression. When closely scrutinized, these systems should be viewed more realistically as fundamental architectural changes that may, in fact, facilitate the suppression of speech far more effectively than national laws alone ever could.[27]

It would seem that both rating and filtering systems are problematic. They do not appear to offer total protection to citizens or address content-related problems in full. They could be defective, and in many cases filtering software results in massive overblocking. At the same time some filtering software has been criticized for underblocking.[28] In general, there is too much reliance on mindless mechanical blocking through identification of key words and phrases. Moreover, this is usually based on the morality that an individual company/organization is committed to while developing their rating and/or filtering criteria and databases. So, broad and varying concepts of offensiveness, inappropriateness, or disagreement with the political viewpoint of the manufacturer are witnessed with such tools.

Limited Functionality. First of all, although various governments welcome the use and development of rating systems, the capacity of these tools is limited to certain parts of the Internet. But official statements offer no warning about these limitations.

Rating systems are designed for World Wide Web sites while leaving out other Internet-related communication systems such as chat environments,[29] file transfer protocol servers (ftp),[30] Usenet discussion groups, real-audio and real-video

[24] See the Bertelsmann Foundation's Memorandum on Internet Self-Regulation, September 1999, at <http://www.stiftung.bertelsmann.de/internetcontent/english/download/Memorandum.pdf>

[25] Ibid.

[26] See generally Electronic Privacy Information Center, *Filters and Freedom – Free Speech Perspectives on Internet Content Controls* (Washington DC: EPIC, September 1999). Please note that partly as a result of the writings contained in this collection, the headlong rush toward the development and acceptance of filtering and rating systems has slowed.

[27] See the Global Internet Liberty Campaign Statement submitted to the Internet Content Summit, Munich, Germany, September 1999.

[28] Websense, at some stage, published a daily list of sexually explicit websites on its own website to show the websites that its competitors did not block. However, anybody – including students from schools that were using SmartFilter and SurfControl – could access the list, simply by clicking a button on the Websense site agreeing that they were over 18. See Peacefire's report on Websense at <http://peacefire.org/censorware/WebSENSE/>

[29] Interactive environments like chat channels cannot be rated as the exchange and transmission of information takes place live and spontaneously.

[30] The estimated amount of ftp servers on the Internet is about a million. Some of these online libraries may have offensive content or legal content that may be considered harmful for children.

systems which can include live sound and image transmissions, and finally the ubiquitous e-mail communications. These cannot be rated with the systems that are currently available and therefore the assumption that rating systems would make the Internet a "safer environment" for children is wrong as WWW content represents only a fraction of the whole of the Internet. Although it may be argued that the World Wide Web represents the more fanciful and most rapidly growing side of the Internet, the problems that are thought to exist on the Internet by regulators are not specific to the World Wide Web.

Definitional and Categorization Problems. Secondly, even on the World Wide Web, where rating and filtering technology applies, it is not clear what the regulators have in mind regarding the sort of content that should be rated. Examples from official statements in which the category is referred to as "harmful", "immoral", "undesirable", "unwanted", or "objectionable" content have been provided above.

According to the UK Internet Watch Foundation, there is "a whole category of dangerous subjects" that require ratings and these relate to drugs, sex, violence, dangerous sports like bungee jumping, and hate speech.[31] This kind of content would certainly include such publications as *The Anarchist Cookbook*,[32] which can be downloaded from WWW sites but can also be obtained through ftp servers or automatic e-mail services, not to mention from well-known bookshops such as Waterstone's, Dillons and Amazon.co.uk in the UK.

Third Party Systems and Problems with Accountability. Thirdly, if the duty of rating were handed to third parties, this would cause problems for freedom of speech and with few third-party rating products currently available, the potential for arbitrary censorship increases. This would leave no scope for argument and dissent because the ratings would be done by private bodies without "direct" government involvement. When censorship is implemented by government threat in the background, but run by private parties, legal action is nearly impossible, accountability difficult, and the system is not open or democratic.[33]

Defective Systems. Fourthly, another downside of relying on such technologies is that these systems are defective[34] and in most cases they are used for the exclusion of socially useful websites and information.[35] It has been reported many times that filtering systems and software are over-inclusive and limit access and censor inconvenient websites, or filter potentially educational materials regarding AIDS, drug abuse prevention, or teenage pregnancy. The general excuse remains the protection of children from harmful content and also the duty of the industry to give more choices to the consumers. However, filtering software and rating systems are being used to exclude minority views and socially useful sites rather than to protect children.[36] According to the report on Internet Filters

[31] *Wired News*, "Europe Readies Net Content Ratings", 7 July 1997.

[32] William Powell, *The Anarchist Cookbook*, paperback reissue edition (Barricade Books, 1989).

[33] See generally Cyber-Rights & Cyber-Liberties (UK) Report, "Who Watches the Watchmen: Internet Content Rating Systems, and Privatised Censorship", November 1997 <http://www.cyber-rights.org/watchmen.htm> and Cyber-Rights & Cyber-Liberties (UK) Report: "Who Watches the Watchmen: Part II – Accountability & Effective Self-Regulation in the Information Age", September 1998 at <http://www.cyber-rights.org/watchmen-ii.htm>

[34] Electronic Privacy Information Center, "Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet", Washington, December 1997, at <http://www2.epic.org/reports/filter-report.html>

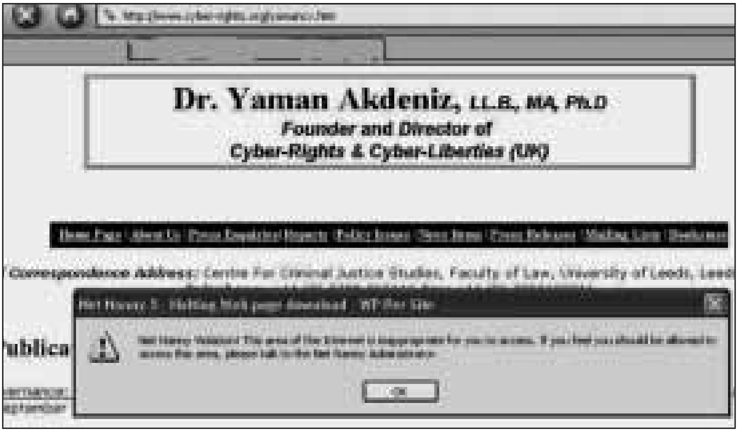
[35] See generally the PeaceFire.Org's pages at <http://www.peacefire.org> as well as Seth Finkelstein's excellent Anticensorware Investigations – Censorware Exposed pages at <http://sethf.com/anticensorware/>

[36] Gay & Lesbian Alliance Against Defamation report, "Access Denied: The Impact of Internet Filtering Software on the Lesbian and Gay Community", New York, December 1997, at <http://www.glaad.org/glaad/access_denied/index.html>

by the National Coalition Against Censorship:[37]

- I-Gear blocked an essay on "Indecency on the Internet: Lessons from the Art World", the United Nations report *HIV/AIDS: The Global Epidemic*, and the homepages of four photography galleries.
- Net Nanny, SurfWatch, Cybersitter, and BESS, among other products, blocked House Majority Leader Richard "Dick" Armey's official website upon detecting the word "dick".
- SmartFilter blocked the Declaration of Independence, Shakespeare's complete plays, *Moby Dick*, and *Marijuana: Facts for Teens*, a brochure published by the National Institute on Drug Abuse (a division of the National Institutes of Health).
- SurfWatch blocked human-rights sites like the Commissioner of the Council of the Baltic Sea States and Algeria Watch, as well as the University of Kansas's Archie R. Dykes Medical Library (upon detecting the word "dykes").
- X-Stop blocked the National Journal of Sexual Orientation Law, Carnegie Mellon University's Banned Books page, "Let's Have an Affair" catering company, and, through its "foul word" function, searches for *Bastard Out of Carolina* and "The Owl and the Pussy Cat".

Moreover, a recent test conducted by the author revealed that popular filtering software such as CyberSitter and NetNanny block the author's homepage at <http://www.cyber-rights.org> for the simple reason that the word "pornography" is used on the homepage of Cyber-Rights & Cyber-Liberties. CyberSitter logs revealed that the pages were filtered and therefore not accessible because the software categorized the pages under the categories of *childporn*, *pedophile*, and *pornsex*. NetNanny's approach was no different. Other pages on the same domain such as <http://www.cyber-rights.org/yamancv.htm> were, however, accessible. While CyberSitter provided no screen information when blocking <http://www.cyber-rights.org>, NetNanny displayed the following warning:



Dr. Yaman Akdeniz, LL.B, MA, Ph.D

Founder and Director of

Cyber-Rights & Cyber-Liberties (UK)

Correspondence Address: Centre For Criminal Justice Studies, Faculty of Law, University of Leeds, Leeds

Net Nanny Violation! This area of the Internet is inappropriate for you to access. If you feel you should be allowed to access this area, please talk to the Net Nanny Administrator.

Similarly, both CyberSitter and NetNanny did not provide any search hits for the words “teenage pregnancy” through Google but both failed to block the Google Ads provided on the same pages with the same words.[38]

In this way, rather than useful software, “censorware” enters homes under the guise of “parental control” and as a purported alternative to government censorship. But in fact such systems impose the standards of software developers rather than leaving the freedom of choice and browsing to the consumers who buy and rely on such products. Most of the companies creating this kind of software provide no appeal

[37] National Coalition Against Censorship, *Internet Filters: A Public Policy Research* (written by Marjorie Heins & Christina Cho, Free Expression Policy Project), Fall 2001, at <http://www.ncac.org/issues/internetfilters.html>

[38] Note the Henry J. Kaiser Family Foundation report, *See No Evil: How Internet Filters Affect the Search for Online Health Information*, December 2002, at <http://www.kaisernetwork.org/health_cast/uploaded_files/Internet_Filtering_exec_summ.pdf>

system[39] to content providers who are “banned or blocked”, thereby “subverting the self-regulating exchange of information that has been a hallmark of the Internet community.”[40] So these tools should never be subject to government mandated usage, or endorsement.[41]

Circumvention is Possible. Apart from the worrying defects explained above, circumvention of such tools is relatively easy. There is not only the often-cited example of children uninstalling or removing such software from their computers, but also a software exists called Circumventor, which beats the censors and makes any attempts to filter content seem futile. Circumventor was developed by Peacefire.Org’s Bennett Haselton and bypasses any content blocking attempts, including those by the likes of CyberSitter and NetNanny.[42]

One of the main motivations behind developing Circumventor was Peacefire.Org’s desire to bypass censorship of political websites. It is a well-known fact that almost all Internet users in China[43] and the Middle East[44] are blocked from accessing a considerable number of political websites. Technologies like Circumventor can help Internet users in censored countries to access such websites. In addition to Peacefire.Org’s Circumventor, websites providing anonymous proxy services and anonymous web surfing, such as anonymizer.com, can also be used to bypass filtering. It is, however, often the case that the filters block such well-known websites and proxy servers. That is why Peacefire.Org’s Circumventor, accessed through an unknown IP address (or known to a limited number of users), provides better success in circumvention and avoids possible unintended risks associated with circumvention technologies.[45]

Adults' Rights vs. Children's Rights. Fifthly, while children's access is the most-cited excuse for the regulation of the Internet, this global medium is not only accessed and used by children. In fact, it is not possible for children to have their own Internet accounts without the involvement of a parent or another adult as in almost all countries you need to be over 18 to open an account with an Internet service provider. Adults should act responsibly towards children's Internet usage rather than relying on technical solutions that do not fully address Internet content-related problems. Librarians[46] and teachers should also have a role to play when Internet access is provided for children by public libraries and schools.

Freedom of Expression & Censorship. Lastly, and more importantly, rating and filtering systems with blocking capabilities

[39] Some companies provide a review mechanism and others allow their databases to be searched online. But in most cases an online content provider would not know if its web pages are blocked by filtering software unless that software is tested by the content provider. Considering the number of such software, to find out whether a certain software blocks a particular website and why is an impossible task.

[40] See CPSR letter dated 18 December 1996 sent to Solid Oak, the makers of Cyber-Sitter at <http://www.cpsr.org/cpsr/nii/cyber-rights/>

[41] But a different approach was adopted in the USA. The Supreme Court held that Congress can give strong incentives to schools and libraries to use filtering software in *United States v. American Library Assn., Inc*, 539 US 194 (2003). According to the Supreme Court, Congress could also take steps to promote the development of filtering software by industry, and its use by parents.

[42] For further information about PeaceFire.Org's Circumventor, see <http://www.peacefire.org/circumventor/simple-circumventor-instructions.html>

[43] Note OpenNet Initiative report, Probing Chinese search engine filtering, August 2004, at <http://www.opennetinitiative.net/bulletins/005/>

[44] See generally the Documentation of Internet Filtering Worldwide pages of the Berkman Center for Internet & Society, Harvard Law School, at <http://cyber.law.harvard.edu/filtering/>

[45] See in detail the OpenNet Initiative report, *Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran*, May 2004, at <http://www.opennetinitiative.net/advisories/001/>

[46] Note E. Werby, The Cyber-Library: Legal and Policy Issues Facing Public Libraries in the High-Tech Era, National Coalition Against Censorship, 1999, at <http://www.ncac.org/issues/cyberlibrary.html>

allow repressive regimes to block Internet content (as mentioned above), or mandate the use of such tools.

> 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 rating protocol as voluntarily created and approved by private industry.[47]

Such a concern on the part of civil libertarians remains legitimate in the light of the Australian Broadcasting Services Amendment (Online Services) Act which mandates blocking of Internet content based upon existing national film and video classification guidelines.[48] So there is governmental support for mandatory rating systems and this is an option that may be considered not only by repressive regimes but also by democratic societies.

Any regulatory action intended to protect a certain group of people, such as children, should not take the form of an unconditional and universal prohibition on using the Internet to distribute content that is freely available to adults in other media. The US Supreme Court stated in *Reno v. ACLU*,[49] that "the Internet is not as 'invasive' as radio or television" and confirmed the finding of the US Court of Appeal that "communications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden." Still, filtering software were seen as preferable alternatives to government legislation at the Supreme Court level, and a similar line of argument was also raised at a later case in which the Supreme Court stated that "promoting filter use does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished."[50] It was argued that filters might well be more effective than certain legislation and impose selective restrictions on speech at the receiving end, not universal restrictions at the source. It was, however, acknowledged by the Supreme Court that "filtering software is not a perfect solution because it may block some materials not harmful to minors and fail to catch some that are."[51]

Problems associated with rating and filtering systems were also acknowledged at the European Union level. As the Economic and Social Committee of the European Commission pointed out in its report[52] on the European Commission's Action Plan on promoting safe use of the Internet, it is highly unlikely that the proposed measures will in the long term result in a safe Internet with the rating and classification of all information on the Internet being "impracticable".[53] More importantly, the Committee was worried that the possibility of Internet service providers using filtering and rating systems at the level of entry would render these systems, dubbed as "user empowering", an instrument of control, "actually taking choice out of citizens' hands." The Committee concluded that there is "little future in the active promotion of filtering systems based on rating."[54] But so far, promotion of such tools by the Internet

[47] See the GILC Statement submitted to the Internet Content Summit, Munich, Germany, September 1999.

[48] See generally <http://www.efa.org.au/Issues/Censor/cens1.html>

[49] *Reno v. ACLU*, 117 S. Ct. 2329 (1997).

[50] *Ashcroft, Attorney General v. American Civil Liberties Union et al.*, certiorari to the United States Court of Appeals for the Third Circuit, No. 03–218. Argued 2 March 2004 – Decided 29 June 2004, at <http://supct.law.cornell.edu/supct/html/03-218.ZS.html>. See further *ACLU v. Reno II*, No. 99–1324. For the full decision see <http://pacer.ca3.uscourts.gov:8080/C:/InetPub/ftproot/Opinions/991324.TXT>.

[51] Ibid.

[52] Economic and Social Committee of the European Commission, Opinion on the Proposal for a Council Decision adopting a Multiannual Community Action Plan on promoting safe use of the Internet (OJEC, 98/C 214/08, Brussels-Luxembourg, 10 July 1998), 29–32.

[53] Ibid. paragraph 4.1.

[54] See ibid. See further Y. Akdeniz, "The Regulation of Internet Content in Europe: Governmental Control versus Self-Responsibility", (1999) *Swiss Political Science Review* 5(2), summer, 123–31.

industry and by regulators within Europe and elsewhere continues, and the conclusions of the Economic and Social Committee were largely ignored by the European Commission while finalizing the Action Plan on safer use of the Internet.

Conclusion. This paper tried to provide an overview of self-regulatory initiatives that aim to tackle the problem of harmful Internet content. For both illegal and harmful Internet content, there is no unique solution for effective regulation; the emergence of "Internet governance" entails a more diverse and fragmented regulatory network that is not necessarily anchored primarily in nation-states.

The Internet is a great challenge for governance. Governance theorists are beginning to recognize that "objects of governance are only known through attempts to govern them"[55] and that "governance is not a choice between centralization and decentralization. It is about regulating relationships in complex systems."[56]

Therefore, a multilayered approach[57] is inevitable in which a mixture of public and private bodies will be involved in Internet governance, including individual Internet users for self-control as far as harmful Internet content is concerned. A multilayered approach will also go beyond the nation-state level to include layers at a supranational and international level of Internet governance. Yet at the same time, "if such mechanisms of international governance and re-regulation are to be initiated, then the role of nation states is pivotal."[58]

However, at a national level, it is now widely accepted that "government cannot simply regulate to achieve its aims in this new global electronic environment,"[59] and therefore a "light regulatory touch" is preferred in terms of the development of e-commerce. Although there has been much call for a partnership between government and industry "to get the right balance" in order to build confidence and protect consumers in the information age, that balance should reflect and respect the rights of individual Internet users, an issue often not considered by the regulators and by the industry. To achieve such a balance, which takes into account individual rights as well as the interests of the business community, there is an urgent need for openness, accountability and transparency in relation to regulatory initiatives[60] aimed at Internet content at the national level, rather than knee jerk reactions to such media-hyped coverage of cases like the Gary Glitter case.[61]

At a supranational (for example within the European Union) or international level (for example within the United Nations),[62] more co-operation will be witnessed between various police forces for Internet-related criminal activity. Interpol holds

[55] A. Hunt and G. Wickham, *Foucault and Law: Towards a Sociology of Law as Governance* (London: Pluto Press, 1994), 78.

[56] R.A.W. Rhodes, "The Hollowing Out of the State: The Changing Nature of the Public Services in Britain", (1994) *Political Quarterly*, 138–51, p. 151.

[57] Y. Akdeniz, "Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach", in L. Edwards and C. Waelde (eds.), *Law and the Internet: Regulating Cyberspace* (Hart Publishing, 1997), 223–41.

[58] P. Hirst and G. Thompson, "Globalization and the Future of the Nation State", *Economy and Society*, (1995) 24 (3), 408–42, p. 430.

[59] Per Tony Blair, foreward to the Cabinet Office Report, e-commerce@its.best.uk, September 1999.

[60] Note also the Cyber-Rights & Cyber-Liberties (UK) Response to Better Regulation Task Force Review of E-Commerce, 12 October 2000, at <http://www.cyber-rights.org/reports/brtf.htm>, and the Task Force's report, Regulating Cyberspace: better regulation for e-commerce, 14 December 2000, at <http://www.cabinet-office.gov.uk/regulation/taskforce/ecommerce/default.htm>

[61] See "Fury as Glitter gets only 4 months", *The Sun*, 13 November 1999.

[62] United Nations, Economic and Social Council, Commission on Human Rights, (Fifty-fourth session), Racism, Racial Discrimination, Xenophobia and Related Intolerance: Report of the expert seminar on the role of the Internet in the light of the provisions of the International Convention on the Elimination of All Forms of Racial Discrimination (Geneva, 10–14 November 1997), E/CN.4/1998/77/Add.2, 6 January 1998.

regular meetings for law enforcement agencies dealing with cybercrimes to stimulate further collaboration. Aligning national criminal laws “in general”, however, does not seem to be a feasible option due to the moral, cultural, economic, and political differences between States. Some sort of consensus may be established in relation to specific crimes such as child pornography following the development of the Council of Europe’s Cybercrime Convention.[63]

The current filtering technology does not respect legitimate differences between nation-states. In fact it does not even respect some basic human rights. The rights to freedom of expression and access to information are enshrined in the European Convention on Human Rights and other international human rights instruments, such as the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights. These core documents explicitly protect freedom of expression without regard to borders, a phrase especially pertinent to the global Internet.[64] The rating and filtering systems violate these freedom of expression guarantees.[65]

Blocking and filtering software is less restrictive than government regulation and censorship but other alternatives do exist. There should be more emphasis on promoting the Internet as a positive and beneficial medium and there is urgent need for awareness of Internet usage. Governments and regulators should invest more in educational and awareness campaigns rather than promoting ineffective rating and filtering tools which only create a false sense of security for parents and teachers, while children quickly manage to find any loopholes. The advice to be given to concerned users, and especially parents, would be to educate your children rather than placing your trust in technology or in an industry that believes it can do a better job of protecting children than parents. The message is to be responsible parents not censors.

[63] See generally Y. Akdeniz, “An Advocacy Handbook for the Non-Governmental Organisations: The Council of Europe’s Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems, Cyber-Rights & Cyber-Liberties”, December 2003, at <http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf>

[64] See further the GILC report, “Regardless Of Frontiers: Protecting The Human Right to Freedom of Expression on the Global Internet” (Washington DC: CDT, September 1998), at <http://www.gilc.org/speech/report/>

[65] See the Global Internet Liberty Campaign Statement submitted to the Internet Content Summit, Munich, Germany, September 1999, at <http://www.gilc.org/speech/ratings/gilc-munich.html>

Hate Speech on the Internet

Sandy Starr

Understanding Hate Speech

Stepping Back from Human Rights. Whenever the problem of hate speech is discussed, it's often in the context of the human rights tradition, where rights have to be balanced with one another and with corresponding responsibilities. For instance, the Council of Europe's Additional Protocol to the Convention on Cybercrime, which seeks to regulate hate speech on the Internet, invokes "the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature".[1]

But despite the common assumption that human rights are an eternal and morally unimpeachable way of understanding freedom, it's important to understand that the doctrine of human rights as currently applied and understood dates back only as far as the Second World War. [2] There is a libertarian tradition quite distinct from the human rights tradition, in which a select number of essential freedoms – including freedom of speech – are understood to be absolute, and not negotiable or subject to being balanced.[3] From this perspective, unless we're free to say what we believe, to experience

[1] Council of Europe, Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, 28 January 2003 <http://conventions.coe.int/Treaty/en/Treaties/Word/189.doc> (.doc 71KB), 2.

[2] For an excellent critical history of human rights, see Kirsten Sellars, *The Rise and Rise of Human Rights* (Stroud: Sutton Publishing, 2002).

[3] See Sandy Starr "The diminishing importance of constitutional rights in the internet age", *From Quill to Cursor: Freedom of the Media in the Digital Era* (Vienna: OSCE, 2003) <http://www.osce.org/documents/rfm/2003/04/41_en.pdf> (.pdf 399 KB), 57–72.

and express whatever emotion we like (including hate), and to hate whomever we choose, then we aren't really free at all.[4] As one senior UK judge has said, "freedom only to speak inoffensively is not worth having".[5]

Even though human rights are now central to European policy and jurisprudence, and it's difficult to envisage the human rights framework being substantially challenged in the foreseeable future, it's nonetheless useful to take a step back from this all-encompassing framework. Only then can we understand the contradictions and difficulties that are thrown up, when categories such as "hate speech" and "hate crime" enter into regulation

Once Free Speech is Limited, it Ceases to be Free. Those who argue for the regulation of hate speech often claim that they support the principle of free speech, but that there is some kind of distinction between standing up for free speech as it has traditionally been understood, and allowing people to express hateful ideas.

For example, the Muslim Council of Britain argues that "a free discourse... on the merits of Islam and Muslims ... is of course necessary in an open society, but to urge others to hate, and thereby oppress, an entire faith community must be unacceptable at all times and all places".[6] And the UK's Institute of Race Relations, in seeking to outlaw hateful content from the popular media, argues that "the 'press freedom' that was fought for in previous centuries ... is not the freedom of large corporations to be involved in the industrialised production of racism for profit".[7]

Elsewhere, the UK's home secretary David Blunkett, proposes to introduce an offence of incitement to religious hatred into British law. He insists that "people's rights to debate matters of religion and proselytise would be protected, but we cannot allow people to use religious differences to create hate".[8]

Divvying up the principle of free speech in this way, so that especially abhorrent ideas are somehow disqualified from its protection, is a more dubious exercise than these sorts of comments suggest. After all, it's not as though the right to free speech contains within it some sort of prescription as to what the content of that speech will consist of. Any such prescription would be contrary to the essential meaning of the word "free".

Free speech is an important prerequisite for the development of progressive ideas, but there's no getting around the fact that it will also be exploited by people with ideas that are far from progressive. We can't enjoy the benefits afforded by free speech, without accepting a concomitant obligation – to use this freedom to contest ideas we disagree with in the court of public opinion, rather than undermining this freedom by calling upon state or private censors to suppress ideas.

Admittedly, the right to free speech has traditionally been subject to certain exceptions, even outside of the human rights framework. In the American legal tradition, for instance, free speech does not provide a defence in instances of "clear and present danger". The "clear and present danger" exception has

[4] See Mick Hume, "Don't you just hate the Illiberati?", *spiked*, 12 July 2004 <http://www.spiked-online.com/printable/0000000CA5E2.htm>

[5] Stephen Sedley, *Redmond-Bate v. Director of Public Prosecutions*, 23 July 1999 <http://www.freebeagles.org/caselaw/CL_bp_Redmond-Bate_full.html>

[6] Inayat Bunglawala, "Law on 'incitement to religious hatred' – responding to Will Cummins", Muslim Council of Britain, 16 July 2004 <http://www.mcb.org.uk/letter76.html>

[7] Arun Kundnani, "Freedom to hate?", Institute of Race Relations, 20 May 2003 <http://www.irr.org.uk/2003/may/ak000012.html>, reproduced from *Campaign Against Racism and Fascism*.

