Spreading the Word on the Internet

The Representative on
Freedom of the Media

16 Answers to 4 Questions

Reflections on
Freedom of the Media and the Internet
Amsterdam Conference, June 2003

osce

VIENNA 2003

OSCE

REPRESENTATIVE ON FREEDOM OF THE MEDIA

Spreading the Word on the Internet

16 Answers to 4 Questions

Reflections on
Freedom of the Media and the Internet
Amsterdam Conference, June 2003

Edited by
Christiane Hardy and Christian Möller

Vienna 2003

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 Foreign Ministry of the Netherlands
for its 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

Photograph on the cover: Arie Kievit/HH

Design: WerkstattKrystianBieniek, Vienna

Contents

What is the situation of Freedom of the Media and the Internet in the OSCE region?

Regulation of decentralized networks: a problem or a necessity for freedom of expression?

The technical and economic framework: How are code and companies influencing Freedom of the Media on the Internet?

How to ensure Freedom of the Media on the Internet in the OSCE region?

Freimut Duve
Preface

After Gutenberg's print centuries telephone, fax, radio and television seemed for a long time to be the twentieth century's modern tools of communication and news distribution. But with the Internet and the WWW a revolutionary technical infrastructure changed not only forms of individual communication but also the way the news is distributed within countries and across borders. What has not changed, however, is the principle of freedom of the press and the fact that free media are an essential part of modern democracies.

New channels of media distribution must not serve as an excuse for new measures of censorship. Whatever was not in line with OSCE commitments regarding freedom of the media in the 'offline world' will not be tolerated in the 'online world'. But it is not only explicit censorship – the blocking or filtering of content – that poses a danger to the free exchange of information on the Internet. The perils are manifold and also encompass excessive regulation by States and governments. Overwhelming copyright law might drain the intellectual commons; self-regulation might move decisions on questionable content from courts to companies; technical standardization might lead to circumstances that influence our daily life. And structural censorship or harassment of journalists do not differentiate between online and offline publications.

Although a small part of the Internet contains criminal content or hate speech, regulation must not target the Internet as a whole or choke technical innovation. Illegal content cannot be tolerated and should be prosecuted in the country of its origin. However, uniform standards cannot be imposed on a global medium at the level of the lowest common denominator.

A developed infrastructure and the responsible use of it are the two crucial factors relating to freedom of the media on the Internet. To find out more about these two aspects my Office organized the conference on ‘Freedom of the Media and the Internet’ in June 2003 in Amsterdam. At the end of this conference the Amsterdam Recommendations were drawn up, which stress the importance of these two sides once again. This publication combines a number of answers to questions that were discussed during this conference.

Vienna, September 2003

Felipe Rodriquez and Karin Spaink
Introduction

Rights and Regulations

Ever since the Internet started to become a popular medium, strong concerns have been voiced about a small amount of content that is distributed on the Internet. There has been extensive media coverage of the dissemination of child pornography, hate speech, racial discrimination, neo-Nazi propaganda, political speech and other types of content that some governments in some countries find offensive.

Different nations have acted in different ways in response to these issues. Some have initiated government-sanctioned censorship of content on the Internet, others have promoted the implementation of industry self-regulation as a method of enforcing local standards. With the exception of several non-democratic countries, none of the attempts to ban illegal and harmful content on the Internet has been successful.

The easiest type of content to ban from the Internet is child pornography. It is relatively easy to act against because child pornographic content is illegal in virtually every country in the world. Therefore, a certain level of international co-operation between law enforcement agencies to find and prosecute the individuals that distribute this type of content can be effectuated without too many hindrances. A number of successes in this area have been attained: law enforcement agencies in recent years have become more skilled at tracking down distributors and passing this information to relevant agencies in other countries. As a result, large groups of child pornography distributors have been caught and prosecuted.

Most other types of content are much more difficult to act against on the Internet, the prime reason being that there is no international agreement about the legality of the content under dispute. An example is neo-Nazi propaganda; most European nations would like to ban neo-Nazi propaganda from the Internet, but other nations protect this type of content under their freedom of expression legislation.