[8] David Blunkett, "New challenges for race equality and community cohesion in the twenty-first century", United Kingdom Home Office, 7 July 2004 <http://www.homeoffice.gov.uk/docs3/race-speech.pdf> (.pdf 104 KB), 12.

in turn been used as a justification for regulating hate speech. But upon closer inspection, this transpires to be a very specific and narrow exception, and not one that supports the idea of hate speech at all.

"Clear and present danger" was originally conceived by the Supreme Court Justice Oliver Wendell Holmes Jr, with reference to those exceptional circumstances where rational individuals can be said to be compelled to act in a certain way. In Holmes Jr's classic example – "a man falsely shouting fire in a theatre and causing a panic" – rational individuals are compelled to act by immediate fear for their safety.[9]

In the vast majority of instances, however – including incitement to commit a hateful act – no such immediate fear exists. Rather, there is an opportunity for the individual to assess the words that they hear, and to decide whether or not to act upon them. It is therefore the individual who bears responsibility for their actions, and not some third party who instructed that individual to behave in a particular way.

Distinguishing Speech from Action. This brings us to what is arguably the most problematic aspect of the category of hate speech – the fact that it implicitly confuses speech with action. In their attempts to tackle prejudice, policymakers are only too quick to conflate these two very different things.

Take Belgian prime minister Guy Verhofstadt's declaration, at the OSCE Conference on Tolerance and the Fight against Racism, Xenophobia and Discrimination held in Brussels in September 2004, that "there must be a coherent legal framework prohibiting discrimination and racism of whatever sort".[10] Interpreted literally, this statement would mean the authorities monitoring our every utterance and interaction, and intervening in any instance where our behaviour matched the official definition of “discrimination and racism”. Is this a society that anyone who genuinely cares about freedom would wish to inhabit?

The British academic David Miller, an advocate of hate crime legislation, complains that “advocates of free speech tend to assume that speech can be clearly separated from action”.[11] But outside of the obscurer reaches of academic postmodernism, one would be hard-pressed to dispute that there *is* a distinction between what people say and think on the one hand, and what they do on the other.

Certainly, it becomes difficult, in the absence of this basic distinction, to sustain an equitable system of law. If our actions are not distinct from our words and our thoughts, then there ceases to be a basis upon which we can be held responsible for our actions. Once speech and action are confused, then we can always pass the buck for our actions, no matter how grievous they are – an excuse commonly known as “the Devil made me do it”.

In truth, it is not words in themselves that make things happen, but the estimation in which we hold those words. And if ideas that we disagree with are held in high estimation by others, then we’re not going to remedy this situation by trying to prevent those ideas from being expressed. Rather, the only legitimate way we can tackle support for abhorrent ideas, is to seek to persuade people of our own point of view. This process, quaint though it may sound to some, is conventionally known as political debate.

[9] Oliver Wendell Holmes Jr, *Schenck v. United States* , 3 March 1919 <http://caselaw.lp.findlaw.com/scripts/printer_friendly.pl?page=us/249/47.html>

[10] Guy Verhofstadt, “Speech by prime minister Guy Verhofstadt at the opening of the OSCE Conference on Tolerance and the Fight against Racism, Xenophobia and Discrimination”, 13 September 2004 <http://www.osce.org/documents/cio/2004/09/3508_en.pdf> (.pdf 24.2 KB), 2–3.

[11] Ursula Owen and David Miller, “Not always good to talk”, *Guardian*, 27 March 2004 <http://www.guardian.co.uk/print/0,3858,4889396-103677,00.html>

When the authorities start resorting to hate speech regulation, in order to suppress ideas that they object to, this is an indication that the state of political debate is far from healthy.

Hate Speech and the Health of Politics. That angst over hate speech goes hand in hand with the degradation of politics can be seen in recent European elections, such as the French presidential elections held in 2002 and the European Parliament elections held in 2004. The response by mainstream political parties, to the perceived threat posed by far-right parties in these elections, was to suggest that the main reason why people should bother to vote is to keep the far right out of power.

This notion – that if you don't vote, then you're automatically giving the far right a helping hand – is a kind of electoral blackmail. It sends out a message that is arguably even more destructive than the bigoted drivel put about by the far right, because if the best reason the political mainstream can offer people for voting is to keep the other lot out, then that's a tacit admission that the political mainstream doesn't actually have any ideas worth voting *for*.[12]

It's also the case that when politicians focus their attention and their policies upon the problem of hate speech and hate crimes, their concerns can become a self-fulfilling prophecy. Constantly flagging up the problems of hatred and prejudice, between people of different races, colours, or creeds, subsequently encourages those people to view their grievances in those terms. A vivid illustration of this was provided by the riots and clashes that occurred in the UK in 2001, in northern mill towns of Oldham, Bradford and Burnley.

The conventional view was that these violent incidents were stoked by the far right, but evidence actually suggests that the racial tensions in these towns owed more to the blanket coverage and policing of hate speech and hate crimes. The police in these regions were so keen to demonstrate their commitment to dealing with hate, that they treated crimes committed by whites against Asians as racially motivated, even when they were not reported as such. It's not so much that these towns had a greater problem with racism than other towns in the UK, but rather that in these towns, the authorities made racism into a higher-profile issue – with explosive consequences.[13]

Distinguishing Prejudice from Emotion. In addition to distinguishing between speech and action, when assessing the usefulness of "hate speech" as a regulatory category, it is also useful to make a distinction between forms of prejudice such as racism on the one hand, and generic emotions such as hate

[12] See Josie Appleton, "Defending democracy – against the voters", *spiked*, 23 April 2002 <http://www.spiked-online.com/printable/00000006D8AF.htm>; Dominic Standish, "Where are Le Pen friends now?", *spiked*, 29 April 2002 <http://www.spiked-online.com/printable/00000006D8BC.htm>; Mick Hume, "Who's afraid of the far right?", *spiked*, 3 May 2002 <http://www.spiked-online.com/printable/00000006D8D1.htm>; Brendan O'Neill, "The myth of the far right", *spiked*, 12 June 2002 <http://www.spiked-online.com/printable/00000006D931.htm>; Josie Appleton, "Cranking up the cranks", *spiked*, 3 June 2004 <http://www.spiked-online.com/printable/0000000CA564.htm>; Jennie Bristow, "Compulsory voting: turnout is not the problem", *spiked*, 16 June 2004 <http://www.spiked-online.com/printable/0000000CA591.htm>; Sandy Starr, "Blowing up the BNP", *spiked*, 16 July 2004 <http://www.spiked-online.com/printable/0000000CA5FC.htm>

[13] See Brendan O'Neill, "Same Oldham story?", *spiked*, 29 May 2001 <http://www.spiked-online.com/printable/00000002D0F7.htm>; Brendan O'Neill, "Why banning the BNP is bad for democracy", *spiked*, 12 June 2001 <http://www.spiked-online.com/printable/00000002D121.htm>; Brendan O'Neill, "Oldham: unasked questions", *spiked*, 9 July 2001 <http://www.spiked-online. com/printable/00000002D179.htm>; Josie Appleton, "After Bradford: engineering divisions", *spiked*, 16 July 2001 <http://www.spiked-online.com/printable/00000002D19A.htm>; Kenan Malik, "The trouble with multiculturalism", *spiked*, 18 December 2001 <http://www.spiked-online.com/printable/00000002D35E.htm>; Brendan O'Neill, "Who divided Oldham?", *spiked*, 1 May 2002 <http://www.spiked-online.com/printable/00000006D8C1.htm>; Bruno Waterfield, "Imposing 'parallel lives'", *spiked*, 22 January 2003 <http://www.spiked-online.com/printable/00000006DBFE.htm>; Munira Mirza, "How 'diversity' breeds division" *spiked*, 19 August 2004 <http://www.spiked-online. com/printable/0000000CA690.htm>

on the other. Whereas racism is a wrongheaded prejudice that deserves to be contested, hatred is not objectionable in itself. Hatred is merely an emotion, and it can be an entirely legitimate and appropriate emotion at that.

When the Council of Europe sets out to counter "hatred", with its Additional Protocol to the Convention on Cybercrime, it uses the word to mean "intense dislike or enmity".[14] But are right-thinking people not entitled to feel "intense dislike or enmity" – towards racists, for example?

Hate is something that most of us experience at one time or another, and is as necessary and valid an emotion as love. Even David Blunkett, the principal architect of initiatives against hate speech and hate crimes in the UK, has admitted that when he heard that the notorious serial killer Harold Shipman had committed suicide in prison, his first reaction was: "Is it too early to open a bottle?"[15] Would Blunkett's perfectly natural reaction be permitted, under a regime where hate speech was outlawed?

Hate speech regulation is often posited as a measure that will prevent society from succumbing to totalitarian ideologies, such as fascism. Ironically, however, the idea that we might regulate speech and prosecute crimes according to the emotions we ascribe to them, is one of the most totalitarian ideas imaginable.

Most countries already have laws that prohibit intimidation, assault, and damage to property. By creating the special categories of "hate speech" and "hate crime" to supplement these offences, and presuming to judge people's motivations for action rather than their actions alone, we come worryingly close to establishing in law what the author George Orwell called "thoughtcrime".

From Hate Crime to Thoughtcrime. In Orwell's classic novel *1984*, thoughtcrime is the crime of thinking criminal thoughts, "the essential crime that contained all others in itself".[16] Hatred is permitted, indeed is mandatory, in Orwell's dystopia, so long as it is directed against enemies of the state. But any heretical thought brings with it the prospect of grave punishment. Orwell demonstrates how, by policing language and by forcing people to carefully consider every aspect of their behaviour, orthodoxy can be sustained and heresy ruthlessly suppressed.

In *1984*, no hard evidence is necessary in order for someone to be held guilty of thoughtcrime. As with hate speech and hate crime today, the authorities in the novel have unlimited latitude to interpret people's words and actions as having suspicious motives. The preoccupation with language and etiquette of those who propose hate speech regulation, and the significance that they ascribe to words, are reminiscent of the strategies employed in *1984* to reduce people's capacity to think prohibited thoughts. As one character says in the novel, "in the end we shall make thoughtcrime literally impossible, because there will be no words in which to express it".[17]

The human instinct to question received wisdom and resist restrictions upon thought is, ultimately and thankfully, irrepressible. But inasmuch as this instinct can be repressed, the authorities must first encourage in the populace a form of wilful ignorance that Orwell calls "crimestop" – in *1984*, the principal means of preventing oneself from committing

[14] Explanatory report, Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Council of Europe, 28 January 2003 <http://conventions.coe.int/Treaty/en/Reports/Html/189.htm>

[15] See "Blunkett admits Shipman error", BBC News, 16 January 2004 <http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/uk_politics/3404041.stm>

[16] George Orwell, *1984* (Harmondsworth: Penguin, 2000), 21.

[17] Ibid., 55.

thoughtcrime. In Orwell's words: "*Crimestop* means the faculty of stopping short, as though by instinct, at the threshold of any dangerous thought. It includes the power of not grasping analogies, of failing to perceive logical errors, of misunderstanding the simplest arguments…and of being bored or repelled by any train of thought which is capable of leading in a heretical direction. *Crimestop*, in short, means protective stupidity."[18]

Labelling speech that we disagree with "hate speech", and seeking to prohibit it instead of taking up the challenge of disputing it, points to a world in which we resort to "protective stupidity" to prevent the spread of objectionable ideas. Not only is this inimical to freedom, but it gives objectionable ideas a credibility that they often don't deserve, by entitling them to assume the righteous attitude of challenging authoritarian regulation.

Better to debate those we disagree with head-on, than make them martyrs to censorship.

Regulating Hate Speech on the Internet. The Internet continues to be perceived as a place of unregulated and unregulable anarchy. But this impression is becoming less and less accurate, as governments seek to monitor and rein in our online activities.

Initiatives to combat online hate speech threaten to neuter the Internet's most progressive attribute – the fact that anyone, anywhere, who has a computer and a connection, can express themselves freely on it. In the UK, regulator the Internet Watch Foundation (IWF) advises that if you "see racist content on the Internet", then "the IWF and police will work in partnership with the hosting service provider to remove the content as soon as possible".[19]

The presumption here is clearly in favour of censorship – the IWF adds that "if you are unsure as to whether the content is legal or not, be on the safe side and report it".[20] Not only are the authorities increasingly seeking out and censoring Internet content that they disapprove of, but those sensitive souls who are most easily offended are being enlisted in this process, and given a veto over what the rest of us can peruse online.

Take the Additional Protocol to the Convention on Cybercrime, which seeks to prohibit "racist and xenophobic material" on the Internet. The Additional Protocol defines such material as "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors".[21] It doesn't take much imagination to see how the Bible or the Qur'an could fall afoul of such extensive regulation, not to mention countless other texts and artistic and documentary works.

In accordance with the commonly stated aim of hate speech regulation, to avert the threat of fascism, the Additional Protocol also seeks to outlaw the "denial, gross minimisation, approval or justification of genocide or crimes against humanity".[22] According to the Council of Europe, "the drafters considered it necessary not to limit the scope of this provision only

[18] George Orwell, *1984* (Harmondsworth: Penguin, 2000), 220–21.

[19] "Racial issues", on the Internet Watch Foundation website <http://www.iwf.org.uk/howto/page.20.27.htm>

[20] "The hotline and the law", on the Internet Watch Foundation website <http://www.iwf.org.uk/public/page.31.htm>

[21] Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Council of Europe, 28 January 2003 <http://conventions.coe.int/Treaty/en/Treaties/Word/189.doc> (.doc 71KB), 3.

[22] Ibid., 4.

to the crimes committed by the Nazi regime during the Second World War and established as such by the Nuremberg Tribunal, but also to genocides and crimes against humanity established by other international courts set up since 1945 by relevant international legal instruments."[23]

This is an instance in which the proponents of hate speech regulation, while ostensibly guarding against the spectre of totalitarianism, are behaving in a disconcertingly authoritarian manner themselves. Aside from the fact that Holocaust revisionism can and should be contested with actual arguments, rather than being censored, the scale and causes of later atrocities such as those in Rwanda or former Yugoslavia are still matters for legitimate debate – as is whether the term "genocide" should be applied to them. The European authorities claim to oppose historical revisionism, and yet they stand to enjoy new powers that will entitle them to impose upon us *their* definitive account of recent history, which we must then accept as true on pain of prosecution.

Remarkably, the restrictions on free speech contained in the Additional Protocol could have been even more severe. Apparently, "the committee drafting the Convention discussed the possibility of including other content-related offences", but "was not in a position to reach consensus on the criminalisation of such conduct".[24] Still, the Additional Protocol as it stands is a significant impediment to free speech, and an impediment to the process of contesting bigoted opinions in free and open debate. As one of the Additional Protocol's more acerbic critics remarks: "Criminalising certain forms of speech is scientifically proven to eliminate the underlying sentiment. Really, I read that on a match cover."[25]

Putting the Internet into Perspective. The Internet lends itself to lazy and hysterical thinking about social problems. Because of the enormous diversity of material available on it, people with a particular axe to grind can simply log on and discover whatever truths about society they wish to. Online, one's perspective on society is distorted. When there are so few obstacles to setting up a website, or posting on a message board, all voices appear equal.

The Internet is a distorted reflection of society, where minority and extreme opinion are indistinguishable from the mainstream. Methodological rigour is needed, if any useful insights into society are to be drawn from what one finds online. Such rigour is often lacking in discussions of online hate speech.

For example, the academic Tara McPherson has written about the problem of deep-South redneck websites – what she calls "the many outposts of Dixie in cyberspace".[26] As one reads through the examples she provides of neo-Confederate eccentrics, one could be forgiven for believing that "The South Will Rise Again", as the flags and bumper stickers put it. But by that token, the world must also be under dire threat from paedophiles, Satanists, and every other crackpot to whom the Internet provides a free platform.

[23] Explanatory report, Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Council of Europe, 28 January 2003 <http://conventions.coe.int/Treaty/en/Reports/Html/189.htm>

[24] Ibid.

[25] Thomas C. Greene, "Euro thought police criminalise impure speech online", *Register*, 11 November 2002 <http://www.theregister.co.uk/2002/11/11/euro_thought_police_criminalize_impure/print.html>

[26] Tara McPherson, "I'll take my stand in DixieNet", in Beth E. Kolko, Lisa Nakamura, Gilbert B. Rodman (eds.), *Race in Cyberspace* (New York: Routledge, 2000), 117. For a review of this book, see Sandy Starr, "Race in Cyberspace", *Global Review of Ethnopolitics*, vol. 1, no. 4 <http://www.ethnopolitics.org/archive/volume_I/issue_4/issue_4.pdf> (.pdf 903 KB), 132–34.

"How could we narrate other versions of Southern history and place that are not bleached to a blinding whiteness⸮", asks McPherson, as though digital Dixie were a major social problem.[27] In its present form, the Internet inevitably appears to privilege the expression of marginal views, by making it so easy to express them. But we must remember that the mere fact of an idea being represented online, does not grant that idea any great social consequence.

Of course, the Internet has made it easier for like-minded individuals on the margins to communicate and collaborate. Mark Potok, editor of the Southern Poverty Law Centre's *Intelligence Report* – which "monitors hate groups and extremist activities"[28] – has a point when he says: "In the 1970s and 80s the average white supremacist was isolated, shaking his fist at the sky in his front room. The net changed that."[29] French minister of foreign affairs Michel Barnier makes a similar point more forcefully, when he says: "The Internet has had a seductive influence on networks of intolerance. It has placed at their disposal its formidable power of amplification, diffusion and connection."[30]

But to perceive this "power of amplification, diffusion and connection" as a momentous problem is to ignore its corollary – the fact that the Internet also enables the rest of us to communicate and collaborate, to more positive ends. The principle of free speech benefits us all, from the mainstream to the margins, and invites us to make the case for what we see as the truth. New technologies that make it easier to communicate benefit us all in the same way, and we should concentrate on exploiting them as a platform for our beliefs, rather than trying to withdraw them as a platform for other people's beliefs.

We should always keep our wits about us, when confronted with supposed evidence that online hate speech is a massive problem. A much-cited survey by the web and e-mail filtering company SurfControl concludes that there was a 26 per cent increase in "websites promoting hate against Americans, Muslims, Jews, homosexuals and African-Americans, as well as graphic violence" between January and May 2004, "nearly surpassing the growth in all of 2003". But it is far from clear how such precise quantitative statistics can be derived from subjective descriptions of the content of websites, and from a subjective emotional category like "hate".

SurfControl survey unwittingly illustrates how any old piece of anecdotal evidence can be used to stir up a panic over Internet content, claiming: "Existing sites that were already being monitored by SurfControl have expanded in shocking or curious ways. Some sites carry graphic photos of dead and mutilated human beings."[31] If SurfControl had got in touch with me a few years earlier, I could still easily have found a few photos of dead and mutilated human beings on the Internet for them to be shocked by. Maybe then, they would have tried to start the same panic a few years earlier? Or maybe they wheel out the same shocking claims every year, in order to sell a bit more of their filtering software – who knows?

Certainly, it's possible to put a completely opposite spin on the amount of hate speech that exists on the Internet. For example, Karin Spaink, chair of the privacy and digital rights

[27] Tara McPherson, "I'll take my stand in DixieNet", in Beth E Kolko, Lisa Nakamura, Gilbert B Rodman (eds.), *Race in Cyberspace* (New York: Routledge, 2000), 128.

[28] *Intelligence Project*, section of the Southern Poverty Law Centre website <http://www.splcenter.org/intel/intpro.jsp>

[29] Quoted in: Nick Ryan, "Fear and loathing", *Guardian*, 12 August 2004 <http://www.guardian.co.uk/print/0,3858,4991037-110837,00.html>

[30] Michel Barnier, French Ministry of Foreign Affairs, "Opening of the meeting", OSCE Meeting on the Relationship Between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes, 16 June 2004 <http://www.osce.org/documents/cio/2004/06/3105_en.pdf> (.pdf 19.2 KB), 2.

[31] SurfControl, "SurfControl reports unprecedented growth in hate and violence sites during first four months of 2004", 5 May 2004 <http://www.surfcontrol.com/news/newsitem.aspx?id=650>

organization Bits of Freedom, concludes that "slightly over 0.015 per cent of all web pages contain hate speech or something similar" – a far less frightening assessment.[32]

It's also inaccurate to suggest that the kind of Internet content that gets labelled as hate speech goes unchallenged. When it transpired that the anti-Semitic website Jew Watch ranked highest in the search engine Google's results for the search term "Jew", a Remove Jew Watch campaign was established, to demand that Google remove the offending website from its listings.[33] Fortunately for the principle of free speech, Google did not capitulate to this particular demand – even though in other instances, the search engine has been guilty of purging its results, at the behest of governments and other concerned parties.[34]

Forced to act on its own initiative, Remove Jew Watch successfully used Googlebombing – creating and managing web links in order to trick Google's search algorithms into associating particular search terms with particular results – to knock Jew Watch off the top spot.[35] This was fair game, and certainly preferable to Google (further) compromising its ranking criteria.[36] Better still would have been either a proper contest of ideas between Jew Watch and Remove Jew Watch, or alternatively a decision that Jew Watch was beneath contempt and should simply be ignored. Not every crank and extremist warrants attention, even if they do occasionally manage to spoof search engine rankings.

Conclusion. If we ask the authorities to shield us from hate speech today, the danger is that we will be left with no protection from those same authorities tomorrow, once they start telling us what we're allowed to read, watch, listen to, and download.

According to the Additional Protocol to the Convention on Cybercrime, "national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems".[37] But legal responses are entirely *inadequate* for this purpose. If anything, legal responses to hateful opinions inadvertently bolster them, by removing them from the far more effective and democratic mechanism of public scrutiny and political debate.

"Hate speech" is not a useful way of categorizing ideas that we find objectionable. Just about the only thing that the category *does* usefully convey is the attitude of the policymakers, regulators and campaigners who use it. Inasmuch as they can't bear to see a no-holds-barred public discussion about a controversial issue, these are the people who really *hate speech*.

[32] Karin Spaink, "Is prohibiting hate speech feasible – or desirable?: technical and political considerations", Bits of Freedom, 30 June 2004 <http://www.osce.org/documents/rfm/2004/06/3263_en.pdf> (.pdf 50.1 KB), 14.

[33] See the Google <http://www.google.com> and Jew Watch <http://www.jewwatch.com> websites.

[34] See "Replacement of Google with alternative search systems in China: documentation and screenshots", Berkman Center for Internet and Society, September 2002 <http://cyber.law.harvard.edu/filtering/china/google-replacements>; Benjamin Edelman and Jonathan Zittrain, "Localised Google search result exclusions", Berkman Center for Internet and Society, October 2002 <http://cyber.law.harvard.edu/filtering/google>; Benjamin Edelman, "Empirical Analysis of Google SafeSearch", Berkman Center for Internet and Society, April 2003 <http://cyber.law.harvard.edu/people/edelman/google-safesearch>

[35] See John Brandon, "Dropping the bomb on Google", *Wired News*, 11 May 2004 <http://www.wired.com/news/print/0,1294,63380,00.html>

[36] For more on the technology and politics of Google search results, see Sandy Starr, "Google hogged by blogs", *spiked*, 15 July 2003 <http://www.spiked-online.com/printable/00000006DE60.htm>; "Giddy over Google".

[37] Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Council of Europe, 28 January 2003 <http://conventions.coe.int/Treaty/en/Treaties/Word/189.doc> (.doc 71KB), 2.

Kurt Einzinger

Media Regulation on the Internet

For hundreds of years the only means of communicating with a large number of people were the spoken word and the printed page, which also had only limited circulation. It is only over the last 50 or 60 years that telecommunications, radio and television developed as mass media and have become widely available. Major debates on politics, social issues and social change now take place through the mass media.

Until recently, only large public or private corporations have had the means to produce material for and through these media, because the cost and complexity of the technology involved were prohibitive. In the Internet age, however, Internet and multimedia technologies are available on every computer and ordinary people now have the opportunity to use mass media, both as audience and producer.

The Internet is a type of mass media with an added quality. Every Internet user has the potential to publish via the Internet and be read or seen by hundreds of millions of people. Due to the continuously growing population of Internet users – the European goal is to reach universal access – the number of people, who are potentially reachable with web publications, is widening constantly.

Paradoxically, although every website can be accessed by hundreds of millions of people, in reality more than 95 per cent of websites will not be seen by many people at all. This is due to the dazzling array and variety of websites on the Web, language barriers and people's usual preference for “local” services and content. To use the Internet as mass media, substantial financial resources are necessary. Advertising, powerful hardware, distributed servers and broad connectivity together with attractive and up-to-date content are minimum requirements and need significant funds. This means that again only the financially powerful institutions and corporations are able to use these new media as mass media. In this way the traditional, large media companies also have a significant advantage on the Internet over other enterprises; indeed the potential leverage via the Internet can be much greater than for other media.

Media Regulation is Content Regulation. If we talk about media regulation we talk predominantly about regulating content. The content published on the Web is expected to comply with societal values, which are reflected in the local legal system. If content infringes a provision of criminal law or is adjudged to be incompatible with civil law, it must be modified or removed. But it must be made very clear: content that is not illegal must be allowed on the Internet. The Internet offers immense potential for civil society and it is in the interests of civil liberties that the public’s access and use of this new medium should not be unduly restricted.

The Internet is a global medium, but applicable legal systems are usually confined to national borders. In many instances national laws differ quite substantially, which can lead to certain difficulties. For example, in some Central European countries there is strict legislation against right wing extremism (neo-Nazism), but this is absent from most other countries. Therefore there are some neo-Nazi sites on the Web, which cannot be removed because their servers are located in countries where there are no legal grounds for their removal.

Such scenarios normally give rise to calls for “filtering” or “blocking”. Filtering is the selective removal of certain content from the flow of data, whereas “blocking” is the practice of making it impossible to reach certain web pages (URLs). Both methods are cost intensive, have very limited effectiveness and can lead to significant “collateral damage” to other parties (false positives). They are simply not feasible or sensible options.

The organization and technology of the Internet does not permit the use of these techniques in a successful way. On the Internet, central nodes, where you could effectively monitor the data flow, just don’t exist. At the point of origin, content is split into many small data packets that seek their way through the networks on their own and are reassembled at the point of destination. There are many, many routes to get from “A to B” on the Internet. Remember: the Internet consists of a myriad of IP networks and Internet service providers can only see and monitor their own small part. Except for totalitarian States, where the Internet is seen as a threat and not as an advantage, the practice of “filtering” and “blocking” is not widely used – thank goodness!

The Responsibility of Internet Service Providers. The European Union’s Directive on Electronic Commerce[1], which was adopted in 2000, defines the different roles and liabilities of Internet service providers. Section 4 deals with the liability of intermediary service providers and differentiates between “mere conduit”, “caching” and “hosting”.

Article 12, relating to “mere conduit”, states: “Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission."

"The acts of transmission and of provision of access referred to […] include the automatic, intermediate and transient storage of the information transmitted, in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission."

In Article 13, "caching" is defined as the "automatic, intermediate and temporary storage" of information. The liability of ISPs is treated more or less like "mere conduit", with the addition that "the provider acts expeditiously to remove or to disable access to the information it has stored, upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement."

Article 14 deals with "hosting", which consists of the storage of information provided by a recipient of the service. It asserts that: "Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

knowledge or awareness, acts expeditiously to remove or to disable access to the information."

Finally, Article 15 affirms there shall be "no general obligation to monitor". "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."

In most Member States this Directive has been transposed into national law and constitutes the basis for the manner in which European ISPs handle illegal content on the Internet. In some countries, including Austria, this set of rules constitutes the background for more precise and detailed self-regulation by ISPs. A code of conduct[2] tries to fill the gaps in the law by clearly defining what an ISP must do in different situations.

In an effort to eradicate criminal law issues like child pornography or right-wing extremism on the Internet, ISPs established hotlines in many countries (or have assisted in their establishment). These hotlines are run by legal experts, who check incoming complaints about criminal content. If the complaint is found to be legitimate, the hotline in the implicated server's country of origin will be contacted and the criminal content will then be removed from the Net by the provider or the appropriate law enforcement agencies. This remains the only really effective method to eradicate illegal material from the Net – it focuses on "removal at source".

Freedom of Communication and Information on the Internet. Excellent guidelines on the issue of freedom of communication and information on the Internet were prepared by the Ministerial Committee of the Council of Europe and adopted on 28 May 2003.[3] In this declaration seven principles are postulated. Excerpts are quoted on the following pages:

- Principle 1 postulates that Member States should not subject content on the Internet to restrictions which go further than those applied to other media.
- Principle 2 states that Member States should encourage self-regulation or co-regulation regarding content disseminated on the Internet.
- Principle 3 calls for an absence of prior state control. Public authorities should not, through general blocking or filtering measures, deny the public access to information and other communication on the Internet, regardless of frontiers. This does not prevent the installation of filters for the protection of minors, in particular in places accessible to them, such as schools or libraries.
- Principle 4 argues for the removal of barriers to the participation of individuals in the Information Society. Member States should foster and encourage access for all to Internet communication and information services on a non-discriminatory basis at an affordable price. Furthermore, the active participation of the public, for example by setting up and running individual websites, should not be subject to any licensing or other requirements having a similar effect.
- Principle 5 asks for freedom to provide services via the Internet. The provision of services via the Internet should not be made subject to specific authorization schemes on the sole grounds of the means of transmission used. Member States should seek measures to promote a pluralistic offer of services via the Internet, which caters to the different

[2] For Austria, see: Allgemeine Regeln zur Haftung und Auskunftspflicht des Internet Service Providers, <http://www.ispa.at/www/getFile.php?id=22>

[3] Council of Europe's Declaration on freedom of communication on the Internet, adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies.

needs of users and social groups. Service providers should be allowed to operate in a regulatory framework that guarantees them non-discriminatory access to national and international telecommunication networks.

- Principle 6 demands a limited liability of service providers for Internet content. Member States should not impose on service providers a general obligation to monitor content on the Internet, to which they give access and transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity. Furthermore Member States should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet. In cases where the functions of service providers are wider and they store content emanating from other parties, Member States may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information. When defining under national law the obligations of service providers as set out in the previous paragraph, due care must be taken to respect the freedom of expression of those who made the information available in the first place, as well as the corresponding right of users to the information.
- Principle 7 argues that anonymity on the Internet should be preserved. In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, Member States should respect the will of users of the Internet not to disclose their identity. This

> does not prevent Member States from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.

With the above-mentioned issues in mind, media regulation on the Internet has to, on the one hand, protect and preserve freedom of communication and information, aiming to secure access for all, and on the other, regulation has to take into account the organizing principles and technology of the Internet if it aims to fight Internet-related crime effectively. At the same time, regulation has to respect and acknowledge the global nature of the Internet. This will not be an easy task for politicians and legislative bodies. Nevertheless, Internet service providers remain willing to contribute their expertise and experience to initiatives that help to curtail illegal activity via the Internet, and at the same time increase users' confidence in this most valuable medium.

Cormac Callanan

Best Practices for Internet Hotlines

The INHOPE[1] association is five years old in November 2004 and, starting from 8 hotlines, has now grown to 20 hotlines located in 18 countries. INHOPE has members from 16 European Union States and outside Europe has members from Australia, South Korea, Taiwan and the United States of America. INHOPE provides a central co-ordination function to the work of Internet hotlines fighting illegal content and illegal use of the Internet.

During the period from March 2003 to February 2004 the INHOPE network processed more than 263,000 reports on illegal content and use of the Internet. While not all members of INHOPE handle reports about hate speech, approximately 1,500 of the reports received related to racial hatred or content against human dignity. In the six-month period from March 2004 until August 2004 INHOPE received approximately 1,700 reports in this same area. In comparison, there were over 57,000 reports about illegal child pornography during the same six months.

One of the impressive facts and strengths about INHOPE is that it brings together a wide range of know-how and varying primary interests with one basic goal – to eliminate illegal material or activity on the Internet!

The members of INHOPE are aware of how the Internet has positively transformed everyone's life and how it continues to do so. INHOPE realizes that when the Internet is used correctly it is a wonderful tool. The benefits are educational, informative and entertaining. It is also an efficient and inexpensive method by which to communicate with friends and family worldwide. However, INHOPE is also conscious that there can be negative aspects, particularly when it comes to its use by children or by those wishing to spread illegal racist/hate speech.

But what is an Internet hotline? Internet hotlines provide a mechanism for receiving complaints from the public about alleged illegal content and/or use of the Internet. Hotlines must have effective transparent procedures for dealing with complaints and need the support of government, industry, law enforcement, and Internet users in the countries of operation.

INHOPE is deeply conscious of the problems created by illegal content and the complexity of responding to such issues as they relate to the Internet. The reason a hotline exists is to cause the removal of illegal material from the Internet quickly, efficiently and transparently, to enable a swift investigation by law enforcement and to collaborate at an international level with other members of INHOPE.

In addition, members of INHOPE co-operate with other members in exchanging information about illegal content, share their expertise, and make a commitment to maintain confidentiality and respect the procedures of other members.

Hotline Procedures. Once a report is received by a hotline, it is logged into the hotline database system and, if the report has not been submitted anonymously, a confirmation of receipt is sent to the reporter. Hotline staff members, who are

[1] INHOPE co-ordinates the work of 20 Internet hotlines in 18 countries around the world. Internet hotlines are an essential element in a co-ordinated response to the illegal and harmful use of the Internet. The work of a hotline would be greatly weakened if it operated alone and isolated from the wider world. The knowledge and training a hotline receives from INHOPE is invaluable and essential to its success.

specially trained in assessing Internet content, examine whether or not the reported material is illegal under their local legislation.

If the material is not illegal, the report is not processed any further. However, the hotline may still forward the report to a partner hotline following the INHOPE Best Practice Paper on the Exchange of Reports.

If the reported material is likely to be illegal under the local legislation of the hotline, the hotline carries out an examination to identify the origin of the material. This examination is time-consuming and requires technical expertise.

If, for example, a website is reachable under a domain name ending with the country code top level domain ".at", which stands for Austria, that does not mean that the web server is actually operated in Austria. It only means that the domain name has been registered with the Austrian domain name registry.

A domain name can be used to refer a user to any web server around the world as the domain name system only provides for the resolution of a domain name into an IP, which is used to establish a connection with a web server. Therefore the IP number has to be traced to find out where the web server is located.

In cases where the reported material is hosted on a locally based server, the hotline involves law enforcement and/or the Internet service provider in accordance with its procedures.

The decision to initiate a criminal investigation is a matter for law enforcement. The Internet service provider is responsible for timely removal of the specified potentially illegal content from their servers to ensure that other Internet users cannot access the material. Once such notifications are carried out, the hotline can close the case.

If the material is located on a server in a foreign country, matters become more difficult. In most cases the hotline does not have direct co-operation with foreign stakeholders.

However, hotline activity must not stop at national borders when a global medium like the Internet is concerned. At this stage, international co-operation is required. More importantly, in such a sensitive area, best possible measures have to be taken to ensure that co-operation is carried out in a trustworthy and secure environment. That is the reason why the INHOPE Association was established.

So, what do hotlines deal with? Even though each country has its own individual legislation relating to illegal material on the Internet, the original focus of INHOPE members related to illegal Internet child pornography and online abuse of children. However, increasingly Internet hotlines now deal with crimes of xenophobia, hate speech and racism.

For example, in the specific area of child pornography, although there is widespread international agreement that such material is abhorrent in modern society there are sometimes substantial, and sometimes subtle, variations in the regulatory environment. It is worth noting that in 2002 UNICEF estimated that 80 per cent of paedophile-related investigations involved more than one country, and 90 per cent involved the Internet. The broad geographical coverage by INHOPE hotlines is a very successful response to this global problem.

INHOPE also respects the different legal and cultural values which different countries observe. Material which might be considered illegal in Ireland, will not be illegal in the United States. Material which the United Kingdom considers illegal, is not illegal in the Netherlands.

While the definition of child pornography is perhaps the most closely resembled legislation across the globe, INHOPE strives to ensure a consistent response in a world of small-but-significant variations. We strongly welcome the development of the Council of Europe Cybercrime Protocol on racism as a significant step forward to clarify and standardize the definitions of hate-style criminality on the Internet. We would strongly encourage governments around the world to further harmonize their legislation and anti-hate initiatives. This would also support the work of Internet hotlines active in this area. This is essential if we are to prevent a proliferation of legislative imperialism – attempts to apply individual, sometimes contradictory, national legislation in a global Internet environment. It is in all our interests if we can approximate our understanding of what is destructive to the common good of society.

Why and how hotlines co-operate. INHOPE also juggles with many different cultural priorities. Illegal activities that are considered of major importance in one country are not given the same level of severity in another country. For example, National Socialist offences, anti-Semitism on the Internet, are of major importance in countries such as France, Germany and Austria, while Internet chat rooms and child grooming are major concerns in the United Kingdom and Canada. This does not suggest that one is more important than the other but each country must establish national priorities and allocate resources.

The work of a hotline would be greatly weakened if it operated alone and isolated from the wider world. The knowledge and training a hotline receives from INHOPE is invaluable and essential to its success. Issues such as tracing material on the Internet, exchange of reports about material located in other jurisdictions and new techniques used by criminals for the exchange of illegal material on the Internet have helped a hotline perform its core activities since the beginning of INHOPE.

Of course, the work of the hotlines and INHOPE is just one of a range of responses to illegal activity on the Internet. Other responses recognized by the EU Safer Internet Action Plan include rating and filtering technologies and awareness programmes.

Experiences: Legislation. There are significant differences between dealing with child pornography and tackling hate speech on the Internet. With child pornography there are clearer, succinct and more closed definitions in international legal instruments, while hate speech has broader, more open and therefore more ambiguous definitions. The Council of Europe Cybercrime Convention is a useful example. The definition of child pornography is:

> For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
>
> a. a minor engaged in sexually explicit conduct;
>
> b. a person appearing to be a minor engaged in sexually explicit conduct;
>
> c. realistic images representing a minor engaged in sexually explicit conduct.

However, in the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, hate speech is defined as:

> "racist and xenophobic material" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

The definition of child pornography is clear and succinct but even the underlined parts of b) and c) can be a challenge to apply. However, the second definition is a major test to match with possible illegal material. Whereas illegal child pornography is primarily image focused with similar global definitions, illegal hate speech is based on text rather than images with very different approaches and different legislation around the world. Hate speech also uses hidden language to avoid detection.

National legislation normally makes it illegal for anyone to knowingly distribute, produce, print, publish, import, export, sell or show any child pornography. However, differences start to emerge immediately after this statement. The definition of a child varies across Europe and the world. In Europe the upper age limit of a “child” ranges from 14 to 18 years. In some countries knowingly possessing child pornography is also a criminal offence. Sometimes the definition of child pornography includes computer generated or altered images. Sometimes it includes cartoon characters. Most definitions require the image (text, etc.) to show a child engaged in explicit sexual activity. This use of the words “explicit sexual activity” has created some difficult problems in relation to pictures of children being abused but with no sexual activity involved.

Regardless of the range of specific legal and jurisdictional definitions, each individual member of INHOPE operates a hotline within a single legal jurisdiction that means that any interpretations of law are subject to critical evaluation of reported material. The problems arise when material is reported to one hotline that is located in a separate jurisdiction from the reported material. If material is not illegal in the country where the hotline receives the report, the report is not usually processed any further. If the material is likely to be illegal in the country where the hotline receives the report, the report is forwarded to the hotline in the country where the material is located. The hotline in that country then determines if the material is likely to be illegal under the local law. If it is not illegal no further processing on the report is performed.

It is perhaps obvious to those with a legal background but the clear definitions included in national legislation are extremely difficult to apply in daily practice. All hotlines receive a broad range of reports for processing. These reports encompass such issues as child pornography, hate speech, adult pornography, unsolicited adult e-mails, virus attacks, financial scams and enquiries about filtering software solutions. There have been many requests for advice about best practices in dealing with non-illegal, yet harmful material on the Internet for the younger Internet surfers. The difference between what is illegal and what is harmful is at the forefront of every assessment performed by the hotline.

Processing Reports. Experience has now confirmed that tracing and tracking illegal Internet content following a report can be time-consuming and difficult. There are major difficulties about a hotline retaining material for law enforcement purposes since there are no exemptions under national law for the work of the hotline service. Therefore INHOPE best practice discourages any hotline from storing illegal content although some hotlines have specific agreements with national police forces to enable them to forward illegal content for investigation. Where hotlines do not keep or pass on specific Internet content a timely investigation is required from all parties to ensure a rapid response to the further spread of illegal content on the Internet.

Lessons Learned. It is clear from the feedback received by the hotlines that Internet users are pleased with the existence of the INHOPE hotline network and the opportunity they provide for Internet users to respond to illegal material on the Internet. It is also clear from the volume of reports processed by the hotlines and the number of convictions which can be linked to successful processing of reports that hotlines play a valuable role in the fight against illegal content on the Internet.

Activities of INHOPE. INHOPE carries out a vast range of activities and the members currently meet at least three times a year. INHOPE facilitates the exchange of reports and expertise among members. When a report is received in one country about material in another, the country hotlines involved are notified for quick and efficient processing. INHOPE also provides training at every meeting from a wide range of experts on issues ranging from technical and psychological to legal and managerial matters. There is a bursary programme for hotline staff which permits the exchange of staff among hotlines for cross-training and one-to-one training and sharing. The programme is highly appreciated by the hotlines that have benefited directly from the scheme. A mentor programme is also in place which follows on from the bursary programme. This gives one-to-one assistance from an experienced INHOPE member to a new hotline initiative. A Vanguard programme permits INHOPE to invite key personnel from a new hotline initiative to participate at an INHOPE members' meeting to enable essential early contacts to develop.

Conclusion. INHOPE has moved progressively from informal to formal co-operation and this move has meant that the organization has had to put in place mechanisms for decision-making that are acceptable for all the different types of organizations involved.

INHOPE is a very successful response to illegal use and content on the Internet. The broad network coverage, the exchange of reports about illegal content, the varied backgrounds and expertise of its membership organizations, the sharing of expertise and knowledge and the respect for cultural and legal diversity across the membership base has demonstrated the effectiveness of the hotline network. INHOPE is an effective response to illegal use and by carefully developing best practice and identifying criminal trends is also able to empower government, law enforcement, child welfare and industry to adopt the appropriate strategies to combat illegal use and content on the Internet.

The original members of INHOPE were mainly ISPs; however the INHOPE network naturally expanded and now includes hotlines set up by children's charities and public bodies, for example. All of them work closely with law enforcement at a national level and across borders. Getting co-operation to work across borders is difficult enough and getting it to work politically across such different types of organizations is an important success.

The experience of INHOPE over the last number of years is that major success can be achieved only with a co-ordinated, cross-sector, cross-cultural response to online illegal content. It is critical to identify key areas of agreement, to clarify the language we use to ensure consistency, to seek consensus on definitions and on priorities in order to enhance co-ordination, to identify good practice in different regions and countries and to prioritize based on our capabilities.

Outreach, training, awareness and education are essential responses to illegal content – especially hate speech. Raising awareness is of major importance in the fight against hate speech, since hate speech cannot be banned from the Internet completely. The inconsistencies of hate speech need to be exposed and the truth needs to be promoted so that the floor is not left only to those who publicize hate speech.

The EU Safer Internet Action Plan has been essential to the success of INHOPE. Without the financial support received under the plan, it is unlikely that so much could have been achieved. Of course, more resources – financial and otherwise – are needed to increase the scope and activities of INHOPE. INHOPE would specifically pay tribute to the staff of DG Information Society for their support and encouragement during the last number of years.

Education & Developing Internet Literacy

Cathy Wing

An Introduction to Internet Literacy

In 1962, Canadian media guru Marshall McLuhan coined the phrase “global village”, to describe how, through electric technology, we were becoming increasingly linked together across the globe. The past two decades have seen the advent of new electronic technologies – the Internet, satellite TV, mobile phones, digital cameras and wireless devices – that are making this notion a reality. While much of the developing world still remains “outside” the village, many people around the globe now watch the same TV shows and movies, listen to the same music and access the same sites on the Web.

In a world that now suffers from information overload, a central message of McLuhan’s – the importance of the active study of media – remains truer than ever. The challenge for educators in the twenty-first century is to respond to multiple literacies, and more specifically, to media literacy – an essential skill in this age of electronic information, entertainment and communications.

Media literacy has been practised around the world for more than 40 years, and in many countries, such as Canada, Australia and the UK, it has a strong presence. Canadians have always felt the need to take an analytical and reflective approach to media, given the pervasiveness of popular culture from our close neighbours, the United States. Despite this, implementing media literacy in Canadian schools has been a fairly recent phenomenon. As recently as the 1980s, critics considered media literacy a “frill”. Fortunately in today’s multilayered, interactive information society, attitudes have changed. Media literacy outcomes now form a substantial part of every Canadian province's Language Arts curriculum. Increasingly school boards are understanding that if young people are to be truly literate they're going to have to develop rigorous critical thinking skills to sift through and make sense of what they see, hear and read – in school and in the wider community.

This article will explore media literacy; what it is, approaches for implementation; and best practices for promotion and integration into schools, homes and communities.

Defining Media Education and Media Literacy. UK media educator David Buckingham defines media education as the "process of teaching and learning about the media; media literacy is the *outcome* – the knowledge and skills learners acquire."

Media education has been called the perfect curriculum because it incorporates the latest thinking in pedagogical practice; it's interdisciplinary; it develops critical thinking; and it is student-centred, putting the emphasis on analysis, enquiry and self-directed learning.

Media education encourages an approach to media that is always probing: Who is this message intended for? Who wants to reach this audience, and why? From whose perspective is this story told? Whose voices are being heard, and what voices are absent? What strategies are being used to engage my attention? Because media education is not about having the right answers but asking the right questions, the result is lifelong empowerment of the learner and the citizen.

The end result of media education is a media literate individual who has the ability to *read* the messages that are informing, entertaining, and selling to him or her daily. It's the ability to bring critical thinking and life skills and pertinent questions to all media productions and texts – from music videos to Web environments, to product placement in films and virtual advertising on football fields. It's about analysing what's there, and noticing what's not, and questioning what lies behind media productions – the motives, the money, the values and ownership – and how these factors influence the content.

The field of media is broad and amorphous, extending not just from information and entertainment mediums such as newspapers, magazines, television, film and the Internet, but encompassing many areas of popular culture such as fashion, toys, the nature of celebrity, etc. Anyone attempting to make sense of this area needs a clear conceptual framework that will allow for discussion of a variety of complex and interrelated factors. The following is a framework that is used by many Canadian educators for the analysis of media messages[1]:

1. All media messages are constructed
2. The media construct reality
3. Audiences negotiate meaning in the media
4. Media have commercial implications
5. Media contain ideological and value messages
6. Media have social and political implications
7. Form and content are closely related in the media
8. Each medium has a unique aesthetic form

A non-protectionist approach key to engaging students in media literacy in a meaningful way. Young people don't need to be protected, but invited to participate in a dialogue about media. David Buckingham argues that young people shouldn't

[1] J.S.J. Pungente and B. Duncan, *Media Literacy Resource Guide*, Ontario Ministry of Education (Toronto, 1989).

be viewed as victims who need to be rescued from the excesses and evils of their culture – which is simply the intersection of high technology, mass media and consumer capitalism – rather we should focus on their emotional engagement with media and the genuine pleasures they receive, promoting real questioning and analysis.[2]

Successful Integration of Media Literacy. In 1990, participants at the UNESCO-sponsored New Directions in Media Literacy conference at the University of Toulouse, including the British Film Institute and the Council of Europe, identified four steps that are required for the successful development of media literacy in a country's education system:

1. The establishment of curriculum guidelines (nationally or regionally) by appropriate educational authorities.
2. Teacher training programmes at university level. These are degree programmes in education with a specific specialization or major in media studies.
3. Teacher support – in-service educational programmes, summer "refresher" courses, national organizations through which teachers grow and develop in their chosen specialization – and through which the specialization itself evolves and develops through feedback by grass-roots teachers.
4. Educational resources for teaching – writing, testing and publishing of the textbooks, lesson plans, activity sheets, videos or other audio-visual materials, posters, supplemental booklets, etc. needed for teaching – developed in collaboration with all of the above.[3]

Canadian media educator John Pungente, S.J., who has studied media literacy implementation in various countries, has identified these additional factors as being crucial to success:

1. Media literacy, like other innovative programmes, must be a grass-roots movement. Teachers need to take the initiative in lobbying for its inclusion in the curriculum.
2. School districts need consultants who have expertise in media literacy, and who will establish communication networks.
3. There must be appropriate evaluation instruments suitable to the unique attributes of media studies.
4. Because media literacy involves such a diversity of skills and expertise, there must be collaboration between teachers, parents, researchers and media professionals.[4]

Integrating Internet Literacy into Media Education. The Internet has increased the importance of developing independent thinkers and informed media consumers. Because the Internet has no geographical boundaries, many regulatory and legislative standards that we take for granted – including advertising and broadcasting to young people – do not apply. The Internet has countless publishers and few gatekeepers, so the standards for authenticity and reliability of information are also absent. Third, media is no longer a matter of a passive transfer of content from producer and carrier to the receiver – it is interactive in nature. And finally; media consumers can now also be media *producers and distributors*. These last two points, specifically – interactivity and capacity for individuals

[2] R. Hobbs, "The seven great debates in the media literacy movement", *Journal of Communication*, 1998.

[3] See *Four Steps to Success in Media Literacy,* 1991 <http://www.medialit.org/reading_room/article125.html>

[4] See *Nine Factors that Make Media Literacy Flourish,* 2002 <http://www.media-awareness.ca/english/resources/educational/teaching_backgrounders/media_literacy/9_factors.cfm>

to produce and distribute media – have fundamentally changed the role that media play in our society, and particularly in the lives of young people. In this new environment, the need for media literacy is more critical than ever.

Educators play a crucial role in bridging traditional media education and Internet literacy, particularly as many societies move towards the convergence of all media platforms – the Internet, television, radio, videos, CD ROMs, DVDs, computer games, and the many forms of advertising – into one multifaceted "small screen" experience.

In a 2003 study conducted by the Media Awareness Network into young Canadians' Internet habits, students expressed frustration with what they identified as adults' need to control their Internet use. Efforts to keep them from being exposed to inappropriate material are ineffective they felt, because there are too many access points and too many places where unsupervised exploration is possible. The Internet doesn't work on the principles of *censorship* or *control* they felt, but rather on the principle of *responsible decision-making.* Rather than spending time and money and energy to try the impossible – keeping children away from material that is not suitable to their maturity or nature – young people said that efforts should be made to develop opportunities, particularly for young children, to learn how to think about choices, and gain decision-making skills.

Teachers are becoming aware that, along with learning how to navigate the Internet, young people need to develop a critical consciousness when dealing with its enormous range of content. Most, however, lack the necessary training to implement Internet literacy into their day-to-day teaching. According to a 2003/04 Statistics Canada study looking at ICT infrastructure and reach in Canada's 15,500 elementary and secondary schools, over 97 per cent of schools were connected to the Internet. Less than half of school principals, however, felt that the majority of their teachers were adequately prepared to engage their students effectively in the use of ICT to enhance learning.

There are many obstacles to preparing teachers to meet this demand, including a scarcity of professional development opportunities and resources to support classroom activity and the lack of pedagogical recognition by faculties of education. While we know that teaching young people to think critically about all the information available to them today is an essential skill, support within the education system is minimal or non-existent.