Once content is (legally) published on the Internet in one country, it is freely available in all other countries connected to the Internet. Users can freely fetch all information available, no matter from where it originates and under which law it was legitimately published. Their local laws might be at odds, but in general, trying to enforce local standards on participants in a global network is futile. This concept in itself renders the notion of enforcing local legislation to ban hate speech and types of political speech rather meaningless. If one accepts the axiom that nations are entitled to have their own cultural and political values and have the right to implement these into national legislation, one must by necessity refrain from attempting to enforce global standards of what is and what is not acceptable on the Internet. If not, one would basically be forcing other countries to drop their own values.

After all, content that is deemed to be harmful, dangerous or perverse in one nation, can be perfectly acceptable in another, and thus – because of the nature of the Internet – it will be freely accessible in both. In other words: governments have to come to grips with the fact that such content cannot be removed from the Internet and that their citizens cannot be prevented from accessing internationally available material, unless these same governments are willing to eradicate all cultural and political differences between the various nations that together form the global fabric.

One important difference between printed and broadcast media on the one hand and digital media on the other may help governments to tolerate this – for them – often difficult notion of accepting national differences and the ensuing impossibility to enforce local standards. While printed and broadcast media are characterized by their one-to-many nature, and cannot allot time and space to each and any opinion or refutation thereof, the Internet has unlimited space. Anybody who wants to publish an opinion or counteract a certain (political) viewpoint on the Net can do so, be it on their own website or on Usenet. People who publish on the Net are not dependent on editors to give them space or time. Thus, many more voices are being heard on the Net and, while some of them might be questionable, there is at the same time quite an abundance of people who will take great efforts to painstakingly refute and counter such opinions.

The interesting effect is that those who argue against opinions deemed politically undesirable or dangerous, depend on the presence of those opinions in order to document and present their *own* counter case. A beautiful example is Nizkor (Hebrew for 'We will remember', see <www.nizkor.org>), an elaborate website that refutes claims made by neo-Nazis in great detail. Nizkor presents original historical records and events, lists and undermines various ploys to deny the Holocaust, and – through their presence on the Internet – tracks the movements and associations of neo-Nazis and their organizations.

Various attempts have been made by European governments to censor content on the Internet by implementing technical solutions (such as filtering or blocking). None of these attempts have been a complete success, one reason being because content on the Internet is very easy to copy and can then be republished in a different location; this technique is called ‘mirroring’. Traditionally, content targeted by censorship is often mirrored on many other places on the Internet, rendering such technical censorship ineffective.

However, the implementation of technical censorship on the Internet invariably causes collateral damage, as the example of the German censorship of the Dutch Internet provider XS4ALL in 1996 proves. A customer of this provider published a German ultra left magazine on his website that contained two articles with instructions on how to sabotage railway lines destined to be used for nuclear transports. While this magazine (*Radikal*) is banned in Germany, and possession of it is illegal in that country, the publication was not illegal in the Netherlands. The German authorities, the *Bundesanwaltschaft*, forced German commercial and academic Internet providers to block the XS4ALL website to prevent Germans from accessing the publication. German providers proceeded to block access to the entire XS4ALL domain. Tens of thousands of completely legal publications were also blocked as a consequence of this action, and thus became the collateral damage of a very coarse censorship act. The end result for the German Government was nil, as the *Radikal* publication was copied to many different websites around the world, and is still available on the Internet today, seven years later. Indeed, the act of censorship caused proliferation of the banned content instead of its discontinuation.

Various governments have implemented content regulations to ban specific content from the Internet. The problem with these regulations is that national regulation has a local focus and limitation; it can only affect content in the country of origin and has no effect on content outside that country. Therefore, virtually all national Internet content regulation systems are ineffective and useless. They basically serve no other purpose than political window dressing: the internal ban might work, but the material in question can still be accessed from locations outside the national jurisdiction as if nothing had happened.