Internet Literacy and Anti-racism Education. Central to all media education is the concept of representation – how we see ourselves and how others see us. The way visible minorities are represented in mainstream media reinforces perceptions of minorities as outsiders, erodes the self-image of young people from these groups and undermines the social cohesion of society. In a multicultural democracy, media education curricula must reflect the concerns of diversity, identity and difference.

While representation, bias and stereotyping in traditional media have always been key areas of inquiry in media education, the Internet presents new challenges. The Web offers easily accessible messages of hate aimed at ethnic and racial minorities. A 2001 Media Awareness Network survey of nearly 6,000 Canadian students, ages 9 to 17, indicates that two in ten youths have come upon a site that was "really hateful" towards an individual or group of people.[5]

[5] See *Young Canadians In A Wired World: The Students' View,* 2001 <http://www.mediaawareness.ca/english/special_initiatives/surveys/phase_one/students_survey.cfm>

In the early days of the Internet, hatemongers tried to spread their messages through interactive forums. The free speech environment of newsgroups, however, ensured that false claims were challenged by healthy and vigorous debate. As a result, hatemongers soon retreated into less interactive areas of cyberspace, such as the Web, allowing them to avoid interacting with those who disagree with their views. Websites also help groups identify potential recruits who can be brought into the hate community through private chat rooms and e-mail, well away from the public eye.

With fewer opportunities for Internet users to openly confront hatemongers and debate their messages, it has become increasingly important to educate young people to recognize online hate in its many forms and to understand the strategies used to target them. Hate on the Net is not always obvious: although hard-core sites are easy to detect, some hatemongers use more subtle tactics to attract new blood. They create fun-and-games sites for children and music sites for teens; infiltrate chat rooms and newsgroups frequented by kids; and even set up sites where children might go for homework assignments. The most effective long-range strategy for helping young people is to give them lots of information about online hate – as well as the critical thinking skills to decode messages of hate, and read between the lines.

Promoting Internet Literacy: A Canadian Response. In 1999, the CRTC, Canada's national broadcast regulator, issued its decision to not regulate the Internet. The decision pointed to the necessity for industry, government and non-governmental organizations to work together, to ensure a self-regulated environment and an education and awareness approach to ensure that the new media environment provided a positive and empowering experience for Canada's young people.

Since then, a broad spectrum of Canadians have worked to develop a partnership model involving public, profit and not-for-profit partners to deliver programmes that empower children and young people with critical thinking skills for their online activities and explorations.

Government of Canada's CyberWise Strategy. In February 2001, the Canadian Government unveiled its strategy for dealing with offensive and illegal Internet content. The CyberWise Strategy focused on educating and empowering Canadians so they can become "safe, wise and responsible" Internet users. Although Canada has strong laws that apply to cyberspace, the Government of Canada acknowledged in its strategy that legislation alone will not solve the problems of illegal and offensive content on the Internet and identified "awareness, education and knowledge" as the foundations of its approach.

Media Awareness Network (MNet), a not-for-profit organization that supports media education in Canadian homes, schools and communities, was recognized in the CyberWise Strategy as the leading public education organization working in this area.[6]

Research into Young Canadians' Internet Use. To maintain critical vigour and the ability to adapt to rapid changes in the new technologies, Internet literacy demands ongoing, in-depth research. In 2000 to 2001, the Media Awareness Network (MNet) conducted the most comprehensive and wide-ranging survey of its kind in Canada in order to gain a fuller and deeper understanding of issues, behaviours and attitudes related to Internet use by young people. Phase I of the *Young Canadians In A Wired World* (*YCWW*) research project, which

[6] Cyberwise Strategy: <http://www.media-awareness.ca/english/special_initiatives/surveys/phase_one/index.cfm>

was funded by the Federal Government, included both qualitative and quantitative findings and comprised:

- a telephone survey of 1,080 Canadian parents with a home computer;
- focus groups of parents and children (aged 9–17);
- a survey of 5,682 students in grades 4 to 11 across Canada.

The survey results reinforce the fact that Canadian youth are highly engaged participants in the online world. However, the data also presents findings which show that, in this age of connectivity, there is a substantial discrepancy between how parents see their children using the Internet, and what their children are actually doing online.

The research findings from *YCWW* Phase I attracted the attention of numerous communities of interest and served as a call to action to address the risks and challenges of new media use by young people. The benefits that Canada derived from the research have been extensive. Data collected from *YCWW* contributed to:

- Internet policies in Canadian schools and public libraries;
- government policy-setting (including the Government of Canada's policy statement on *Illegal and Offensive Content on the Internet*);
- an extensive Internet education programme to educate teachers, parents, librarians and students how young people can get the most out of new technologies while being safe and responsible Internet users.[7]

In autumn 2003, Media Awareness Network embarked on Phase II of *YCWW* with a series of national focus groups with young people and parents. This qualitative research, funded by Industry Canada, showed a media landscape that has evolved significantly since 2001. In 2005 MNet will return to the classrooms from *YCWW* Phase I and survey another 6,000 students in order to revisit the benchmark measures from the original data and assess how patterns of use and attitudes have changed.[8]

Web Awareness Canada. In 1999, the Media Awareness Network (MNet) launched an Internet public awareness programme, *Web Awareness Canada.* The objective of this initiative was to ensure that public librarians and educators were informed about the challenges and opportunities that young people face when they go online and to ensure that adults are more informed and confident in supporting young people's use of Internet and ICT. The focus of the programme was to build partnerships in schools and libraries – the first public sectors to be completely connected to the Internet – by training teachers and librarians, and building the capacity in those sectors for decentralized local and regional delivery of the programme.

Web Awareness Canada has received awards and international recognition for promoting and fostering the positive use of ICT in the education and community sectors. Perhaps most importantly, provincial governments have purchased licences for these workshops, allowing thousands of teachers, librarians, parents, community leaders and health workers across Canada to use the *Web Awareness* workshops as part of their professional development and self-directed learning programmes.

Canadian Library Association (CLA) Initiatives.Canada's libraries are well connected – 98 per cent are linked to the Internet, and over 90 per cent provide public access to their

[7] Canada's Children In A Wired World: The Parents' View:
<http://www.media-awareness.ca/english/special_initiatives/surveys/phase_one/parents_survey.cfm>
Young Canadians In A Wired World: The Students' View:
<http://www.media-awareness.ca/english/special_initiatives/surveys/phase_one/students_survey.cfm>

[8] Young Canadians In A Wired World – Phase II, Focus Groups:
<http://www.media-awareness.ca/english/special_initiatives/surveys/phase_two/upload/yccww_phase_two_report.pdf>

patrons. In recent years, the Canadian Library Association (CLA), a national English library association, has taken a leadership role on the issues related to Internet access in public libraries. In Canada, many public libraries have come under fire for offering unfiltered Internet access and have subsequently found their relationships of trust within their communities undermined. Librarians now find their traditional role as protectors of the free flow of information measured against the protection of their patrons, and in particular children, from offensive and potentially illegal online content.

The CLA Statement on Internet Access, encourages libraries to "offer Internet access with the fewest possible restrictions" and to "assume active leadership in community awareness of, and dialogue on, the issues inherent in the *informed* use of this essential, yet non-selective and unregulated medium in libraries."[9]

The CLA developed an initiative, centred on the *Web Awareness* workshop series, in co-operation with MNet, to deliver Internet education in public libraries across Canada. The programme provides professional development for library staff, who in turn raise awareness of Internet issues among those accessing the Internet from public libraries. In response to demand from libraries, MNet produced a *Parenting the Net Generation* workshop to present to the public.

In February 2003 and 2004, the CLA, in partnership with the Media Awareness Network (MNet) and Bell Canada (one of Canada's largest Internet service providers) proclaimed a national *Web Awareness Day.* The purpose of the event was to build public awareness of Internet literacy and of the role being played by Canada's public libraries. To celebrate *Web Awareness Day* libraries around the country promoted Internet literacy through open houses, workshops on safe Internet use and other special events, as well as handing out information pamphlets and other materials for parents. Public libraries used *Web Awareness Day* as a positive opportunity to deliver the message that they are ready to support parents and communities in teaching young Canadians literacy skills for the twenty-first century.

Be Web Aware Campaign. Much work needs to be done in empowering adults to address Internet issues in homes, schools and communities. This is especially true for parents, who are frustrated with what they see as the negative aspects of the technology and with their inability to control what their children are accessing and doing online. If parents are to be effective Internet gatekeepers for their children, they're going to need tremendous advice, guidance and support from the education system, government and industry.

In 2004, Media Awareness Network with Microsoft Canada and Bell Canada, and a coalition of leading Canadian organizations, launched *Be Web Aware* – a national, public education campaign on Internet safety.[10] The goal of the *Be Web Aware* initiative is to raise awareness amongst parents that there are safety issues when their children go online and that they need to get involved. The *Be Web Aware* initiative includes public service announcements (PSAs) on television, radio, print and outdoor media that direct parents to a comprehensive *Be Web Aware* website. The site, developed by Media Awareness Network, is full of information and tools to help parents teach their children to handle the potential risks associated with going online.

Every day, each of us assimilates, evaluates, and controls immense amounts of data and diverse messages in a complex information and entertainment culture. Given this climate, it

[9] Canadian Library Association, Internet Service in Public Libraries – A Matter of Trust. Net Safe/Net Smart: Managing and Communicating about the Internet in the Library, 2001. Available at: <http://www.cla.ca/netsafe/index.htm>

[10] Be Web Aware: <http://www.bewebaware.ca>

makes sense that we expand the notion of what it is to be literate beyond the limits of the traditional areas of reading, writing and numeracy, to include information, visual, and media literacy.

Young people today use technology for entertainment, to learn, to research, to buy and to communicate. Governments, industry, education and library sectors realize that the thinking must change regarding the importance of traditional literacies – not to upstage them – but rather to encompass all the lifelong learning skills that young people require for the management and understanding of information and messages that they receive, create and repurpose.

Christian Möller and Arnaud Amouroux (eds.)

Good Practices for Media Education: Examples from the Canadian Media Awareness Network*

Most experts during the different conferences organized by the OSCE Representative on Freedom of the Media agreed that labelling, filtering and blocking are not suitable means to protect the young from potentially harmful or allegedly unsuitable material on the Internet. Instead, the consensus was that media education in general and the development of Internet literacy is the best way to enable children to deal with whatever content they find online. Or, as Prof. Frederick M. Lawrence put it during the Human Dimension Implementation Meeting in Warsaw 2004: The educated mind is the best filter imaginable.

The goal of media education is to create a media literate individual. It is now widely accepted in education circles that in order to be literate today, children and young people must be able to read, understand and bring critical thinking skills to information in many different forms. Media literacy involves analysis, evaluation, production and critical reflection. These skills are at the heart of a healthy, informed society, and they are increasingly important as young people turn to the Internet as their main source of information.

Today's children are growing up in a rapidly evolving global media environment. A 2001 UNESCO report concluded

* These good practices have been compiled from different presentations of the Media Awareness Network and would not have been possible without the kind help of Cathy Wing, Jane Tallim and Margaret Skok of the Canadian Media Awareness Network.

that a new media landscape and new media order are emerging. Media cultures are changing; information is flowing more freely and the volume of information is expanding; national media markets are being integrated into a global power structure; people from around the globe can now view media from many different places; and the distinction between computers, television, radio, press, books and telephones is dissolving.

In this borderless media world of VCRs, DVDs, satellite TV, and the Internet, children and young people have increasing access to media products from around the globe. Rating and classification systems, legislation and industry codes and guidelines are no longer enough to protect children – particularly as more young people use wireless devices to access the Internet, play video games, watch movies and listen to music. Digital media are forcing a shift in responsibility from statutory regulators toward the individual household.

Nevertheless a strategy on illegal and offensive Internet content should be developed that can include legislation and self-regulation. However, the difficulty of controlling content in a global medium means that awareness, education and knowledge should form the foundations of any approach. The work in Internet literacy should be focused on developing education resources; influencing public policy; and conducting research on young people's Internet use.

Research of the Canadian Media Awareness Network (MNet) showed that young Canadians are heavy Internet users: almost 50 per cent go online for one to three hours each day and 50 per cent are alone most of the time. A significant number indicated they'd been exposed to hateful messages on the Internet. Eighteen per cent said they have come across a website that was really hateful towards someone. Twenty-one per cent of these sites targeted a group of people based on race, gender, religion, language or sexual orientation.

To help young people deal with such Internet experiences and to develop critical thinking and decision-making skills, it is also vital to invest in training teachers and librarians. Anti-racism programmes aimed at educating teachers and students about diversity representation in the media and online hate were funded by the Canadian Government. These programmes included professional development workshops for teachers, classroom teaching lessons and interactive games for students.

An effective media education strategy to address online hate starts with an examination of stereotypes and bias. Teachers and students are encouraged to examine their own cultural biases and preconceived notions. Next they need to understand how stereotypes function in society and popular culture and how negative stereotypes can influence our perceptions of entire groups of people.

An award-winning poster, issued by the Urban Alliance for Race Relations in Toronto, sets the tone for the *Exploring Media and Race* programme by emphasizing how easily false judgements and assumptions about people are made. The poster lists a series of crimes which we connect with the face. At the bottom of the list we discover that this is a photo of the arresting police officer, not the criminal.

To help educators better understand media representation, the key concepts that are at the heart of media education are introduced. The first concept is that audiences *negotiate* meaning. We all bring our own life experience, knowledge and attitudes to the media we encounter. The objective of media education is to help students to step back and ask critical questions about what they're seeing – rather than just absorbing media messages passively and unconsciously.

The next key concept is that all media are constructed. The process of representing people, places and events to viewers involves steps and decisions on who to leave in, and who to leave out. Through representation of minorities, media have the power to grant or deny legitimacy to whole groups of people. The chronic under-representation makes those few minority faces, voices and realities that we *do* see, even more significant. When media depictions of a particular group in society reflect a full range of characters we are less likely to make generalizations about them. Many mainstream media portrayals rely on and reinforce racial stereotypes. Consider the kinds of messages about race and gender promoted in popular youth-oriented genres such as music videos and movies. Even well-intentioned portrayals can still perpetrate stereotypes while reinforcing the concept of "the other".

Another key concept of media education looks at the role of mass media as "big business". It examines how, for example, the demand from lucrative foreign markets for action films, preferably with white action heroes, affects film content and development in North America.

And finally, the key concept is introduced that ideological messages about values, power and authority underpin all media.

Following an examination of how stereotyping and bias in media culture may contribute to racist attitudes and beliefs, teachers and students learn the ways in which hate is expressed on the Net in MNet's second programme *Deconstructing Online Hate*. The educator workshop starts with a series of seemingly innocent Web resources that are in fact fronts for the white supremacist organization Stormfront. When examining hateful content it's difficult to isolate it from the culture of the Internet – in particular kids' online culture. The programme looks at the whole "spectrum" of hateful messages that kids are being exposed to – starting with the cruel satire and tasteless humour sites so popular with young people; moving on to online games that promote degradation and violence as entertainment; and finally, at the furthest extreme, examining websites designed by organized hate groups. The fine line between satire and humour, and intolerance and hurtfulness is addressed by asking participants to decide for themselves whether or not particular Internet sites would be considered as tasteless humour or hate.

Next, participants examine the ways hate groups use the Internet to target young people, through music, clubs, discussion forums and online games. They examine the ways that hatemongers exploit the multimedia capabilities of this powerful, interactive medium, and the clever use of deceptive keywords in meta-tags. They look at how propaganda is used to sway opinion by deconstructing actual hate sites on the basis of wordplay, name-calling, symbols and imagery, religious authority, pseudo-science, nationalism, fear mongering and revisionism.

Participants are led step-by-step through the deconstruction of this revisionist site that is hosted on a US university server. They learn how to authenticate the source of the information by comparing search results on the author, recognizing personal page notations in URLs, and doing a link search to see which organizations link to or talk about this particular website.

Students are encouraged to debate pertinent issues relating to online hate, such as the appropriateness of a university hosting web pages known to contain false and inflammatory information or where the line should be drawn between freedom of expression and indecent or illegal web content. And, of course, the programme helps them understand that at its core, online hate is nothing more than old-fashioned propaganda, wrapped in flashy new packaging.

One of the more ambitious teaching tools in this programme, which is currently in development is an interactive game – Allies and Aliens. In this game players are exposed to varying degrees of prejudice, misinformation and discrimination as they visit websites from other planets – first uncritically, and then with guidance and direction. This resource will allow students to explore the issues surrounding hate sites in an educational and non-threatening manner.

Teaching kids how to assess the credibility of online information is essential because studies have shown that children believe information on a computer screen before they believe something an adult has told them. Almost 40 per cent of teenagers in the MNet survey believe that they can trust *most* of the information they find online.

MNet's *Fact or Folly* programme teaches online authentication skills to teachers and students. MNet has also developed a series of games and learning modules to help students learn to discern fact from fiction in Internet content:

- *Reality Check* is a new classroom resource to teach kids strategies for authenticating online information and detecting bias and stereotyping in Internet content.
- *CyberSense and Nonsense*, is an interactive game on the MNet website where young children learn about authenticating online information in a humorous way. When three CyberPigs stumble across a "We Hate Wolves" website they experience first hand the difference between information on valid, authenticated sites, and sites which are nothing more than the outpouring of emotion and opinion.
- For pre-teens MNet has developed "Jo Cool, Jo Fool" in which students follow a brother and sister team as they surf the Net. Students must decide if the Jos are being cool

> or fools as they make various decisions. When Joseph discovers a homework site while researching human rights he must decide whether to use the information he's found. Kids discover Jo's a fool for accepting the content on this site at face value – it turns out that the Homework Nook is actually a cleverly disguised hate site.

One of the cornerstones of media literacy initiatives – be they governmental or NGO – is to get the materials into communities where they are needed. One way of distributing is the Internet itself. For example, many resources, including teaching lessons on stereotyping, diversity, online hate, authenticating Internet information and many more media-related topics, are available free to download from the Media Awareness Network's website.

Another good practice is a partnership approach engaging not-for-profit, government and industry partners in bringing programmes to schools and the public. This ensures efficient delivery of resources and links to public policy.

National public awareness campaigns with the support of all stakeholders including the media industry, ISPs, government, NGOs, and schools should be initiated to raise awareness of Internet issues among parents, and to get them involved in their children's online activities.

Eventually, the increased profile the Internet offers hate groups may be their undoing. By bringing what used to be secretive and hidden out into the mainstream, the Internet is exposing racist propaganda for what it is – and also providing us with tremendous opportunities to counter this issue.

From taunting and bullying, to hate-related symbols, to hate literature and hate sites we must confront and challenge hate in all its forms and what better place to start this process than in the safe, caring – and respectful – environment of our schools.

Media Awareness Network Internet Literacy Resources. Since the mid-1990s, Media Awareness Network has pioneered the development of Internet literacy resources for use in schools, libraries and communities. The following is a sampling of productions, many of which are available free on the MNet website (http://wwww.media-awareness.ca):

i) **Race and Media**

Media Stereotyping: This online resource includes Portrayals of Aboriginal Peoples in the Media, and Ethnic and Visible Minorities in Entertainment Media, which examine why, and how, stereotyping is used as a convention by media producers and writers.

Exploring Media and Race: A professional development workshop for teachers about diversity representation in the media.

Classroom teaching lessons: Perceptions of Race and Crime, The White Screen, Too White: Minority Representation in the Media, Diversity Audit, Bias in the News, and Ethnic and Visible Minorities in Entertainment Media.

ii) **Online Hate**

CyberSense and Nonsense: An interactive game for children, with an accompanying teachers' guide, in which surfing CyberPigs learn about prejudice, racism and hate on the Internet.

Challenging Online Hate: An online resource that explores the motives and targets of online hate, and suggests ways to safeguard children and teens.

Deconstructing Online Hate: A professional development workshop for teachers that examines the spectrum of hateful messages on the Internet.

Classroom teaching lessons: Free Speech vs. the Internet, Challenging Hate Propaganda, Thinking about Hate, Understanding Online Hate, Techniques on Hate Sites. Allies and Aliens: An interactive online student game, with an accompanying teachers' guide, to help teens understand and recognize the often subtle language and tactics of hatemongers.

iii) **Authentication of Information**

Fact or Folly: An online resource that teaches online authentication skills to teachers and students.

Reality Check: An interactive module to teach teens strategies for authenticating online information and detecting bias and stereotyping in Internet content.

Jo Cool or Jo Fool: An interactive online game, with an accompanying teachers' guide, where pre-teens learn to make informed online decisions in various Internet environments.

Classroom teaching lessons: Deconstructing Web Sites, A Tale of Two Cities, Hoax? Scholarly Research? Personal Opinion? You Decide!, ICYouSee: A Lesson in Critical Thinking.

iv) **Electronic Privacy and Marketing**

Privacy Playground: An interactive game for children, with an accompanying teachers' guide, in which CyberPigs learn about online marketing, and about protecting their privacy as they surf the Internet.

Kids for Sale: An online resource that examines marketing and privacy concerns on the Internet.

Classroom teaching lessons: Online Marketing to Kids: Protecting Your Privacy, Online Marketing to Kids: Strategies and Techniques, What Students Need to Know about Freedom of Information and Protection of Privacy, Who Knows: Your Privacy in the Information Age.

Marcel van den Berg and Pascal Hetzscholdt

The National High Tech Crime Center in the Netherlands

Tackling high-tech crime is a vital concern for the Dutch Government

The Dutch ministries of Justice, Interior and Kingdom Relations, Economic Affairs and the Dutch National Police combined their expertise to co-ordinate (inter)national investigations regarding high-tech crime. This National High Tech Crime Center (NHTCC) is based at Schiphol Airport – Amsterdam, the Netherlands.

In co-operation with its national and international partners regarding high-tech crime, terrorism and critical infrastructure protection the main objectives of the NHTCC are to exchange and co-ordinate information and intelligence to combat serious ICT crime.

The partnership is designed to provide early warning of and a swift and effective response to serious crimes using or directed against ICT – collectively known as high-tech crime. One specific focus will be the consequences that high-tech crime can have for Dutch society in general and for vital information infrastructures in particular. These include the computer systems at Schiphol Airport and computer networks at major financial institutions or in the energy sector.

Tackling high-tech crime is an integral part of the Dutch Government's drive to put concrete effective measures in place to tackle ICT-related crime. This is a goal that calls for a proactive approach, and it can only be achieved by bringing together the experience, knowledge and expertise of the various organizations involved. This is why it is so important at both the national and the international level for government and the private sector to collaborate.

The general manager of the National High Tech Crime Center (NHTCC), Nienke van den Berg stated: “Our society is now highly dependent on ICT. That is why it is imperative that we make sure criminals or terrorists cannot hack into our company networks or misuse government information. But if things should ever go wrong it will be essential to take swift action to limit the damage as far as possible, enable public and private bodies to get back to work, and round up the suspects. And that is precisely what the NHTCC has been created to do.”

The multi-agency approach of the NHTCC is a new method in combating organized crime: governments, private companies and law enforcement are working closely together to prevent criminals and criminal organizations from ICT abuse. An announcement is expected in the near future about how members of the public can turn to the Government for advice on the potential for serious high-tech crime or to report criminal and/or terrorist ICT incidents. This is vital if the Government is to take swift action following such an incident or while it is still going on – and, in particular, to forestall major ICT problems in the future.

Access to Networks and to Information

Dejan Milenković

Freedom of Information

Freedom of information, usually understood as freedom of access to information held by public authorities, is today widely recognized as an essential human right.[1] This is usually defined as each person's right to request and receive relevant information of public interest from the power holders (i.e. from public authorities). This should offer insight into the actions of people who were democratically elected to perform the functions of power and conduct other public affairs on behalf of the people.[2] To put this simply, it is about the right of any person to have access to data held by public bodies and to acquire information about the actions of those with public authority.

The modern age, and especially the second half of the twentieth century, has become complex beyond our wildest dreams – from living and working in megacities, to global telecommunication networks and the Internet. The complexity of the modern world is reflected in the soaring number of sources which generate enormous quantities of information by the minute. In this sense, the world today differs from past ages when the "number of mines and factories" defined the level of social development. In contemporary society information is the most important development resource.

Throughout the long history of human society, information often represented one of the essential instruments in the

[1] See Toby Mendel, *Freedom of Information (A Comparative Legal Survey)* (New Dehli: UNESCO, 2003), 3.

[2] See Zoran Jelic, *U susret zakonskom regulisanju slobodnog pristupa informacijama,* Ekonomika, Belgrade, No. 3/2002.

hands of those in power. Information has been – and still is – a key to exercising power over people, because if the actions of those in power remain secret, human rights and freedoms are considerably curtailed and citizens are prevented from taking an active part in complex social processes.[3]

"Secrecy" often represents the only way to remain in power, concealing illegal and improper actions of top state officials, wastefulness and corruption and other features inherent to an undemocratic and closed society. Even democratic governments tend to attend to their affairs far from the public eye.[4] This opinion predominated during the 1940s (and to be honest is still evident even today). It was clearly expressed by the American writer Walter Lippmann, who thought that an elected official was responsible to his or her office and not to the voters: "Where mass opinion dominates the government, there is a morbid derangement of the true functions of power." On the other side of the Atlantic, the British system of parliamentary democracy was based on the assumption that the legislature put government actions to the test, not the public. According to Walter Bagehot, the famous theoretician of British parliamentary government, democracy could only work "if its real rulers are protected from vulgar enquiries."[5]

Contrary to these opinions, freedom of information in today's world represents a fundamental prerequisite for openness and transparency about the actions of public authorities and bodies and about any issues relevant to the public that are related to these bodies.

It is rightfully stressed today that information is the "oxygen of democracy".[6] Accepting free access to information represents a turning point in the transformation of a State and its administration from an apparatus of repression and power towards a system geared towards public service. Free access to information broadens the field of public information and guarantees the exercising of a human right that provides citizens with the resources with which to shape and express their sovereign political will, thus making them better equipped to monitor state powers and administration.[7]

Freedom of information relates "only" to access to information which is held by public authorities or bodies in the widest sense of these terms. In defining "public body", the emphasis is on the services rendered by these authorities or bodies rather than on their formal designations. It therefore follows that even private persons or organizations could, in certain cases, be considered to hold obligations regarding freedom of information. Today it is a recognized principle that the information held by public bodies is in the public domain belonging to all citizens, and therefore it is their obligation to ensure free access to this information.

II

The right to free access to information evolved out of the right to having an opinion and expressing it, which led on to the right to be informed. Today it is a fundamental human right

[3] See Dejan Milenkovic, "Access to Information as a Fundamental Human Right", in Stevan Lilic and Dejan Milenkovic (eds.), *Free Access to Information* (Belgrade: YUCOM, 2003), 44–48; Richard Calland and Alison Tilley (eds.), *The Right to Know, the Right to Live – Access to Information and Socio-Economic Justice* (Cape Town: Open Democracy Advice Centre, 2002).

[4] See Dejan Milenkovic, "Access to Information as a Fundamental Human Right", in Stevan Lilic and Dejan Milenkovic (eds.), *Free Access to Information* (Belgrade: YUCOM, 2003), 44.

[5] Article 19, *Freedom of Information (Training Manual for Public Officials)*, chapter one: What is Freedom of Information? (London: Article 19, 2004), 10.

[6] See *Pravo javnosti da zna*, Article 19, Crnogorski helsincki komitet za ljudska prava, Cetinje, January 2003, 7.

[7] See Andrew Puddephatt, "Flow of Information Empowers Ordinary People", in Richard Calland and Alison Tilley (eds.), *The Right to Know, the Right to Live (Access to Information and Socio-Economic Justice* (Cape Town: Open Democracy Advice Centre, 2002), 10–11.

enshrined in important documents and declarations of international organizations. These include the United Nations' Universal Declaration of Human Rights (Article 19) and International Covenant on Civil and Political Rights (Article 19), the Council of Europe's European Convention on Human Rights (Article 10), and the American Convention on Human Rights (Article 13) of the Organization of American States.

Based on these essential documents from these international organizations and others, concrete international standards have also been developed. The Council of Europe Committee of Ministers adopted Recommendation R 81 (19) on the Access to Information held by Public Authorities and Recommendation R 2002 (2) on Access to Official Documents. These represent a framework within which Member States should promote, secure and protect free access to information in their legal systems.[8] The Inter-American Commission on Human Rights ratified the Inter-American Declaration of Principles on Freedom of Expression in 2002, which also stipulates that free access to information is a fundamental right of every individual.[9] The African Commission on Human and People's Rights adopted the Declaration of Principles on Freedom of Expression in Africa, which also contains a separate section on freedom of information.[10]

III

National legislation also made a considerable contribution to establishing freedom of information. In Sweden a law granting access to government information was enacted back in 1776. Public access law also developed early on in the North American state of Wisconsin. In 1849 statutes were adopted which provided for public access to the meetings and records of county government. In South America a statute concerning freedom of information was enacted in 1888 in Columbia.[11]

Yet the age of free access to information only really gathered momentum in the 1960s when the Freedom of Information Act was passed in the USA in 1966. In the thirty years that followed, the right to free access to information was acknowledged in national legislations all over the world, in accordance with the principles of the Welfare State and the concept of administration as a system of social regulation of processes in society.[12] In some countries free access to information has become a constitutional right.[13]

International and regional rights and standards demonstrate that legislation in this field is based primarily on the following principles[14]:

1. There should be maximum disclosure of information held by public authorities, which presumes that access to information is the rule and denial of access the exception.
2. Certain expressions such as "information", "document", "public authorities" or "public bodies" must be broadly defined.

[8] These Council of Europe documents are available at <http//www.coe.int>

[9] 108th Regular Session, October 19, 2002.

[10] 32nd Ordinary Session of the African Commission on Human and People's Rights, 17–23 October, 2002, Banjul, the Gambia.

[11] See Vladimir V. Vodinelic, Sasa Gajin, *Sloboda pristupa informacijama (ustavno jemstvo I zakonske garancije)*, Fond za otvoreno drustvo (Belgrade, 2004), 11.

[12] For example USA. (1966), Canada, Australia (1982), New Zealand (1982), Portugal (1993), Denmark (1970), Norway (1970), Greece (1999), Ireland (1997), France (1978), Holland (1991), Poland (2001), Albania (1999), Czech Republic (1999), Slovakia (2000), Bosnia and Herzegovina (2000), Romania (2001) (source: David Banisar, Privacy International, July 2000 + FOIA news).

[13] Albania, Austria, Belgium, Canada, Philippines, Portugal, Slovakia, South Africa, Serbia and Montenegro (source: David Banisar, Privacy International, July 2000 + FOIA news).

[14] See *The Public's Right to Know – Principles on Freedom of Information Legislation*, Article 19, June 1999 <www.article19.org>; The Committee of Ministers of the Council of Europe: Recommendation R 81(19) on the Access to Information held by Public Authorities, Recommendation R 2000 (13) on a European Policy on Access to Archives or Recommendation R 2002 (2) on Access to Official Documents, at <www.coe.int>

3. Every member of the public has the right to access information held by public bodies and these should ensure maximum ease of access without any unnecessary formalities.
4. The public authority may deny access only under certain strictly defined conditions. If access is denied, the reasons must be stated in writing.
5. Legitimate grounds for refusing access to information must be stipulated in the law. These are restricted mainly to state, official or military secrets; privacy; public health and safety and national security; information relating to law enforcement; and information that could jeopardize commercial interests or influence the independence of courts. However, information that falls into these categories must be disclosed when the reasons justifying exemption cease or after a time limit has expired.
6. If the application is rejected, the applicant has the right to appeal to a higher, second instance body, which will reconsider the original decision. Access to information is often connected with references to Ombudsman institutions, in case the applicant believes his or her right to freedom of information to be infringed. In certain countries there are also special commissioners in charge of access to information.
7. In order to ensure transparency and openness, public authorities are obliged to publish key information on the Internet and in periodical and annual reports (information on their activities and organizational structure, certain decisions etc.).
8. Meetings and conferences held by public authorities must be open to the public (not only to journalists but also to all members of the public).

9. There should be no charges or just minimal fees for providing information.

10. Whistleblowers – public officials who disclose information about wrongdoing – must be protected from legal or any other sanctions if the publication of this information is in the public interest.

IV

The importance of freedom of information demonstrates that a democratically elected government needs to prove to citizens that it is fulfilling its mandate in its daily work. Centuries of experience have revealed that power corrupts, especially if no limits are imposed. Access to information sheds light on the actions of those in power. "Since power is like a fungus [and] it is in darkness that it feels most at home and thrives", illumination is vital.[15]

Moreover, without free access to information, citizens are deprived not only of being able to scrutinize the actions of people they voted into power, but also of the opportunity to contribute to the public interest and common good. This is crucial in order to establish genuine democracy, in which power is vested in the people, and to build the institutions of an open, free and civil society which depends on self-organization and self-determination.

When discussing democratization today we think primarily of transition countries, and expect this process to be based on the principles of social welfare, rule of law, transparency and open society. This presupposes attaching ever greater importance to the public sphere. It represents a field of tension between politics and private persons who, while

[15] Miroljub Radojkovic, *Za slobodan pristup informacijama*, Prizma, Centar za liberalno-demokratske studije, No. 4, April 2002, 29.

enjoying their rights and freedoms in private, press for these rights and freedoms to be fulfilled in politics.[16]

Because freedom of information is acknowledged as a basic human right, citizens today can find out how a department of local government is spending its budget; how tuition fees at a university are calculated; how many members of an ethnic community attend a vocational school in a particular city; or the salary of a public official. People can also find out information about whether a mayor used his official car for private purposes at the taxpayers' expense; who travelled to the Olympic Games in Athens on the State's behalf and why; if and when the country's President and the Chief of General Staff met, and so on.

We are talking here about citizens being able to express, protect and satisfy their interests because they have access to information and can enjoy the advantages of the "third generation" of human rights and freedoms. It is this right that empowers citizens to become the fourth power, keeping an eye on those whom they entrusted with government functions in elections.

V

Freedom of information is a right that has evolved from freedom of expression. In this context, this obviously holds enormous importance for the media as well. But numerous issues that would interest individuals, families or NGOs do not necessarily represent information relevant for society as a whole. Most of this type of information would therefore not be of interest to the media. This does not mean, however, that the "seventh power" does not benefit from free access to information. The journalist who investigates reports on maladministration or corruption in public bodies can request information such as court decisions, or reports on budget expenditures in order to establish whether or not officials have abused their authority. It is therefore of utmost importance that the media have access to information of public interest. "If investigative journalism has to be based on rumours rather than verifiable facts, journalistic practice risks becoming defamatory, … and the public is unable to judge the competence of the administration and the country's leadership."[17]

After the fall of totalitarian non-democratic regimes, some journalists and media professionals in these regions now seem to view freedom of expression as an absolute right. Violence by journalists occurs if they report on events and persons untruthfully and incompetently and "brainwash" readers, spectators or listeners, aiming to influence their political views. There are cases when journalists quote "unnamed sources" and in this way spread false and sensational information which jeopardizes public security, encourages disorder and crime or besmirches the reputation and honour of others. On the other hand, there is violence against journalists. This is when journalists are pressurized to report in a way that is unobjective and false, favouring a political group or individual. This also occurs when, for instance, journalists are denied access to information or to the scene of an event.

If a legal framework for freedom of access to information exists, journalists can check information provided by "unnamed sources" working for public authorities. If this right is protected by law, a journalist can no longer be denied access to information without a legitimate reason. Thus, freedom of information is also a way of safeguarding the correctness and

[16] Ibid.

[17] Article 19, *Freedom of Information (Training Manual for Public Officials)*, chapter six: Who are the Requesters? (London: Article 19, 2004), 63.

truthfulness of information in the media, and in this way contributes to this fundamental principle of journalists' codes of ethics all over the world.

VI

Freedom of access to information is also a vital weapon in the battle against corruption.[18] One efficient mechanism in this fight, which is normally included in the law on free access to information, is the protection of whistleblowers – insiders who disclose hidden information. Individuals who have disclosed in good faith an illegal or unlawful act or corruption by a higher civil servant or public official have the right to be protected from any legal, administrative or employment-related sanctions.[19] Whistleblowers should also be protected if they have violated their legal and contractual obligations by disclosing certain information, provided that this is done in good faith and in the belief that the information was true and related to a serious matter of public interest.[20]

For years, public officials have avoided public expression of doubts about the politics and actions of state authorities and public administration. Those who did take this step tended to be criticized rather than applauded by their colleagues. This reflects a special form of "organizational ethics" which plays a very important role for public officials. These organizational ethics require loyalty and acceptance of institutional tactics and politics, offering in return "friendship, security, promotion and mutual adventure in a mutual undertaking". These ethics prevail in the majority of organizations and in state organizations in particular. Organizational or bureaucratic ethics often require "turning a blind eye" and unreserved conformity from members of the organization. As a result, public officials, regardless of whether they are truly loyal to the boss or are just afraid of losing their job or reputation, tend to show emphatic loyalty rather than adopting a critical attitude to difficult issues. In such a system, “bright” people who question issues or who bother others, are not the “right” people.[21]

This system has been gradually changing, in part because of the pressure to broaden access to information. Nevertheless, in many countries the attitude still prevails that provisions relating to “an insider” should not be included in the law on free access to information. However, with freedom of information legislation, a conscientious public official can be a “hidden insider” or “unnamed source”, without risking arbitrary dismissal, pressure to resign, or loss of salary.

VII

The Internet has changed working and communication methods in all areas of life. Today the possibilities of the Internet appear to be virtually unlimited. From the point of view of freedom of access to information held by public institutions, the Internet is ideal, providing the cheapest and quickest instrument available. Detailed information about the work of state institutions can be placed on websites. It should not be forgotten that freedom of access to information presumes that public institutions are meeting their obligation to publish information about their work. This should include details of their objectives, activities, organizational structure, expenses and sources of financing, decisions and policies that affect citizens’ lives, and the reasons behind these decisions. It could also

[18] See *Antikorupcijski zakoni: Iskustvo Slovenije I izazovi Srbije (Slobodan pristup informacijama I sukob interesa)*, Vladimir Goati, *Uvodno izlaganje*, Transparentnost Srbije, Belgrade, 2004, 1.

[19] Vladimir V. Vodinelic, Sasa Gajin, *Slobodan pristup informacijama (ustavno jemstvo I zakonske garancije)*, Fond za otvoreno drustvo, Belgrade, 2004, 29–30.

[20] Article 19, *Freedom of Information (Training Manual for Public Officials)* (London: Article 19, 2004), 29–30.

[21] See Milan Markovic, “Pravna pitanja reorganizacije uprave u Srbiji I Crnoj Gori” (doctoral thesis), Podgorica, 1997, 359–60.

include information about requests, complaints, letters, suggestions and other actions that members of the public may take relating to these public institutions. Naturally, websites and the Internet are an ideal way of fulfilling these obligations.

There is a vital connection between freedom of access to information held by state institutions and the Internet. This is especially true because data processing is now one of the fundamental functions of the State. Effective data processing is an important precondition for the lawful, efficient and economical fulfilment of the State's role. In many countries, especially those in transition, a key issue in reforming the State relates to realizing the e-Government programme, or e-Administration, as part of the overall process of digitalization of government services.

To conclude, I would like to repeat that the right to free access to information is vitally important for the following reasons: 1) as a crucial human right, necessary in order to respect other rights; 2) to make the actions of powerful bodies transparent and accountable; and 3) to enable public participation in social policies and government decision-making. Yet the right to free access to information is only effective if it is legally enshrined and enforced in accordance with international standards. The Internet as the technical infrastructure to disseminate information easily can assist state authorities in fulfilling their obligations.

Colin Guard

The Internet Access and Training Program in Central Asia

The Internet Access and Training Program (IATP) is an international assistance programme funded by the Bureau of Educational and Cultural Affairs (ECA)[1] of the US Department of State. It is administered by IREX in Central Asia (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan); the Caucasus (Georgia, Armenia, Azerbaijan); and Western Eurasia (Ukraine, Moldova)[2]; and by Project Harmony in the Russian Federation.

IATP is a public diplomacy programme, originally intended as a cost-effective follow-on to US Government-funded academic and professional exchanges, giving alumni the chance to maintain contact with their US colleagues and friends after returning to their home countries. Since its launch in the mid-1990s, IATP has expanded significantly beyond its mission to serve alumni, who now constitute only between one and five per cent of the total user base in each of the countries of Central Asia. As recently as the end of 2003, alumni constituted over five per cent of the user base in the region; their decrease as a proportion of users has been the result of a large increase in the total number of users while the number of alumni has increased only slightly.

[1] The former United States Information Agency (USIA), merged with the Department of State and renamed in 1999.

[2] Until July 2003 IREX administered IATP in Belarus as well; after the Government of Belarus rejected IREX's application for renewal of registration, programme administration was transferred to the United Nations Development Programme and the United States Embassy in Minsk.

As an ECA-funded public diplomacy programme, IATP is directed toward enhancing ties and increasing mutual understanding between the people of the United States and the people of Eurasia. It is not intended primarily as a development programme, but its impact on Internet development in Central Asia has been significant, for two reasons. First, in order to carry out IATP's public diplomacy mission in Central Asia, it has been necessary to make an investment in local infrastructure and human capacity. In many cities, IATP has been the first customer of the local Internet service provider (ISP), often co-ordinating efforts and expanding in tandem. In most of the region, electricity and telephone services are unreliable, requiring significant improvements before it is possible to open an access site. Only a very small portion of the population has Internet access, ranging from roughly one per cent in Turkmenistan to ten per cent in the larger cities of Kazakhstan and Kyrgyzstan; correspondingly, levels of computer and Internet literacy are low. Therefore, it is necessary to train users in basic computer and Internet use before it is possible to conduct any public diplomacy with them using the Internet, whether by e-mail, chat rooms, or websites. All of IATP's efforts in creating the conditions necessary in order to conduct public diplomacy online have a direct effect on Internet development.

Second, IATP has the largest footprint of any Internet-related programme in Central Asia, with 65 Internet access sites covering nearly every major city in the region, training between 4,000 and 5,000 individuals per month and providing free Internet access to 25,000 to 30,000 people per month. In addition, the programme provides dialup Internet connections to more than 1,000 alumni and NGO leaders at their homes and offices. The programme's five web servers host more than 4,000 websites created by Central Asians, accounting for a proportion of the total web content in each country ranging from 12 per cent in Kyrgyzstan to 80 per cent in Turkmenistan.[3] Such a large-scale programme, which by itself accounts for the majority of the free, public Internet access and training in the region, cannot but have an impact on the general level of Internet development. Rare is the qualified system administrator or web designer in Central Asia who has not at some point taken advantage of IATP's facilities and services. Local Internet cafés benefit more from the increased number of Internet-literate customers who have been trained at a nearby IATP access site than they suffer from the competition from a free provider; there have been several instances in which the number of for-profit Internet cafés in a particular city has increased after the introduction of IATP.

IATP has been an extraordinarily successful programme in Central Asia, both in terms of furthering the cause of public diplomacy and in terms of bringing improvements to the lives of Central Asians. To cite just a few examples:

- Muslim leaders from Kazakhstan and Uzbekistan have returned home after trips to the United States to report to large online audiences of young people that the United States is not an enemy of Islam, and that in fact millions of Muslims are able to practice their religion there freely. These online chats, and the media coverage resulting from them, have done a great deal to address inaccurate images and representations of the US in the region.
- Young entrepreneurs in Turkmenistan have used IATP's Internet access to obtain technical information on the

[3] Measured in gigabytes as a proportion of the total web content hosted on the territory of each country (not as a percentage of the number of websites, and not as a percentage of the total content on a particular country domain, e.g. .kg, .tm, which can be hosted physically anywhere in the world). Information is updated monthly through an informal survey of the technical staff of the web hosting companies in each country.

satellite television packages available in the country, which makes it possible for them to set up dishes and receivers for their customers. At least two satellite TV installation companies have been founded as a direct result of IATP, providing jobs for the young people who run them and alternative sources of information for their customers. Broadcast television in the Republic is monopolized by the four government channels.

- Disabled people have found in IATP an outlet for their talents and energies, in societies that still by and large stigmatize physical and mental disabilities. Not content to equal the accomplishments of their peers, some disabled users have gone beyond full participation in the programme in the form of online chats and authoring sophisticated websites to actually teach courses to non-disabled users. Disabled IATP users are typically more productive than the general user community, perhaps because the local IATP access site is one of the few places where they feel they can reach their full potential.
- A radio station in isolated Naryn, Kyrgyzstan, in the mountainous south-east of the country, uses the local IATP access site to obtain news, which it then rebroadcasts to the surrounding region. The only other source of information in the area is print media; newspapers are usually one to two weeks late in arriving.
- Journalists in several countries in Central Asia have used a series of IATP-hosted online chats to compare notes on election-related activities and coverage, both before and after elections. With print and broadcast media firmly under the control of governments, the Internet is the only way that journalists can learn what is really going on in other regions of the country.

These stories and others can be found on the IATP Central Asia website at http://www.iatp.centralasia.net. IATP's experience has not been an unbroken string of successes, however. The difficulties and unintended consequences encountered by IATP may be a useful object of study for anyone involved in Internet development in the region. Following are some observations, mixed with practical recommendations.

Interestingly, although IATP's purpose is to improve communication between Central Asia and the United States, it has also had the effect of improving communication between Central Asia and Russia. Russian is still the lingua franca of Central Asia, used by Turkmens to communicate with Tajiks and by Kazakhs to communicate with Uzbeks. The Russian-language content available on the World Wide Web, while only a tiny fraction by comparison with English-language resources, still dwarfs the amount of content available in any of the Central Asian languages. While IATP's web content development efforts have made progress in helping local languages catch up, Russian-language websites based mostly in Moscow are the source of the majority of content that is of interest and accessible to Central Asians. Information flows in the other direction, too: 85 per cent of the hits on the website of the National Library in Kazakhstan, hosted by IATP, originate from Russia. Russia is the source of the bulk of the content and the bulk of the web surfers in Eurasia. This is expected to remain the case in the intermediate term, but IATP's large-scale web content development in local languages can be expected to reach a critical mass in the next few years, at which point Central Asian users will be able to switch from Russian search engines and web-based e-mail providers to local ones.

Programmes to develop basic Internet literacy and provide infrastructure are generally uncontroversial even in States where there is a high degree of government control of information.

In fact, in all five former Soviet republics of Central Asia, official government policy calls for an increase in the number of computers available to the public and improvements in Internet infrastructure. Programmes to improve infrastructure and raise Internet literacy meet with little resistance from governments; whereas direct co-operation with political opposition and pressure on policymakers can result in problems with the authorities. There is an argument to be made for separating programmes dedicated to infrastructure and literacy on the one hand from programmes devoted to policy and political liberalization on the other. The former can do their work quietly and without public controversy, laying the long-term foundation for healthy civil societies and participatory democracy. The latter must be backed up by powerful governments and/or multilateral organizations that have leverage in negotiations with host governments. Combining the two aspects in one programme and/or organization can result in a situation wherein political difficulties resulting from work with opposition can jeopardize parallel efforts in basic literacy and infrastructure.

The economic policies of Central Asian governments have been an important but uncontrollable factor determining the sustainability of the programme. In Turkmenistan and Uzbekistan, registration of both businesses and NGOs has become progressively more difficult, new restrictions are continually imposed on trade, taxes are regularly increased, and new regulatory requirements are frequently imposed. As a result, incomes in both countries have been shrinking steadily for several years. In this environment, it becomes impossible to find new, local sources of funding. Fee-for-service schemes become unworkable as the disposable income of the population decreases. Internet cafés close, leaving IATP as the only source of the Internet, free or otherwise, in many cities. In a growing economy, IATP's investments are profitable, as trainees obtain jobs at Internet cafés and even start their own Internet cafés, but in a shrinking economy, IATP's investments are cancelled by the counterproductive economic policies of the government. Internet development alone does not affect government policy; what is required is pressure from governments and multilateral organizations that have leverage.

Internet development is a chicken-and-egg problem. Without web content that addresses local needs and interests, users have little incentive to get online. But without an Internet-literate population with access, there is no audience for web content developers to target. Therefore efforts to develop the Internet must be both comprehensive and large-scale, training both creators and consumers and providing an infrastructure for access. If a single element is missing, the network effect is lost and development is not sustainable.

Education, in order to have a quick and measurable impact on development, should not be excessively theoretical. Training in IATP is obsessively output-oriented. For example, intermediate courses in web design require all participants to arrive on the first day of training with the complete text and photos in paper form that they intend to publish online. By the end of the course, each trainee actually publishes a website either individually or as part of a group. Web training is therefore not held in a vacuum with no real-world consequences. Participants learn web design in order to do web design. This system was developed for the purpose of raising Internet literacy as quickly as possible to the point where Central Asians are able to participate effectively in public diplomacy, but the lesson is useful for more general development purposes as well. Training without a goal cannot be expected to reach a goal.

Jelena Surčulija

Experiences from South-Eastern Europe

One of the aims of the first OSCE workshop on Freedom of the Media and the Internet, held in Vienna in November 2002, was to target the most important issues relating to the Internet in the OSCE participating States for the upcoming Amsterdam conference in June 2003. The topics raised by the participants, who were mainly from the European Union and the United States of America, were generally related to the content of the Internet and included child pornography, cybercrime, intellectual property and anti-Semitism. My concern was that most OSCE countries outside the European Union, United States of America and Canada have more "basic" problems which should also be addressed at the conference like access to the Internet and still existing state monopolies in telecommunications sectors.

Access to a network is a must for access to online information. In South-Eastern Europe, the number of individuals using the Internet is still very low, although it is rapidly increasing. The International Telecommunications Union's (ITU) statistics from the year 2003[1] show that there were 190,190,000 Internet users in Europe. Out of this number there were 39 million users in Germany and more than 25 million in the United Kingdom, but only 30,000 in Albania and around 100,000 in Bosnia and Herzegovina and in Macedonia. The European average in 2003 was 2,388 users per 10,000 inhabitants. Northern European countries have more than 5,000 users per 10,000 inhabitants, which means that more than 50 per cent of the population has Internet access, while in South-Eastern European countries it is only in Slovenia that over 37 per cent of the population goes online. The percentage falls the further south-east we travel. Croatia was closest to the European average with almost a quarter of the population using the Internet. In Bulgaria and Romania this dropped to around 20 per cent, but in Albania there were only 97.63 users per 100,000 inhabitants – less than 1 per cent of its population. In 2003 the percentage of the population using the Internet was only 2.6 in Bosnia and Herzegovina, nearly 5 per cent in the former Yugoslav Republic of Macedonia and almost 8 per cent in Serbia and Montenegro.

These examples demonstrate how the countries in South-Eastern Europe are at very different stages of development. Slovenia is a European Union Member State so the EU regulatory regime applies there. A survey recently published in the Bulgarian daily newspaper *Sega*, citing data from Alpha Research polling agency, stated that more than three-quarters of the Bulgarian population have never used the Internet, and 23 per cent does not know what the word means. Bulgaria is a European Union candidate country. The same research states that 77 per cent of the country's population, numbering eight million, has never been online. Reuters reported a statement in May by the Bulgarian Telecommunications Minister that only four per cent of Bulgarian companies use the Internet in their daily work and that Bulgarian schools had only one computer for every 200 students.[2] This last example clearly demonstrates the importance of spreading computer literacy and widening the opportunities of access to networks in the region.

[1] <http://www.itu.int/ITU-D/ict/statistics/at_glance/Internet03.pdf>

[2] The entire article may be found at: <http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=6640128>

The twenty-first century is often described as the era of the Information Society. The WSIS Declaration of Principles[3] defines the Information Society as "a society where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and people to achieve their full potential and improve their quality of life in a sustainable manner." The ITU World Telecommunications Development Report 2003[4] defines types of information and communications technologies (ICT) that help us live in such a society. The report makes a distinction between radio, television and fixed telephones, which are often considered to be "old ICTs", and the "new ICTs" that are mobile telephones, personal computers (PCs) and the Internet. Most of the developing nations, including many countries in South-Eastern Europe, tend to have data on the "older" ICTs, while most of the developed nations focus on the newer ones. New ICTs enable instantaneous exchange of information, but without access to these, many people around the world are still excluded.

From State Monopolies to Convergence. "The European telecommunications sector has historically been characterised by a strong public sector monopoly tradition together with an industrial policy of creating 'national champions', often run in conjunction with postal services. The monopoly environment began to change in the early 1980s, with privatisation and the introduction of limited competition in some Member States. The development was primarily driven by the increasing application of information technology in the telecommunications sector, which offered the potential to revolutionise the industry."[5] The first phase of Community policy was initiated in 1984. The aim of this Community strategy was to develop common lines for the telecommunications sector. A second phase of Community policy was initiated in 1987 and culminated in the liberalization of all telecommunications services and networks by 1 January 1998. The main direction of the common telecommunications policy has been set by the consultative process initiated by the Commission in 1987 and by key resolutions adopted by the Council and European Parliament, and by the European Court of Justice. The Commission's White Paper on Growth, Competitiveness and Employment, with the full political support of the Council, has placed the Union's telecommunications policy at the heart of its general policy. In terms of opening up the market there are three instruments which have been used to liberalize telecoms in the European Community:

- Progressive liberalization of a former monopoly sector
- Accompanying harmonization measures
- Competition rules

The convergence of the telecommunications, media and information technology sectors means that a single regulatory framework should cover all transmission networks and services. The European Union has already prepared a regulatory framework that consists of the Access Directive, Authorisation Directive and Framework Directive. In addition there are specific directives on universal service, privacy and electronic communications, to establish a framework for electronic signatures and on the re-use of public sector information.[6] The intention of

[3] World Summit on the Information Society (WSIS) Declaration of Principles.

[4] International Telecommunications Union, *World Telecommunication Development Report 2003 – Access Indicators for the Information Society*, Executive Summary, December 2003, 8.

[5] European Commission <http://europa.eu.int/information_society/topics/ecomm/all_about/history/index_en.htm>

[6] A full list of legislation in force concerning information technology, telecommunications and informatics may be obtained at <http://europa.eu.int/eur-lex/en/lif/reg/en_register_132060.html>

the European Union is to separate the regulation of transmission from content regulation. As a result, the new regulatory framework does not cover the content of services delivered through electronic communications networks, such as broadcasting content, and financial and information society services.

Initiatives in South-Eastern Europe. South-Eastern Europe lags behind the European Union in the transformation from an industrial to an information society. In the 1990s, telecommunications sectors started developing in just a few countries in South-Eastern Europe. Many countries are still at the very beginning of the demonopolization and liberalization process, which puts them almost twenty years behind the European Union States. There are various reasons for the delay, but the main causes are economic crisis, effects of war devastation in some countries in former Yugoslavia, a lack of state strategies for the development of Internet technologies, unfavourable tax and customs policies, and a ruined and/or old-fashioned infrastructure. Further reasons include a lack of initiative and shortage of competent human resources. As a result, one of the first steps forwards should be to create a proper legal framework for the telecommunications sector. Legal certainty is necessary for the further development of the sector, especially to attract investments in networks which would provide conditions for wider access to the Internet and other telecommunications services.

The initiative for the development of the Information Society in this region of Europe occurred within the scope of the Stability Pact for South-Eastern Europe. In October 2002 the countries of South-Eastern Europe signed the eSEEurope Agenda for the Development of the Information Society[7] in Belgrade. This verified the responsibility of these countries in the region to develop the proper environment for an Information Society for all. Governments should play the crucial role by taking definite action based on the positive experiences of the eEurope and eEurope+ processes.

The governments of South-Eastern Europe agreed to establish an institutional and legislative framework for an ICT-based society, to promote the liberalization and privatization of the infrastructure for electronic communications and to encourage regional activities through joint e-Governance, e-Learning, civil society and non-governmental organizations. In addition, governments recognized that building the Information Society was essential for the further development of the region, and vital in order to close the gap between South-Eastern Europe and the European Union, and between the region and the rest of the world. The governments acknowledged that building and developing the Information Society is the only path towards the European Union for the countries in the region. Each signatory country, and member of the Stability Pact, has associated itself with the eEurope process, thus agreeing to take concrete action and especially to:

- Adopt policies and strategies to develop the Information Society, particularly the regionally co-ordinated guidelines for the creation of national information society policies, and the national enformation society strategy and action plan. All these strategies should be based on the eSEE Agenda, with clear goals, responsibilities and timelines for implementation, and may be the basis for all legislative and other regulatory actions.
- Prepare, adopt and implement the legal framework for the Information Society in accordance with the European Union

[7] eSEEurope Agenda for the Development of the Information Society: <http://www.eseeuropeconference.org/agenda.html>

directives. This applies especially to electronic signatures, commerce and contracts; intellectual property rights; copyright; databases; patents; software; semiconductors and protection of privacy on the Internet. The Council of Europe Convention on Cybercrime shall also be implemented.

- Establish mechanisms for regional co-operation and national implementation. Each country has accepted responsibility to establish an authority to oversee the Information Society and implement the relevant policies, strategies and regulations. A special line in the budget should be allocated to the eSEE working group and its appointed representatives. The countries shall encourage the foundation of non-governmental national ICT forums where information, experiences and best practices can be exchanged with other national forums and advice can be offered to information society state bodies. eSEEurope countries agreed to establish regional automated information systems and to create national centres that would be able to offer regional interconnection of electronic communications networks at affordable rates.
- Promote the development of the Information Society in several ways. This entails providing an infrastructure for free access to public information; exchanging information on liberalization of the market and the regulatory framework through conferences and seminars; establishing regional telecommunications service standards and universal service obligations; and drawing up aims to ensure equal opportunities for development. Each signatory country has accepted responsibility to promote better co-operation in employment and education. The countries agreed to establish the regional backbone to connect national academic and research institutions and create a joint project between teachers and students in the region. Regulations relating to the

foundation, operation and taxation of companies involved in e-commerce and telecommunications shall be improved.

Each government in the Stability Pact for South-Eastern Europe has committed itself to start putting these principles into practice immediately.

Difficulties Limiting Wider Access to Networks in South-Eastern Europe. The telecommunications infrastructure is not the only barrier blocking individual access to networks. There are also logistical, economic, educational and political obstacles. Logistical problems are mostly evident in rural areas, which do not have the appropriate infrastructure for Internet access. The economic problems are that most people cannot afford computer equipment to access the network or pay for provider fees; in this way South-Eastern Europe is similar to other transitional and developing countries. Educational barriers raise the question of computer literacy. Although almost every country in the region has computer studies on the school curriculum, lack of equipment – especially in remote areas – means that these classes are often based entirely on theory. Young people are an important target group for computer education and ensuring that they have the opportunity to access networks is of utmost importance. The middle-aged generation usually has a hard time accepting and operating new technology, unless required to do so for work. Moreover, a reasonable knowledge of English is needed in order to use new technologies. Finally, in some countries in South-Eastern Europe the absence of political will to implement the eSEE Agenda, to improve national legislation on information technology and to promote the Information Society through co-operation within the region has created further obstacles to Internet access.

Recommendations. Countries in South-Eastern Europe need to make the development of the Information Society and wider access to networks one of their priorities. The Internet is geographically independent, which means that there are plenty of opportunities for co-operation when developing national strategies. Countries may benefit and learn from experiences and best practices in other States in order to create an environment where there is wider access to online information. Training journalists to use new technologies and providing them with greater Internet access in their daily work is also an important step towards freedom of the media on the Internet.

A good example of a regional Internet portal for journalists[8] was recently launched by the Media Center Sarajevo in co-operation with the Media Center Belgrade and the Center for Investigative Journalism in Zagreb. This provides media professionals, students and any other interested parties with useful training materials and information, details of media laws, news about seminars in the region, relevant research as well as instructions on how to use computer-assisted reporting software.

Access to networks is a gateway to online information. However, promoting access must go hand in hand with education about new technologies and the Internet, targeting the younger generation especially.

Finally, a proper legal framework needs to be established in accordance with existing EU legislation. International organizations can play an important role in assisting countries in South-Eastern Europe to achieve all these goals.

In my opinion, political commitment, a proper legal framework and good education are the three ingredients in the recipe for wider Internet access. If these are achieved then citizens in South-Eastern Europe will be able to enjoy the benefits of the new Information Society and the opportunities of free media in an online environment.

[8] See <www.netnovinar.org>

Future Challenges of the Information Society

Mogens Schmidt and Sylvie Coudray

Future Challenges to Building Knowledge Societies

Introduction. The transformation in the nature and development of human knowledge is one of the most pervasive changes in the last century and is largely responsible for the compression of space and time experienced by greater numbers of people.

UNESCO encourages the construction of "Knowledge Societies", which goes beyond the narrower concept of the "Information Society" by recognizing the multilayered strands of knowledge that contribute to the making of the world. The concept of the Knowledge Society encourages the growth of capacity building so that information can be identified, produced, processed, transformed, disseminated and used as knowledge for human and social development.

Information, communication and knowledge are at the core of human progress, endeavour and well-being. Along with the Knowledge Society comes the concomitant recognition that all societies are innovative in the face of challenges and can contribute to the flow of knowledge in the world. Indeed, the concept offers a holistic and comprehensive vision with a clear development-oriented perspective that captures the complexity and dynamism of current changes in the world.

Current Challenges to Building Knowledge Societies for All. Traditional and new information and communication technologies (ICT) open up completely new opportunities to attain higher levels of development for the benefit of millions of people in all parts of the world. In light of these technological advances and their pervasive societal and ethical implications and impacts, UNESCO's mandate to "promote the free flow of ideas by word and image" and to "maintain, increase and spread knowledge", takes on new dimensions. It exerts an even greater responsibility on the Organization to contribute proactively to addressing potential challenges, maximizing benefits and supporting equitable access to the opportunities provided by ICT to all people. The most serious of these challenges are not technological but social and they force us to answer the most fundamental questions at the heart of the development today. These challenges include the issue of freedom of expression, the goal of education for all, universal access to knowledge and information, and cultural and linguistic diversity. What they have in common is the call to continuously adapt and affirm our commitment to free flow of information as a fundamental principle underlying the production and exchange of knowledge in society.

The concept of knowledge societies acknowledges the inequalities in access to the conditions of production and reception of knowledge on a world scale, especially in terms of access to new information technologies (ICT). New information technologies offer lightning-fast access to the world's body of knowledge and the possibility of instant exchange of perspectives and information for many people on the globe. Nevertheless, the "digital divide" is a stark reality, with 80 per cent of the world's population lacking access to basic telecommunications, approximately 860 million illiterates and 2 billion people lacking electricity. But the real issues in the creation of knowledge societies are less technological than human – how can we take the human dimension into account when dealing with the "digital divide" and why is it important?

Principles for Building Inclusive Knowledge Societies. From its mandate to encourage free flow, UNESCO has identified four key principles at the heart of its work in developing knowledge societies:

The **first**, the principle of freedom of expression, must apply not only to traditional media but also to new media, including the Internet. It is the basic premise of knowledge societies. UNESCO, whose mandate is to promote the "free flow of ideas by word and image", is therefore acting unequivocally in keeping with Article 19 of the Universal Declaration of Human Rights.[1] It is important then to continue to mobilize energies and efforts to promote freedom of expression and its corollary, freedom of the press, as a basic right indispensable to the exercise of democracy. Freedom of expression is a major avenue through which creativity, innovation, criticism and questioning can be brought. This has enabled citizens to gather information and mobilize coalitions in major policy debates, and to trigger improvements in government efficiency and transparency through better communication with citizens. Our insistence on the plural form of knowledge societies rests on the conviction that there is no single uniform model, dictated by technology or market relations, to which all societies must conform. The nature of knowledge societies should be conceived as plural, variable and open to choice, and freedom of expression is inseparable from this vision.

The **second principle**, access to quality education for all, is essential for building and developing the necessary skills and capacities for development, progress and social peace in all societies. This is a fundamental right, confirmed in Article 26 of

[1] Article 19 of the Universal Declaration of Human Rights: "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."

the Universal Declaration[2], as well as a tool for combating illiteracy, marginalization, poverty and exclusion. Education is the greatest capacity-builder of all. Without education, knowledge societies cannot exist. As knowledge becomes central to development, the worldwide challenge of providing quality lifelong educational opportunities for all is becoming critical. Throughout history, education has been constrained within an eternal triangle of quality, access and cost. With conventional systems, quality often declines with an increase in access or cuts in costs. However, the appropriate use of ICT, with its potential for wider access, higher quality and lower costs, holds great promise to achieve these goals at the same time.

Education for All is the foremost priority of UNESCO, because education is both a fundamental human right and a key to sustainable development and peace within and among countries. Achieving the goals set in Dakar[3] and at the Millennium Development Summit[4] means ensuring that the digital divide does not further marginalize the poorest sectors of the population, and it entails finding creative, alternative paths to learning. It also calls for continuous reflection on ensuring that education does justice to the local context – particularly cultural, linguistic and economic needs – and the global one, in light of the reality of growing interdependence between nations.

The **third principle**, universal access to information and knowledge, especially information in the public domain, is a prerequisite for broader participation in development processes. Universal access to knowledge and information is a fundamental building block inseparable from freedom of expression. There can be no genuine knowledge societies if universal access to knowledge and information is denied. The concept of universal access is underpinned by the presence of several essential supporting components, namely: availability of communication infrastructure and connectivity; available content relevant to the user; affordable services within reasonable distances; users with the necessary information literacy skills to use these services and to add value by developing, exchanging and creating new services.

As the majority of the world's population does not have access to ICT, the development of a modern ICT infrastructure should have high priority. Both commercial and not-for-profit providers should help schools, libraries, community centres, civil society organizations and government agencies to connect to the Internet, in support of universal access principles. Access to traditional media, such as radio, must also be widened as the basic building blocks of knowledge societies and their potential as relays of digital information in developing countries should be explored. Access to public domain information, also known as the "information commons" should also be encouraged. Public domain information is publicly accessible information, the use of which does not infringe any legal right, or breach any other communal right (such as indigenous rights) or any obligation of confidentiality. States should recognize and enact the right of universal online access

[2] Article 26 of the Universal Declaration of Human Rights:

"(1) Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit.

(2) Education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms. It shall promote understanding, tolerance and friendship among all nations, racial or religious groups, and shall further the activities of the United Nations for the maintenance of peace.

(3) Parents have a prior right to choose the kind of education that shall be given to their children."

[3] The World Education Forum, Dakar, Senegal, 26–28 April 2000. See <http://www.unesco.org/education/efa/ed_for_all/dakfram_eng.shtml> for more details.

[4] See <http://www.un.org/millenniumgoals/> for more details.

to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation.

The **fourth principle** is cultural and linguistic diversity. In addition to art and literature, culture encompasses lifestyles, ways of living together, value systems, languages, traditions and beliefs. Cultural diversity is the common heritage of humankind and the understanding of and respect for other cultures is a prerequisite for building knowledge societies.

A central feature is the need for policies as well as actions that support plurality and diversity, so that citizens can access and create information and knowledge in their own languages and within their own cultural frameworks. The creation of environments conducive to the development of local content in digital format and the preservation of digital heritage will benefit present and future generations. Digital heritage consists of human knowledge and expression – whether cultural, educational, scientific or administrative – created on or converted to digital media. Concerted and urgent attention to this fast growing heritage is needed because of the rapid obsolescence of the hardware and software on which it is maintained. There are many constraints – economic, political, administrative, social, cultural and technical. For example, many electronic networks are currently inadequately adapted to handle the diversity of the world's languages, with only 12 languages out of the world's 6,000 or so accounting for about 90 per cent of the total web content. Two new UNESCO standard-setting instruments, adopted in October 2003 at the last General Conference, the Recommendation on the Promotion and Use of Multilingualism and Universal Access to Cyberspace and the Charter on the Preservation of the Digital Heritage, propose strategies for addressing these challenges.

From Geneva to Tunis. The Geneva phase of the World Summit on the Information Society was a critical milestone in international co-operative efforts to promote knowledge societies and to understand their prerequisites. The Summit provided an important platform for promoting UNESCO's concept of knowledge societies. The four principles, which UNESCO took to the Summit, discussed earlier, are now reflected in the Summit Declaration and Action Plan. UNESCO is working unstintingly to maintain this momentum and to advance the WSIS process. The phase leading up to the second Summit in Tunis provides an opportunity to assess progress made since Geneva on implementation plans and actions, to explore new initiatives and solutions, and to mobilize future partners.

An Upcoming Issue: Internet Governance. An upcoming issue for UNESCO in the WSIS process is the question of Internet governance. UNESCO observes that the term "Internet governance" has not yet been clearly defined. For some, it describes the narrow issue of the management of domain names and infrastructure that are presently administered by the Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit corporation under Californian Law. The prevailing tendency in the current debate, however, is to attribute to this term a much broader meaning comprising not only technical, but also ethical, societal and legal issues. Moreover, the term "Internet governance" is misleading as it is laden with presumptions about governing approaches which for some may imply governmental involvement.

UNESCO will continue to safeguard key values like freedom of expression, cultural diversity and openness. It will advocate that existing mechanisms such as ICANN, or any modification of these mechanisms, must reflect the following principles:

- The inherent openness of the Internet infrastructure must be preserved and should be conducive to the free flow of ideas and knowledge through word and image;
- Modifications must not result in the global Internet governance system becoming subjected to governmental control, nor should they facilitate or permit censorship;
- There must be a precise correlation between new mechanisms and the problems they seek to address;
- Technical innovation must continue to be encouraged;
- Modifications to ICANN or new mechanisms should not inhibit interoperability, cause instability, nor should they slow down the continued technical development of the Internet; and
- Any global Internet management system or mechanism must be technically competent, transparent and non-partisan.

Whichever mechanism manages the current responsibilities of ICANN, the result should be one that enables greater use of the Internet, and thereby greater participation in the modern information world, by an increasing number of citizens from diverse linguistic and cultural backgrounds.[5]

Conclusion: Constructing Knowledge Societies Together.

UNESCO is committed to fostering the creation of equitable and just societies, supporting human rights and human development in all spheres and working for achievement of the Millennium Development Goals. The necessary political, social, economic and attitudinal changes to realize these goals will not occur overnight. This will require persistent long-term actions that combine a range of multidisciplinary skills and perspectives. UNESCO has prepared a series of publications on various aspects of the WSIS[6] as well as a website[7], to inform participants of UNESCO positions and actions. UNESCO is committed to work with its partners to help implement these actions.

The challenges facing knowledge societies are those that stem from the two basic principles of UNESCO's mandate mentioned at the beginning of this article – to promote the unrestricted flow of word and image and to widen access to information. Knowledge societies should be firmly based on a commitment to human rights and freedoms, including freedom of expression. They should also help all citizens realize their cultural and linguistic rights, including the right to an education, and guarantee access to all media, traditional and new for the purposes of knowledge creation and exchange. These are long-term challenges that require analysis, investment and co-operation among States, the private sector and civil society.

[5] For more information, see UNESCO Position Paper on Internet Governance at <http://portal.unesco.org>

[6] See <http://portal.unesco.org> and type in "WSIS Document Series". Selected publications include "Cultural and Linguistic Diversity in the Information Society," "Gender Issues in the Information Society", "Social Transformation in the Information Society", *inter alia*.

[7] <http://portal.unesco.org/wsis>

Steve Buckley

Whose Information Society? Communication Rights and the WSIS

Introduction. In January 2002 the United Nations General Assembly confirmed its intention to sponsor the World Summit on the Information Society (WSIS), an event to be organized in two phases – Geneva 2003 and Tunis 2005. In doing so the General Assembly stressed the urgent need to put knowledge and technology “at the service of development for all”.

In the same month, a civil society coalition, the campaign on Communication Rights in the Information Society (CRIS), was launched at the second World Social Forum. The aim of the CRIS campaign was to broaden and deepen the debate on the Information Society, to promote democratization of access to communications and to strengthen commitments to communications in the service of sustainable development.

For the members of the CRIS campaign and other civil society organizations involved with the WSIS process it has been an intense period of activity which has highlighted major fault-lines in global debate on the human communications environment. During the Geneva phase, civil society actors worked closely with government delegations, lobbying on points of drafting, advising on others. Despite the holding of some key intergovernmental sessions behind closed doors, civil society participants gained a high level of insight into government positions and in some cases influenced those positions to significant effect.

The communication rights perspective is concerned with the process of human communication and with the moral and legal rights that enable us to defend our right to communicate. Of particular importance is the legally understood right to freedom of information, opinion and expression, but closely linked to communication rights are also the right to freedom of association, the right to privacy and the right to one's own culture.

But the call for "communication rights" is not a juridical quest. Rather it is a social demand for a fairer communications environment. This is a demand articulated by marginalized communities worldwide and by civil society groups concerned as much by the rise of private media concentrations and new unaccountable multinational communications gatekeepers as by the more familiar problem of authoritarian governments.

WSIS 2003 – The Geneva Phase. The idea of having a World Summit on the Information Society can be traced back to the growing economic importance of the global information and communication industries and the opening of the Internet to private commercial use accompanied by a United States vision, articulated by Al Gore, of a global "information superhighway". The European counterpoint, under the leadership of European Commissioner Martin Bangemann, spoke of the "information society" backed up by social as well as economic analysis, even including one paper with the title "People First in the Information Society".

The US and Europe built consensus in Japan at the G8 meeting in Okinawa in July 2000, which agreed the Okinawa Charter on the Global Information Society and established the G8 Digital Opportunities Task Force with the objective: "To promote international co-operation with a view to fostering policy, regulatory and network readiness; improving connectivity, increasing access and lowering cost; building human capacity; and encouraging participation in global e-commerce networks."[1]

The Okinawa Charter was drafted at a time of economic optimism in the prospects of information technology driven economic growth. Stock markets were at the peak of the speculation fuelled dot-com boom. The Okinawa Charter and the follow-up report of the G8 Digital Opportunities Task Force strongly influenced the drafting framework for the WSIS and particularly the emphasis in the Action Plan on network infrastructure and the promotion of national "e-strategies", a term which first appears in the Charter.

At the same time, there were moves within the United Nations system to develop a strategic approach to information and communication technologies. The International Telecommunications Union (ITU) had tabled proposals as early as 1998 for a World Summit on the Information Society. In 2001 the United Nations Secretary General, at the request of Heads of State, launched the UN ICT Task Force "to lend a truly global dimension to the multitude of efforts to bridge the digital divide, foster digital opportunity and thus firmly put ICT at the service of development for all."[2]

When the UN General Assembly in January 2002 adopted a resolution endorsing a framework from the ITU for a World Summit on the Information Society (WSIS), it was in recognition of: "The urgent need to harness the potential of knowledge and technology for promoting the goals of the United Nations Millennium Declaration and to find effective and innovative ways to put this potential at the service of development for all."[3]

In contrast to the G8 position, the UN mandate was explicitly development oriented and the ITU was mandated to take the lead within a "multi-stakeholder" framework. It was agreed the Summit would take place in two phases – Geneva in 2003 and Tunis in 2005. A WSIS Secretariat was established to support the first phase in Geneva and this included, from the start, a Civil Society Division to facilitate civil society participation.

For civil society groups such as those grouped together in the CRIS campaign, the WSIS presented a unique opportunity to engage with and raise awareness among governments and multilateral agencies and to strengthen civil society alliances and common positions. Civil society groups organized around WSIS from the earliest stage and have been vigorously present at all official preparatory meetings.

Civil society activists working in the communication environment have long recognized the social importance of access to and the effective use of communications tools. But equally there is well-founded scepticism about a narrowly drawn "Information Society" in which the key technologies are taken to mean telecommunications and the Internet.

Although much is promised by the Information Society – access to vital knowledge for health and education, better information from governments and corporations, electronic democracy, global trade and exchange, up to the minute news – many people face the danger of being left out. This danger is often called the "digital divide" by those who choose to frame the debate in terms of telecommunications and the Internet. In reality it is a broader "communications divide" characterized by the unequal access of poor people to the means of communication and to freedom of information and of expression.

In the narrow vision of the Information Society the solution to the "digital divide" is simple. It is essentially a matter

[1] Okinawa Charter on the Global Information Society, Group of Eight, Okinawa, July 2000.

[2] Plan of Action of the ICT Task Force, United Nations, 2001.

[3] United Nations General Assembly, Resolution 56/183, 31 January 2002.

of rolling out the network infrastructure so that everyone in the world can have access to the Internet. This vision was explicit in the G8 Okinawa Charter on the Global Information Society adopted in July 2000 at the G8 Summit. It is a political-economic perspective which underpins the early WSIS texts and which in effect gives priority to building the infrastructure and the consumer base for global e-commerce over the public interest in communications for development. It does so by claiming that the former will lead to the latter without providing supporting evidence for its case.

One early draft of the WSIS Declaration described the Information Society as "a new and higher form of social organisation where highly developed ICT networks and ubiquitous access to information… improve quality of life and alleviate poverty and hunger".[4]

Others have argued compellingly that giving universal access to the Internet will cost a lot and accomplish little. Bill Gates, speaking in October 2000 at a Seattle conference on the "digital dividend", famously argued that investment in health and literacy is more important for poor people than providing access to PCs and the Internet.[5] Charles Kenny, an economist with the World Bank, has estimated that the worldwide subsidy needed for everyone living on $1 a day to get one hour of access a week might reach $75 billion – considerably more than the global total of aid flows each year.[6]

Despite such concerns, the roll-out of ICT-based products, service and applications remained a dominant perspective in the WSIS debate. This calls for market freedoms and pro-competition policies but also includes limits on freedoms and rights where this serves the interests of corporate stability and growth e.g. intellectual property, proprietary software, security, Internet governance, spectrum planning and licensing.

The CRIS campaign and other civil society participants in WSIS rejected this perspective as the basis for negotiation, arguing instead for a people-centred approach, based on human rights principles and sustainable development priorities. By the completion of the Geneva phase of the WSIS many of the concerns expressed by the CRIS campaign and other civil society groups had been adopted in the WSIS Declaration of Principles.[7] The WSIS Action Plan, however, remains largely framed in the narrow perspective.[8]

Rejection of the narrow vision of the Information Society and its assumption that ICT networks and access to information will automatically lead to the alleviation of poverty creates a serious dilemma for WSIS but one which remained unresolved at the conclusions of the Geneva Summit. If WSIS is to fulfil its mandate, it is necessary that there be sufficient analysis of the proposed actions to reasonably conclude (a) that they would indeed make a net positive contribution to the agreed development goals; and (b) that the resources deployed could not be more effectively used elsewhere.

WSIS 2005 – the Tunis Phase. The second phase of the WSIS is scheduled to end in a Summit in Tunis from 16 to 18 November 2005. There is to be a further series of preparatory meetings leading up to the Summit. The main focus of the second phase is intended to be the implementation and monitoring of the Action Plan. There are also two high level task

[4] World Summit on the Information Society, Draft Declaration, Document WSIS/PCIP/DT/1(Rev.1)-E, 30 May 2003.

[5] Remarks by Bill Gates, Digital Dividends Conference, Seattle, Washington 18 October 2000 <http://www.microsoft.com/billgates/speeches/2000/10-18digitaldividends.asp>

[6] Charles Kenny, "Development's False Divide", *Foreign Policy*, January – February 2003 <http://www.foreignpolicy.com/issue_janfeb_2003/kenny.html>

[7] World Summit on the Information Society, Declaration of Principles, 12 December 2003.

[8] World Summit on the Information Society, Plan of Action, 12 December 2003.

forces under the patronage of Kofi Annan, the UN Secretary General. One of these is to deal with the contested issue of Internet governance. The other will examine the African proposals for a Digital Solidarity Fund and the wider context of financing ICTs for development.

During the Geneva phase civil society's role has been to bring critical and independent voices to the debate and, where those voices have themselves been able to find a common position through their own dialogue, to articulate that collectively to those in government. The main focus of the Geneva phase was clear – the political process leading to the intergovernmental Declaration of Principles and the Plan of Action.

In parallel, however, were a wide range of WSIS related activities and outcomes. For civil society these included meetings, conferences, announcements, partnership-based initiatives, publications and exhibitions through to counter-actions and demonstrations.

For the Tunis phase the extent and the nature of civil society engagement is likely to be significantly different. The focus of the Tunis phase is more diffuse. Governments have agreed the Tunis Summit should lead to a "political and operational statement" to reaffirm and enhance the commitments undertaken in the Geneva phase but there is unwillingness to re-open the terms of the Declaration or the Plan of Action.[9]

Having formally rejected the intergovernmental texts from the Geneva phase and with fundamental differences with governments on the framing of the Plan of Action, civil society actors who played a lead role in the Geneva phase are not in a position now to "reaffirm" the validity of governmental commitments which they never fully endorsed.

At the same time there is wide expectation that Tunis will provide a less supportive environment for civil society. Several civil society actors have drawn attention to serious human rights violations in Tunisia and media groups have been particularly concerned with Tunisia's poor record on freedom of expression, including systematic blocking by government-owned ISPs of Internet sites critical of the Tunisian Government. Civil society participation in WSIS 2005 inevitably must also put the spotlight on Tunisia.

In addition to the drafting of a "political and operational statement" for the Tunis Summit, governments have committed to a "stocktaking" exercise, the results of which may provide a more substantive tool for measuring the effectiveness of WSIS in contributing to the development goals. The stocktaking exercise is to gather a broadly representative body of information on actions being taken by governments, private sector and civil society in furtherance of the commitments to harnessing ICTs for development.

The stocktaking explicitly requires respondents to describe the contribution that projects and actions are making to achievement of internationally agreed development goals. In this respect the results could provide a useful empirical base against which the effectiveness of WSIS commitments can be further monitored and evaluated.

Alongside the preparatory process for the Tunis Summit, two high level task forces will address the unfinished business of the Geneva phase – Internet Governance and Financing for Development. It would seem, in these fields at least, that the role and interest of civil society will continue albeit with different rules of engagement.

The establishment of the task forces by the UN Secretary General takes these fields partly outside of the WSIS process.

[9] World Summit on the Information Society, Concluding statement, Hammamet, 26 June 2004.

In the case of the Financing for Development Task Force, in particular, there have already been civil society concerns expressed at the lack of transparency in the process and the absence of mechanisms for participation.

The Task Force on Internet Governance has adopted a more open and participatory methodology but there may be reluctance to open the agenda beyond a fairly narrow set of technical parameters such as the international domain name and numbering system.

Conclusions and Priorities for Civil Society. From the above it should be clear that the Tunis phase of WSIS does not have a single central focus but offers multiple points of intervention. This presents both difficulties and opportunities for civil society. In the absence of a clear external focus and goal around which to organize, civil society engagement may itself become more fragmented.

One possibility is that civil society actors who have played a lead role in the Geneva phase may simply pull back leaving new civil society actors to occupy the political space of WSIS. The resulting civil society input would probably be less critical of government and perhaps more ready to accept and work within the market-oriented paradigm.

The alternative is for civil society to "reaffirm and enhance" the civil society commitments made in the Geneva phase by building an alternative agenda to the WSIS. The best prospects for this lie with those civil society organizations and activists who have worked together in or with the campaign on Communication Rights in the Information Society.

Some principles and objectives can be drawn from the communication rights perspective and the work that has been achieved by civil society groups in the Geneva phase:

1. The market driven development of the infrastructure for access to the Internet is characterized by gross asymmetry in access to information and in information flow resulting from but also reinforcing existing social and economic inequality. In an increasingly information-based economy a more equitable access to information is essential if global social and economic inequalities are to be reduced rather than maintained or increased. This must not become a pretext for restrictions on the freedom of expression or the free flow of information but requires positive action to ensure inclusive access to communication and to defend and promote cultural diversity.
2. Universal access to communication services and networks is essential for the realization of communication rights but will not be delivered, within the foreseeable future, by providing everyone with domestic access to the Internet. Access for all to the global communications environment requires investment not only in public access centres but also in traditional communication technologies such as community radio and television. Public investment in local communications facilities is one approach. Conditionalities or levies placed upon private telecommunications providers is another. Community-based initiatives should be encouraged and supported including legal and/or regulatory reforms where there are legislative or regulatory barriers to establishment.
3. Literacy is an essential prerequisite to access and use of the Internet. Free and universal access to basic education must be ensured and supported. Media literacy and practical communications skills have become an essential component of a basic education and are necessary for the effective realization of communication rights.

4. The Internet is not intrinsically a guarantor of freedom of opinion and expression. New corporate gatekeepers have increasingly developed policies and technologies of control which go beyond the legitimate and include the arbitrary and the indiscriminate. Commercial technologies to control the Internet are also increasingly being used by governments to introduce new forms of censorship. Freedom of expression on the Internet must be protected, as elsewhere, by the rule of law rather than relying on self-regulation or codes of conduct. There must be no prior censorship, arbitrary control or unjustified constraints on the content, transmissions and dissemination of information. Pluralism of the sources of information and the media must be safeguarded and promoted including diversity in systems for information retrieval.

5. The right to privacy faces new challenges and must be protected. Every person must have the right to decide freely whether and in what manner he or she wishes to receive information or to communicate with others including the right to communicate anonymously. The collection, retention, processing, use and disclosure of personal data, no matter by whom, should remain under the control of the person concerned. Powers of the private sector and of governments to access personal data risk abuse of privacy and must be kept to a legally acceptable minimum and subject to public accountability.

6. The Internet provides enormous scope for the sharing and development of the common pool of human knowledge but this potential is increasingly held back by the reinforcement of private information property regimes in the Internet environment. There is a need for fundamental review of the international instruments governing copyright,

> patents and trademarks to incentivize development of the public domain of global knowledge, to ensure the right of access to information and the right to creative reuse and to adaptation of information, and to accelerate the social and economic benefits of freely available information including free and open source software.

The reaffirmation and enhancement of principles and priorities articulated by civil society in the Geneva phase will need a commitment to sustained partnership after the completion of the Tunis phase of the WSIS. We might call this the Communication Rights Agenda. Its focus would be on building civil society knowledge, networks and advocacy for a more people-centred communications landscape based on human rights and social justice. It may not be immediately apparent but, when we look back at the WSIS process, possibly the most significant outcome will be the extent to which the process has brought together civil society actors into the beginnings of a movement for a better communications environment that could equal the movement for a better natural environment that emerged in the closing decades of the last millennium.

Gus Hosein

Open Society and the Internet: Future Prospects and Aspirations

We once dreamed about the future. It involved a global information infrastructure that was not hampered by borders and governments. Human potential would reach beyond its prior limits as we communicated without interference in a space that was separate from flesh and steel. The Internet would set truth free, and we would follow.

And this truth and liberty are required for the maintenance of an open society. In an open society, social actors yearn for improving society, knowing that no one has perfect knowledge or control of the outcome of decisions – thus creating a space for further actors to join in and participate. It is taken for granted that actors are able to contribute, to participate, and to submit their ideas for consideration. It is far too often taken for granted that the marketplace of ideas will be filled with merchants vying for attention. It is far too often taken for granted that we have the ability to interact, to communicate, to speak freely. The Internet was supposed to be the veins through which this lifeblood could sustain an open society.

I have no intention of mocking the Free Internet image of the future. Although it is common to argue that we were ignorant when we had that dream, such hindsight is uninteresting. I am more interested in the questions of "Why did we want that dream to be true?" and "What was it that we were once seeking that we seem to be so far away from now?"

We Sought in Technology What We Were Promised. Before the popularization of the Internet, the media world was relatively stable. Film and broadcasting industries were regulated with regards to what they could show, and ratings schema applied. Print and newspaper media were regulated through liability regimes, codes of practices, and ownership regimes, amongst other forms of intervention into the marketplace of ideas. And borders were reasonable constraints on the flow of information, where books and other material could be stopped at borders in accordance with national laws.

Yet we were promised so much more, and we heard of the potential of that promise. Free speech and free expression were long heralded values, core beliefs, and rights. Freedom of speech was enshrined in constitutional documents, international charters, and sustained in jurisprudence.

The law took some time to come around, however. Consider a case in the United States, decided in the Supreme Court in 1919. The case involved five Russians in the United States who were accused of violating the Espionage Act for conspiring with the Imperial Government of Germany. The conspiracy took the form of printing, writing and distributing copies of a leaflet entitled "Revolutionists Unite for Action" and "The Hypocrisy of the United States and her Allies" that criticized the US Government's attitudes towards Soviet Russia, calling upon "workers" for solidarity and to strike, and to fight. The Court sided with the Government, contending that

> while the immediate occasion for this particular outbreak of lawlessness, on the part of the defendant alien anarchists, may have been resentment caused by our government sending troops into Russia as a strategic operation against the Germans on the eastern battle front, yet the plain purpose of their propaganda was to excite, at the supreme crisis of the war, disaffection, sedition, riots, and, as they

> hoped, revolution, in this country for the purpose of embarrassing and if possible defeating the military plans of the government in Europe.[1]

The country, after all, was at war. In a famous dissenting opinion, Supreme Court Justice, Oliver Wendell Holmes argued that the accused were not impeding the war by expressing their opinions.

> [I]t is evident from the beginning to the end that the only object of the paper is to help Russia and stop American intervention there against the popular government – not to impede the United States in the war that it was carrying on.

Controversially, he argued:

> Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition. To allow opposition by speech seems to indicate that you think the speech impotent, as when a man says that he has squared the circle, or that you do not care whole heartedly for the result, or that you doubt either your power or your premises. But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas – that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.

With this statement he opened discussion on the "marketplace of ideas" and the importance of speech and contestation. Holmes's words were most surprising because he was behind two court decisions in the previous year that took harsh views of freedom of expression during war time.[2] This change of faith reflected conversations he held with others in the meantime, and also that the war was over by the time of the decision. He concludes:

> That at any rate is the theory of our Constitution. It is an experiment, as all life is an experiment. Every year if not every day we have to wager our salvation upon some prophecy based upon imperfect knowledge. While that experiment is part of our system I think that we should be eternally vigilant against attempts to check the expression of opinions that we loathe and believe to be fraught with death, unless they so imminently threaten immediate interference with the lawful and pressing purposes of the law that an immediate check is required to save the country.[3]

In declaring this he revised his earlier opinion that falsely screaming fire in a theatre was worthy of infringing First Amendment rights to free speech, calling instead for such infringement to occur only in the case of imminent threats and immediate interference. The essence of this dissent was adopted by the Supreme Court 50 years later.

Even before that, however, the promise of speech and protecting its conditions grew greater. In a 1960 court decision in the case *Talley v. California*, the US Supreme Court upheld the right to anonymous pamphleteering. This case involved a Los Angeles city ordinance restricting the distribution of handbills. The ordinance required the naming of the person who wrote, printed, and distributed the handbill. The petitioner, Talley, was arrested and tried for violating this ordinance with handbills urging readers to boycott against certain merchants and businessmen on the grounds that they carried products of "manufacturers who will not offer equal employment opportunities

[1] *ABRAMS v. US*, 250 US 616 (1919).

[2] Peter Irons, *A People's History of the Supreme Court* (Penguin, 1999).

[3] *ABRAMS et al. v. UNITED STATES*.

to 'Negroes, Mexicans, and Orientals'." The Supreme Court supported Talley, arguing that

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws anonymously. The obnoxious press licensing law of England, which was also enforced on the Colonies was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers. John Lilburne was whipped, pilloried and fined for refusing to answer questions designed to get evidence to convict him or someone else for the secret distribution of books in England. Two Puritan Ministers, John Penry and John Udal, were sentenced to death on charges that they were responsible for writing, printing or publishing books. Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. (...) It is plain that anonymity has sometimes been assumed for the most constructive purposes.[4]

A similar decision emerged 35 years later that contended that there was a marketplace of ideas, as promised by Oliver Wendell Holmes in 1919. In 1995, the Supreme Court decided that anonymous pamphleteering was protected under the Constitution, in *McIntyre v. Ohio*.

> The interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like

> other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[5]

Beginning with a dissent, and then adopted into mainstream jurisprudence, free expression is considered as a key component to a functioning democracy, and something that should be upheld, promoted, and protected. This is even the case when it involves anonymous speech.

Law Unto the Internet. The printing press was heralded because it *democratized* publishing, decentralizing power to all those who owned printing presses. This was not everyone, obviously. As such, the ability of individuals to rise and speak freely was inhibited by the lack of technology available to all.

The promise of the Internet changed this. Everyone was potentially a printing press. Everyone could broadcast information, and could be the recipient of broadcasts, one-to-one, many-to-one and one-to-many forms of communications. And this was to be beyond the reach of legislatures, courts, and others who wished to impede the flow of information. And no one would know if you were a dog whilst on the Internet due to promises of privacy and anonymity. We wanted an infrastructure that could sustain our liberties, and believed that the Internet would be it.

It almost was. A most celebrated case is the fate of the Communications Decency Act, passed by the US Congress in 1996. The law required access control mechanisms on sites that made "indecent" information available to the general public, to verify the age of visitors. The constitutionality of the

[4] *Talley v. California*, Supreme Court of the United States, 362 US 60, decided 7 March 1960.

[5] *McIntyre v. Ohio Elections Commission*, Supreme Court of the United States, No. 93-986, decided 19 April 1995.

CDA was questioned immediately. According to David Sobel, a leading expert on the matter,

> Whether the millions of individuals visiting sites on the Internet are seeking information on teenage pregnancy, AIDS and other sexually transmitted diseases, classic works of literature or avant-garde poetry, they enjoy a Constitutional right to do so privately and anonymously. The CDA seeks to destroy that right.[6]

The US District Court injunction on the CDA used similar ideas.

> Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR). Many members of SPR's mailing list have asked to remain anonymous due to the stigma of prisoner rape.

The Act was eventually struck down on the grounds of identity, anonymity, and free speech. According to the District Court decision, "any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig", and this was "due to the nature of the Internet." That is,

> There is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms. An e-mail address provides no authoritative information about the addressee... There is also no universal or reliable listing of e-mail addresses and corresponding names or telephone numbers, and any such listing would be or rapidly become incomplete. For these reasons, there is no reliable way in many instances for a sender to know if the e-mail recipient is an adult or a minor.[7]

At the Supreme Court, the majority concurred.

> This dynamic, multifaceted category of communication includes not only traditional print and news services, but also

> audio, video, and still images, as well as interactive, real-time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, "the content on the Internet is as diverse as human thought."[8]

The Internet was the newest incarnation of the "press" that the Founders of the US had envisioned when they adopted the Constitution, and thus was worthy of all the protections from incursions under the First Amendment. The Supreme Court concluded:

> The Government apparently assumes that the unregulated availability of "indecent" and "patently offensive" material on the Internet is driving countless citizens away from the medium because of the risk of exposing themselves or their children to harmful material.
>
> We find this argument singularly unpersuasive. The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.

[6] Electronic Privacy Information Center, "Internet 'Indecency' Legislation: An Unconstitutional Assault of Free Speech and Privacy Rights" (Washington DC, 1996).

[7] *American Civil Liberties Union et al. v. Janet Reno* Civil Action No. 96–963, In The United States District Court for the Eastern District Of Pennsylvania.

[8] *Reno v. ACLU*, 26 June 1997, 521 US 844.

The marketplace of ideas seemed secured from extraneous interference of censorship and content controls.

This all probably appears to be a bit dramatic, however. Consider the *Abrams* case: we were really talking about controversial political speech at a time of war. Certainly that deserves some constitutional scrutiny and protection. Similarly, the *Talley* case involved anonymous pamphleteering regarding racially discriminatory hiring practices at companies; and proportionately, the Supreme Court decision referred to dramatic transgressions upon expression in history as the root of oppression. But when it came to the CDA, this involved a law that merely restricted access to pornography. Why did everyone get so excited, speaking of pigs, and the marketplace of ideas, just because of mechanisms to restrict access to pornography?

My answer to that question is quite simple, and perhaps simplistic. We, and I count myself amongst those who opposed the CDA, saw this as the first step to greater controls. It is a case of the ever-articulated "slippery-slope" argument: if you begin with one form of content regulation, even with the most noble intents the rest will naturally follow. Other forms of regulation will arise either intentionally, through using the "verification" technologies to verify someone's geographic location to prevent access to non-indecent information, or less directly through the chilling of online speech for fear of surveillance or eventual censoring.

We Are Left with Strengthened Politics. Despite the "victory" in the CDA decision, the incursions upon free expression continued. Regardless of calls by experts, technologists, and lawyers that the Internet would not respond well to content regulation, content regulation followed nonetheless.

Even in the CDA decision, we were warned that the technology of the Internet could be changed. The technology could be shaped, the structure of the market altered, to permit censorship. According to the dissenting opinion from Justice O'Connor:

> Cyberspace differs from the physical world in another basic way: Cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws. This transformation of cyberspace is already underway. (...) Internet speakers (users who post material on the Internet) have begun to zone cyberspace itself through the use of "gateway" technology. Such technology requires Internet users to enter information about themselves – perhaps an adult identification number or a credit card number – before they can access certain areas of cyberspace much like a bouncer checks a person's driver's license before admitting him to a nightclub. Internet users who access information have not attempted to zone cyberspace itself, but have tried to limit their own power to access information in cyberspace, much as a parent controls what her children watch on television by installing a lock box. This user-based zoning is accomplished through the use of screening software (such as Cyber Patrol or SurfWatch) or browsers with screening capabilities, both of which search addresses and text for keywords that are associated with "adult" sites and, if the user wishes, blocks access to such sites.[9]

Slowly the marketplace of ideas could be chipped away at, through law, and other mechanisms.

Filtering technology emerged and is now enshrined in laws and policies in a number of countries, calling for their use at the end-user level (e.g. Australia), at service providers (e.g. US schools and libraries), and at the national level (e.g. China and Saudi Arabia). Whether through direct regulation of individuals'

[9] Justice O'Connor, *Reno v. ACLU*, 521 US 844.

conduct or indirect regulation of Internet service providers, censorship is occurring. In the United Kingdom, mobile phone providers are now filtering access to pornographic content in order to prevent children from accessing these sites. An adult customer would have to contact the phone company to prove her age.[10]

There are other mechanisms, however. Notice and take-down procedures are being implemented into a number of laws in a number of countries. The United Kingdom is particularly proud of the regime for preventing access to criminally obscene material, enforced by a self-regulating Internet Watch Foundation. The IWF is now supporting other countries in copying the UK's success. But what starts with "criminally obscene" for the protection against child pornography will soon be used for other purposes. A number of countries in Continental Europe have harsh regimes to combat xenophobia by requiring the takedown of online material.

"Notice and takedown" requests are used now for the protection of "copyright". A recent study by the Dutch NGO Bits of Freedom found that, when combined with the European E-Commerce Directive that placed liability for illegal content upon website-hosting providers, the effects of copyright protection laws upon free speech are increasingly dangerous. Bits of Freedom tested ten Dutch ISPs on their practices of notice and take down by creating a number of websites quoting a text written by Multatuli, a famous author, in 1871. The text is clearly something that belongs to the public domain, and is no longer subject to copyright protection. Bits of Freedom then filed complaints to the ISPs on behalf of a fake society that was created to act as a copyright holder. Seven providers removed the text without even looking at the website, "or demonstrating any clue about copyright basics". One provider went so far as to send all the personal details of their customer to the complainant, breaching privacy protections.[11]

Copyright laws are the creature of increased lobbying by increasingly powerful content production industries. This is a different form of politics from the politics of child protection that led to the CDA. Both political stratagems, however, rely on personal information. Simultaneously, we are seeing a return of the politics that led to the decision in Abrams, in policies and initiatives to combat terrorism. This strategy also relies on the reduction of privacy.

Politics of Surveillance-Enabled Censorship. While the CDA decision noted the challenges in requiring age verification, the minority opinion noted that technology is malleable and can be shaped to meet the concerns of those who wrote the CDA. For a reasonably-regulated Internet, all we would require is every user to disclose her name and country of residence (and even state/province), age, and then bind that information to her network information (e.g. IP address, account number at ISP).

The judges who decided that the CDA was unconstitutional argued that no such infrastructure of personal information disclosure existed at the time. The dissenting justice said that it is possible to do what the CDA envisioned. A French Court made an analogous argument in 2000 when it required Yahoo! to prevent French network users from accessing message boards where users can trade in Nazi memorabilia.

On the other hand, a US Federal court struck down a Pennsylvania law that forced Internet service providers to block access to sites thought to be distributing child pornography,

[10] BBC News, "Mobile censorship" for under-18s, 19 January 2004.

[11] Sjoera Nas, Bits of Freedom, *The Multatuli Project: ISP Notice & take down*, 1 October 2004.

by filtering the IP addresses.[12] Because over 80 per cent of websites on the Internet are served from IP addresses that are shared amongst sites, it was argued that the law overblocked legitimate sites. The court agreed with this contention, concluding that

> with the current state of technology, the Act cannot be implemented without excessive blocking of innocent speech in violation of the First Amendment.[13]

These three decisions all have differing conceptions of the technology. Technology can be constructed to limit access, according to the dissenters in the CDA decision and the French court, while in the Pennsylvania case the technology to limit access also limited access to protected speech, and was thus unconstitutional.

If every user was compelled to disclose this information, these regulations could work. Then if she was under 18 she could not access pornography; if she was from France, she could not access sites that trade in Nazi memorabilia. The Pennsylvania problem does not go away in her case, but if we also required that all those who speak (and set up websites) must first identify themselves, then it is likely that he would risk prosecution. It is also possible that if they both knew that this level of information was available and required in order to speak and gain access to speech, they would probably not bother in the first place. This is the way that surveillance can act as prior restraint, chilling free speech by threatening surveillance.

This is in essence what is occurring currently in the surveillance of subscriber and traffic data, but is being exhibited in two different ways on both sides of the Atlantic Ocean. In North America, under claims of copyright infringement, content-producing industry associations such as the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), and the Canadian Recording Industry Association (CRIA) are approaching ISPs to demand subscriber information based on IP addresses. That is, the RIAA and the MPAA are capturing IP addresses of individual users and approaching ISPs so that they will disclose customer information, informing the RIAA and MPAA which user was using what IP address at what moment. Once legal avenues are opened to allow industry associations access to this information, these same avenues will be used by others. In so doing we will increase the use of subscriber information and other sensitive information for any number of purposes.

In Europe, the surveillance of traffic data is not yet focused on copyright infringement policies, but it soon will be, and when combined with anti-terrorism policies, it could be disastrous. Currently various governments in the European Union are establishing national policies that compel communications service providers (telephone companies [land and mobile], ISPs, etc.) to *retain* their traffic data logs. Under previous law, these service providers would have to delete this personal information once it was no longer necessary for billing or engineering purposes. Now in countries like Italy, France, and the United Kingdom, service providers will have to retain this information regarding users' e-mail, Internet and telephone habits (and locations) for periods ranging between one and five years. The UK, France, Ireland and Sweden are also pushing for this policy to be adopted at the EU, thus obliging all countries to compel all communications providers throughout

[12] Tom Zeller Jr., Court Rules Against Pennsylvania Law That Curbs Child-Pornography Sites, 11 September 2004.

[13] *Center for Democracy & Technology v. Pappert,* United States District Court for the Eastern District of Pennsylvania, No. 03-5051, 10 September 2004.

Europe to keep this information for a number of years, just in case one day this information is of value to law enforcement authorities.[14]

The surveillance of subscriber and traffic data is tantamount to the collection and tracking of all human conduct in the Information Society: who we speak with, who we move with, what we look for, where we receive information from, and where we send it to. As a result of these policies, European users of the Internet will have to grow accustomed to the idea that their actions will be logged for a number of years and accessible to any government that is interested, and possibly others. North American users live under the threat of their personal information being divulged to the content industry which would result in further legal proceedings. If the users are aware of these policies and mechanisms it could chill their ability to create and impart information, hampering their right to free speech. They would be less likely to consult "controversial" information for fear that it will eventually be used against them. On the other hand, if they are unaware of these policies the users will not be changing their conduct in the face of one of the largest threats to personal privacy in the modern era.

The Politics of Security-Induced Censoring. An increasingly common argument for creating structures to limit free expression is that it will aid in the war on terror. Some countries have returned to the public state of fear in which the US found itself at the time of the *Abrams* case during the First World War. Governments have called for stricter rules, greater powers, and increased funding to combat terrorism, and it was inevitable that these changes would have effects on free expression.

There are many instances of countries announcing the "takedown" of websites hosting "radical" Islamist material. In reaction to the assassination of a Dutch film director, Belgium announced its intention to shut down certain Islamic websites and closely monitor radio programmes promoting violence.[15] A number of anti-terrorism laws introduced around the world involved curbing hate speech. In reaction to threats made on websites or the posting of messages from terrorists, websites have been removed or their contents blocked. It is likely that the website logs were also seized in this process.

One example of this is what happened to Indymedia. The Independent Media Center is an international news network of individuals, independent and alternative media activists and organizations. On 7 October 2004 its servers were seized from the London office of Rackspace, a server-hosting firm. The loss of these servers resulted in the removal of content from twenty news websites. Rackspace received a US Court order to hand over the servers in London. According to the General Secretary of the National Union of Journalists in the UK

> To take away a server is like taking away a broadcaster's transmitter. It is simply incredible that American security agents can just walk into a London office and remove equipment.[16]

The reason for the seizure remains under seal, and no US law enforcement agency has taken responsibility for the investigation into Indymedia. No UK law enforcement authorities were involved in the seizure, even though it took place in London. A public prosecutor in Italy admitted that she did request the IP logs from the server through a request to the American authorities, on grounds of combating terrorism.

[14] Privacy International, *Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention*, 15 September 2004.

[15] Reuters, "Mosques, Islamic school attacked in the Netherlands", *Financial Times*, 8 November 2004.

[16] Indymedia UK, *Ahimsa Gone and Returned: Responses to the Seizure of Indymedia Harddrives*, 09.11.2004 19:56.

There was apparently also a request from the Swiss authorities, but this cannot be confirmed either.[17] This is the new face of censorship.

Another example of a law developed to combat terrorism that increased surveillance at ISPs is the USA PATRIOT Act, passed by the US Congress in October 2001. Under the USA PATRIOT Act, the Federal Bureau of Investigations may demand information from Internet service providers by showing a "national security letter", without any judicial oversight. ISPs are then required to comply and are gagged from disclosing their compliance. The NSLs are issued without any judicial review, or any requirement to show individualized suspicion, compelling need, and it cannot be contested.[18] The American Civil Liberties Union challenged this procedure on many grounds including that it chilled First Amendment rights. In September 2004 a US District judge agreed. Referring to *Talley v. California*, and other decisions on restraint on freedom of association,

> The Court concludes that such First Amendment rights may be infringed […] in a given case. For example, the FBI theoretically could issue to a political campaign's computer system operator a […] NSL compelling production of the names of all persons who have email addresses through the campaign's computer systems. The FBI theoretically could also issue an NSL […] to discern the identity of someone whose anonymous online web log, or 'blog,' is critical of the Government. […] These prospects only highlight the potential danger of the FBI's self-certification process and the absence of judicial oversight.[19]

The Court also argued that "transactional records" deserve privacy protection, despite existing jurisprudence on telephone traffic and bank records that leaves Internet traffic data in legal limbo:

> NSLs can potentially reveal far more than constitutionally-protected associational activity or anonymous speech. By revealing the websites on visits, the Government can learn, among many other potential examples, what books the subscriber enjoys reading or where a subscriber shops.

Without judicial review, the Court concluded, this power was unconstitutional.

Surveillance has indeed been used to limit political activity. These policies are not limited to online activity either. Surveillance has been used as a coercive measure to prevent or disable free assembly. In August 2004 the UK Appeals Courts approved of the United Kingdom Government's use of stop and search powers at protests. This involved a case where police stopped-and-searched attendees of a protest outside an arms fair in London. The police were empowered to stop and search anyone in the city of London without any precondition of reasonable grounds of suspicion. During the course of the case, it was discovered that since February 2001, this authority, granted to the Government under the Terrorism Act 2000, has been in effect on a rolling basis.[20]

Similarly, in the summer of 2004 during the American political campaign season, anti-terrorism powers were used against protestors at the presidential conventions. First the FBI would surveil activists using the Internet, and then interrogate activists before the conventions.[21] Later, at the Republican

[17] Electronic Frontier Foundation, Indymedia Server Seizures <http://eff.org/Censorship/Indymedia/>

[18] Anita Ramasastry, *Why the Court Was Right to Declare a USA Patriot Act Provision Dealing with National Security Letter Procedures Unconstitutional*, FindLaw Legal Commentary, 13 October 2004.

[19] *John Doe, ACLU v. Ashcroft*, 04 Vic. 2614, United States District Court Southern District of New York, 28 September 2004.

[20] Privacy International, *UK Appeals Court Approves Stops and Searches at Protests*, 8 August 2004.

[21] ACLU, *ACLU Denounces FBI Tactics Targeting Political Protesters*, 16 August 2004.

Convention, New York police routinely fingerprinted 1,500 people arrested during the convention. This fingerprinting had the effect of delaying the release of detainees.[22]

In another American case, police installed metal detectors to scan protestors at an annual protest at the School of the Americas in Georgia. On average 15,000 people attend these yearly protests, and in the 13 years of protests, no weapons have ever been found and no protestor ever arrested for an act of violence. A week before the November 2002 protest, the City of Columbus instituted police requiring all protestors to submit to a metal detector search at a checkpoint away from the protest site. If metal was detected in the scan, the police would search through the protestor's belongings. The City claimed that the decision was due to the elevated risk of terrorist attack, prior "lawlessness", and problematic "affinity groups". The Circuit Court in this decision, known for often conservative decisions,[23] decided that the practice violated the Fourth Amendment to be free of "unreasonable search and seizures" as "there is no basis for using September 11 as an excuse for searching the protestors", and "September 11, 2001, already a day of immeasurable tragedy, cannot be the day liberty perished in this country." The Court also found that the practice violated the First Amendment by burdening free speech and association, that the checkpoints and searches were a form of prior restraint, and that the policy was content-based in that it was geared towards these protestors on this issue. Finally, the Court concluded that the search constituted "an 'unconstitutional condition;' protestors were required to surrender their Fourth Amendment rights in order to exercise their First Amendment rights."[24]

In the coming months and years more decisions will emerge from courts around the world, and they are equally as likely to conflict with one another as they are to lead to a renewed right to free expression. Each case and every decision highlights the tightening relationship between surveillance and censorship, and the risks to privacy and free expression emerging from our responses to terrorism.

Paths to Re-invigorating the Open Society and Protecting the Marketplace. When we imagine the right to free expression, as it is enshrined in constitutional and international human rights declarations and treatises we imagine situations involving small printing presses distributing revolutionary material under an oppressive regime. Certainly the pro-Soviet Abrams and his colleagues believed that they were revolutionaries when they printed pamphlets during the First World War. Or Talley when he appealed to consumers regarding discriminatory hiring practices. Or McIntyre who insisted on publishing pamphlets despite regulations by the state of Ohio. We do not imagine people trying to download pornography, share copyrighted music illegally as champions in an oppressed world. Yet the fight for both types of people, those who are struggling against oppression and for justice, and those who wish to impart and access information are one and the same. Once we start building mechanisms to control one, the others will also be affected.

It is hard to believe, but is true nonetheless, that we need unfettered speech and privacy rights to ensure the marketplace of ideas, that will sustain the open society. Unless people can

[22] Diane Cardwell, "City Challenged on Fingerprinting Protesters", *The New York Times*, 5 October 2005.

[23] C.G. Wallace, "Screening of Protesters Unconstitutional, Court Rules", Associated Press published in *Washington Post*, 17 October 2004.

[24] *Bourgeois et al. v. Peters et al.*, United States Court of Appeals for the Eleventh Circuit, No. 02-16886, 15 October 2004.

speak freely, and not be encumbered by surveillance, particularly from recent policies and practices created to combat terror, then we will not have the dream that we once had, of a place where we can all come together and communicate, separate from flesh and steel.

If we are still seeking such a world, and I think we are, then we need to fix many things. We need to understand that a zone of autonomy exists around all individuals, supported, enhanced, and protected by privacy. This will be supported through laws upholding long-respected rights to be secure from interference.

We also need to halt this alarming progression of policies and practices introduced with the intent of combating terrorism, that in the end have the effect of reducing our rights collectively. We do indeed live in perilous times, just as we did when Abrams was of issue at the end of the Great War. I acknowledge that Oliver Wendell Holmes, whom I celebrate in this paper, actually was quite unforgiving in two previous cases involving similar wartime activity, and wrote opinions condemning the accused. But I remain optimistic. Just as Holmes turned the bend and acknowledged that war does not mean the suspension of rights, and just as the US jurisprudence followed in the 1960s, and reaffirmed in the Georgia decision, rights may prevail.

If rights prevail, then the marketplace of ideas may be secured. I imagine it will be a struggle, but this is not a bad thing in itself. As Holmes noted, when speech is threatened it only reaffirms its importance. Speech is only valuable when governments try to limit it. And as he says, the "ultimate good desired is better reached by free trade in ideas." We dreamed that the Internet would sustain this marketplace, which in turn would sustain the open society. We were wrong, but our goals remain intact.

Our reasons are thus noble, as we recognize that any incursion upon free expression, even the smallest, interferes with the marketplace of ideas. This marketplace is too important to sustaining an open society to have it damaged. It offends me to see limits placed upon this marketplace, as it offends others too. And these “others” will be visionaries, coming up with legal, political, and technological innovations that may yet deliver on that dream, and bring us in from the cold.

Amsterdam Recommendations
14 June 2003
Freedom of the Media and the Internet

Convinced that no matter what technical means are used to channel the work of journalists to the public – be it TV, radio, newspapers or the Internet – the basic constitutional value of freedom of the media must not be questioned;

Reaffirming that this principle, which is older than most of today's media, is one that all modern European societies are committed to;

Alarmed that censorship is being imposed on the Internet and new measures are being developed to prevent the free flow of information;

Reaffirming the principles expressed in the Joint Statement by OSCE, UN and OAS in London on 20 November 2001;

Taking note of the Council of Europe Declaration on freedom of communication on the Internet from 28 May 2003;

The OSCE Representative on Freedom of the Media invited representatives from academia, media, specialized NGOs from Europe and the US as well as from the European Parliament, Council of Europe, European Commission, and OSCE to take part in a conference on "Freedom of the Media and the Internet" held 13-14 June 2003 in Amsterdam, the Netherlands.

During the conference the following recommendations, proposed by the OSCE Representative on Freedom of the Media, were made:

Access

- The Internet provides a number of different services. Some of them are still in the development phase. They serve as tools, often indispensable ones, for citizens as well as journalists and thus are important for a free media landscape. The technology as such must not be held responsible for any potential misuse. Innovation must not be hampered.
- Access to digital networks and the Internet must be fostered. Barriers at all levels, be they technical, structural or educational, must be dismantled.
- To a considerable extent the fast pace of innovation of digital networks is due to the fact that most of the basic code and software are in the public domain, free for everyone to use and enhance. This free-of-charge infrastructure is one of the key elements of freedom of expression on the Internet. Access to the public domain is important for both technical and cultural innovation and must not be endangered through the adoption of new provisions related to patent and copyright law.

Freedom of Expression

- The advantages of a vast network of online resources and the free flow of information outweigh the dangers of misusing the Internet. But criminal exploitation of the Internet cannot be tolerated. Illegal content must be prosecuted in the country of its origin but all legislative and law enforcement activity must clearly target only illegal content and not the infrastructure of the Internet itself.
- The global prosecution of criminal content, such as child pornography, must be warranted and also on the Internet all existing laws must be observed. However, the basic principle of freedom of expression must not be confined and there is no need for new legislation.
- In a modern democratic and civil society citizens themselves should make the decision on what they want to access on

the Internet. The right to disseminate and to receive information is a basic human right. All mechanisms for filtering or blocking content are not acceptable.

- Any means of censorship that are unacceptable within the "classic media" must not be used for online media. New forms of censorship must not be developed.

Education

- Computer and Internet literacy must be fostered in order to strengthen the technical understanding of the importance of software and code. This is necessary so as to keep open a window of opportunity for defining the future role of the Internet and its place in civil society.
- Internet literacy must be a primary educational goal in school; training courses should also be set up for adults. Special training of journalists should be introduced in order to facilitate their ability to deal with online content and to ensure a high standard of professional journalism.

Professional Journalism

- More and more people are able to share their views with a widening audience through the Internet without resorting to "classic media". Privacy of communication between individuals must be respected. The infrastructure of the Internet is used for many different purposes and any relevant regulatory bodies must be aware of that.
- Journalism is changing in the digital era and new media forms are developing that deserve the same protection as "classic media".
- Traditional and widely accepted values of professional journalism, acknowledging the responsibility of journalists, should be fostered so as to guarantee a free and responsible media in the digital era.

The Authors

Yaman Akdeniz is a lecturer at the School of Law, University of Leeds where he teaches about Internet-related legal and policy issues. He is also the director of the LLM programme in CyberLaw as well as the founder-director of Cyber-Rights & Cyber-Liberties (UK), a non-profit civil liberties organization. Dr. Akdeniz was an international policy fellow of the Open Society Institute working on a project about the development of an Information Society in Turkey. His publications include *Sex on the Net¿ The Dilemma of Policing Cyberspace* (1999); *The Internet, Law and Society* (ed. with C. Walker and D. Wall, 2000); and *Regulation of Investigatory Powers Act 2000: Bigbrother.gov.uk: State Surveillance in the Age of Information and Rights*. His forthcoming publications include *Internet Child Pornography and the Law: National and International Responses* (to be published in early 2005).

Arnaud Amouroux is Assistant Project Officer at the Office of the Representative on Freedom of the Media, which he joined in February 2004. He was an OSCE long-term electoral observer in Georgia in 2003. He holds a master's degree in Political Sciences and a postgraduate diploma (DESS) in International Administration Law from the Université Panthéon-Sorbonne of Paris. He has studied in Cardiff and Milan.

Marcel van den Berg works for the Dutch National Police where he specializes in Internet investigations. He is currently an Internet specialist at the National High Tech Crime Center.

Steve Buckley is a communications activist and media policy consultant with particular interests in communication for development, freedom of expression and communication rights. He has been a member of the International Board of the World Association of Community Radio Broadcasters (AMARC) since 1992 and President of AMARC since 2003. He is also a member of the Executive Secretariat of the Communication Rights in the Information Society campaign (CRIS) and a member of the International Council of IFEX, the International Freedom of Expression Exchange. Steve was a founder of the UK Community Media Association in 1983 and its Chief Executive from 1991 to 2004.

Cormac Callanan is Secretary General and past-president of INHOPE – the association of Internet Hotline Providers. The mission of INHOPE is to facilitate and co-ordinate the work of Internet hotlines responding to illegal use and content on the Internet. He was founding Chairman of the ISP Association of Ireland and Secretary General of the European Service Provider Association until February 2003. He was founding Director of the Irish www.hotline.ie service responding to reports about illegal child pornography and hate speech on the Internet. He established the first commercial ISP business in Ireland in 1991, EUnet Ireland. Cormac is a board member of the Copyright Association of Ireland. He served on the Rightswatch UK & Ireland Working Group developing best practice guidelines for notice and takedown procedures as they relate to intellectual property rights (IPR).

Sylvie Coudray has worked at UNESCO since 1989 in the Division of Freedom of Expression, Democracy and Peace (FED). She is responsible for the planning, co-ordination and organization of the World Press Freedom Day in close co-operation with the UN and NGOs. Ms. Coudray has also worked on media in conflict areas. She was involved in the preparation of the World Summit on the Information Society, focusing on issues concerning freedom of expression.

Nico van Eijk is a professor of Media and Telecommunications Law at the Institute for Information Law (IViR) in Amsterdam, the Netherlands. He was awarded his doctorate from the University of Amsterdam in 1992 for a thesis on "Government interference with broadcasting". He also works as a legal adviser to Rabobank International and the law firm Nauta Dutilh. He is the Vice-Chairman of the Dutch Federation for Media and Communications Law (VMC) and a member of various advisory boards.

Kurt Einzinger studied in the Department of Atomic Energy at the Institute of Technology, Vienna. He was awarded his PhD in Social Anthropology from the University of Vienna for field research in India. He has written for and edited several magazines and has directed the IT departments at the SPÖ Headquarters (1989–96), GiroCredit Bank (1996–97), Erste Bank Informatics (1997–98) and Österreichische Kontrollbank (1998–99). Since 1999 he has been Secretary General of ISPA (Internet Service Providers Austria). He is also a member of the Austrian Data Protection Council and Vice President of EuroISPA.

Colin Guard is the Regional Program Manager for Central Asia of the Internet Access and Training Program (IATP), a programme funded by the Bureau of Educational and Cultural Affairs of the United States Department of State and administered by the International Research and Exchanges Board (IREX). In Central Asia, IATP consists of a network of 66 Internet access sites in Uzbekistan, Kazakhstan, Kyrgyzstan, Tajikistan and Turkmenistan. Previously, Colin was the IATP Regional Program Manager for Western Eurasia, responsible for a network of 42 Internet access sites in Ukraine, Belarus and Moldova. Before joining IREX, Colin worked on a higher education reform project at the Salzburg Seminar. Colin has an M.A. in Russian from Middlebury College, and has studied in Vladivostok, Novosibirsk and Moscow.

Miklós Haraszti is a Hungarian writer, journalist, human rights advocate and university professor, who was appointed the OSCE Representative on Freedom of the Media in 2004. He was born in Jerusalem in 1945 and studied Philosophy and Literature at the University of Budapest. He received in 1996 an honorary degree from Northwestern University in the United States. In 1976, Mr. Haraszti co-founded the Hungarian Democratic Opposition Movement and in 1980 he became editor of the samizdat periodical *Beszélo*. In 1989, he participated in the round-table negotiations on transition to free elections. A member of the Hungarian Parliament from 1990 to 1994, he then became a lecturer on democratization and media politics at various universities. Mr. Haraszti has written several essays and books, including *A Worker in a Worker's State* and *The Velvet Prison*, both of which have been translated into several languages.

Pascal Hetzscholdt works for the Dutch National Police in the fields of cyber intelligence, cyber security and the fight against cybercrime. He is the strategic adviser for the National High Tech Crime Center.

Lee Hibbard works as an administrator at the Council of Europe and has been dealing with, *inter alia*, the Convention on legal co-operation and information concerning "Information Society Services" (CETS 180) and questions concerning private international law often in co-operation with many Central and Eastern European States. He is now working for the Media Division of the Council of Europe and is actively involved in the area of the media, human rights and the Information Society.

Gus Hosein is a Senior Fellow at Privacy International (PI), a London-based watchdog organization. At PI he directs a programme that researches international anti-terrorism policies and their implications for civil liberties. He also advises a number of non-governmental organizations on issues relating to censorship, surveillance, and governance. He is a Visiting Fellow at the London School of Economics and Political Science where he lectures on topics related to the Information Society, data protection and privacy, regulation and technology. He holds a B.Math from the University of Waterloo and a PhD from the University of London.

Hans J. Kleinsteuber has been a professor of Political Sciences and Journalism at Hamburg University since 1982. He teaches media policy from a comparative perspective, the Internet, electronic democracy and public spheres. Prof. Kleinsteuber was nominated by the German Government to be Chairman of the Online Programming Committee for *Deutsche Welle*. He is Head of the Research Centre for Media and Politics at the Institute for Political Science. Prof. Kleinsteuber is a member of the Group "Cyberdemocracy" in COST A 14/EU, curator of the association politik-digital.de/europa-digital.de and has worked for the German branch of UNESCO. His recent publications include *Information Superhighway in the US* (1996); *Information Highway in Hamburg* (1997); *Recent Trends in US Media* (2001), and *Handbook on Media and Journalism* (2005).

Morris Lipson is a lawyer currently working for Article 19, an international NGO campaigning for free expression by providing legal analysis and consultation. He was external consultant for the UN Office of the High Commissioner for Human Rights in Geneva. He produced a study for OHCHR on Racism and the Internet, published by UNESCO. He also worked on a compilation of anti-racism practices.

Christopher T. Marsden is a cyber-law writer, researcher and consultant. His research at Oxford University's Centre for Socio-legal Studies PCMLP focuses on broadband mobile Internet regulation and policy. He was the project manager of the IAPCODE project in 2004 and is a Scholar in Residence at the Stanhope Centre, London. His latest publications are at www.selfregulation.info. He has written chapters in *Internet Television* (ed. Eli Noam et al., 2003) and *Digital TV in Europe* (eds. Picard and Brown, 2004, with Monica Arino) both published by Lawrence Erlbaum. He has edited the following collections of essays: *Convergence in European Digital TV Regulation* (1999, with Stefaan Verhulst) and *Regulating the Global Information Society* (2000).

Dejan Milenković graduated from Belgrade University Law School in 1994. He works as a Professor of Business Law and Environmental Law and Regulations in Serbia at the University of Belgrade. As a founding member and full-time legal expert for the Lawyers Committee for Human Rights (YUCOM), since 1997 he has engaged in various legal and human rights related projects and activities. He collaborated with the OSCE Mission to Serbia and Montenegro on the issues of self-government and media regulation (2002–2004).

Christian Möller has been Project Officer at the Office of the OSCE Representative on Freedom of the Media in Vienna since 2003. From 1999 to 2002 he worked for the *Unabhängige Landesanstalt für das Rundfunkwesen* (ULR) in Kiel, one of Germany's federal media authorities. He holds an M.A. in Media Studies, German Language and Public Law from Christian Albrechts University, Kiel. His publications include *From Quill to Cursor: Spreading the Word on the Internet* (2003, ed. with Christiane Hardy) and *The Impact of Media Concentration on Professional Journalism* (2003, with Johannes von Dohnanyi).

Mogens Schmidt joined UNESCO in 2003 where he was nominated Director of the Division for Freedom of Expression, Democracy and Peace. After teaching Literature and Mass Communication at the University of Aarhus, he was nominated Managing Director of the Danish School of Journalism in 1988, where he was one of the initiators of the European Journalism Training Association. His dedication to international collaboration was reflected in the media assistance projects run by the Danish School of Journalism, primarily in Central and Eastern Europe and the Balkans, but also in Mongolia and southern Africa. In 1995, he was appointed Director at the European Journalism Centre in Maastricht, the Netherlands. In 2001, Schmidt joined the World Association of Newspapers (WAN) as Assistant Director General. He is the author of many books and articles about journalism, mass communication and press freedom.

Margaret Skok is Director in charge of International Marketing and Government Relations with Media Awareness Network (MNet). She is currently on Executive Interchange with MNet, hosted by the Department of Canadian Heritage. Her focus is corporate and policy work. She functions as lead support to the Board of Directors on sustainability issues related to all levels of government and international development. Margaret has held several policy, trade development and trade policy positions with the Federal Government, both in Canada and overseas, with experience in the departments of Fisheries and Oceans, Agriculture and Agri-Food Canada, Foreign Affairs Canada and Canadian Heritage.

Sandy Starr is technology editor and public relations officer at the online current affairs publication spiked *www.spiked-online.com*. He also writes on technology and culture for print publications ranging from the *Times Literary Supplement* to *The Sun* newspaper, and for online publications stretching from *openDemocracy* to *Tech Central Station*. He has worked with the European Commission research project RightsWatch on copyright regulation issues, and with the OSCE on Internet regulation more broadly. He is a passionate believer in unqualified freedom of speech.

Jelena Surčulija is a lawyer currently reading for the LLM in Computer and Communications Law at Queen Mary, University of London. She has worked as a legal consultant to GIPI (Global Internet Policy Initiative) and as an external consultant and media legislation expert to the OSCE Mission to Serbia and Montenegro. Ms. Surčulija graduated from the University of Belgrade, Faculty of Law, in 2000 and completed the Media Law Advocates Training Programme at the PCMLP, Oxford University, in 2002. She is a founder member of the International Media Lawyers Association. She was actively involved in drafting new media laws in Serbia, initiated and assisted the establishing of the Association of Internet Service Providers and of Internet Users. She has held training courses for journalists on Article 10 ECHR and on media legislation. Her publications include *The Legal Situation in Serbia* (SEEMO Handbook 2003/04) and a study *The European Legal Framework for ICT in Serbia*.

Jane Tallim works as a senior educator with Media Awareness Network (MNet). She is the author of Reality Check!, a comprehensive module for students in Grades 9 to 12 about authenticating online information, as well as the lead researcher and producer of the authentication of online information, and marketing/advertising and privacy components of the Web Awareness Canada professional development programme. Jane manages the “For Teachers” section of the MNet website and creates educational resources on a wide range of media-related topics. She promotes MNet to educators through national and international speaking engagements and is MNet’s primary professional development trainer.

Cathy Wing is Director of Community Programming at Media Awareness Network (MNet), a committed Canadian NGO in the field of educating young Internet users and developing online literacy. She manages partnerships with parent and community organizations, as well as creating resources for these sectors. Cathy’s career includes working in the film and television industries as project manager and television news producer.

www.osce.org/fom

Yaman Akdeniz
Arnaud Amouroux
Marcel van den Berg
Steve Buckley
Cormac Callanan
Sylvie Coudray
Nico van Eijk
Kurt Einzinger
Colin Guard
Miklós Haraszti
Pascal Hetzscholdt
Lee Hibbard
Gus Hosein
Hans J. Kleinsteuber
Morris Lipson
Christopher T. Marsden
Dejan Milenković
Christian Möller
Mogens Schmidt
Sandy Starr
Jelena Surčulija
Cathy Wing