A lot can be learned from the Australian Internet content censorship bill that was passed in 1999. This censorship framework was implemented in 2000 to protect minors from offensive content. A study by the Australia Institute in 2003 demonstrated that the Australian censorship framework was completely ineffective, and that minors could – and did – access any type of content on the Internet.

Another way governments have tried to deal with content on the Internet is by promoting the concept of industry self-regulation. In 1996, when governments became aware of the nature of the Internet and called for action, the Internet industry stakeholders called for self-regulatory action as opposed to government regulation.

The Internet has a long tradition of self-regulation. Various protocols and networks on the Internet are managed and co-ordinated by its users. Examples are the Usenet newsgroup hierarchy and the Internet Relay Chat networks, which have no central management, but are kept in working order by volunteers without a central hierarchy. The engineering of new protocols and the implementation of new technology on the Internet is also largely the result of the work of Internet users and experts who co-operate without any central hierarchy or organization; instead, the modus operandi is community consensus, based on open discussion, public engagement, expert input and transparency.

The type of industry self-regulation on the Internet that has been promoted by governments differs radically from the traditional Internet self-regulation. Industry self-regulation is usually co-ordinated by industry associations, there is no public participation, and the actions of industry self-regulation are usually not transparent to the public, nor is there a possibility to appeal against decisions. Hence, industry self-regulation is a misnomer: Internet users are not regulating themselves, on the contrary, it is the industry imposing its regulations upon users. In practice, industry self-regulation is regulation by the industry of the Internet community. Thus, a better term would be 'industry regulation' omitting the world 'self'.

Moreover, in many instances the industry didn't start this practice of self-regulation of its own accord: there was a clear threat that if the industry didn't impose rules upon itself and on users soon, the government would. Hoping to both prevent stricter (government imposed) rules and to codify their own influence, the industry as a whole opted for this so-called 'self-regulation', thereby – as many critics have stated – accepting and furthering the process of the privatization of state censorship. The industry ends up being the governments' handmaiden, while users are simultaneously deprived of their democratic and judicial rights: there is no voting, no public participation or representation, no accountability, no redress and no transparency.

Leaving enforcement of Internet regulations to the industry is a fundamentally flawed concept, because the industry is driven mainly by a profit motive and not motivated by the civil rights of Internet users. The profit motive causes industry players to have risk-averse behaviour, which can infringe citizens' rights of expression. In addition to industry self-regulation, the industry often uses the licence agreement with its customers to ban content or ban the customer. When users are confronted by their providers they usually have nowhere to turn, and are faced with an asymmetric balance of power. If anything Internet citizens need stronger protection of their rights, to be protected from industry initiatives that are overly restrictive or obscure.

Due to the widely varying nature of content on the Internet, it is natural that some people are concerned and call for government action against Internet content. But history and facts demonstrate that governments are incapable of enforcing their local standards on a global network. Hence governments should not focus on additional attempts to censor content on the Internet, but should instead focus on empowering the end-user.

The attitudes towards content on the Internet are highly subjective. Some users may be offended by erotic content because minors access the Internet, whereas a young adult may be perfectly entitled to view that same content; hence censorship is not a solution. After all, censorship affects all users, not only minors. The solution might be to emphasize to users that they can implement their own filters to prevent the viewing of specific content according to their own standards instead of general, government imposed standards. End-user empowerment teaches the population about the Internet, and how users can become more aware of content on the Internet and protect themselves against it.

An analogous situation has spontaneously developed in the area of computer viruses. The distribution of computer viruses is an illegal act in most countries, yet this has not prevented the proliferation of viruses in recent years. Citizens realize that governments cannot mount an effective defence against viruses despite the fact that they do occasionally prosecute virus writers. As a result people are forced to protect themselves by installing anti-virus software, which is what most people have ended up doing in recent years. Censoring content on the Internet by the government is as hopeless an attempt as preventing the proliferation of computer viruses. Another problem that is receiving a lot of attention is unsolicited commercial bulk e-mail, usually dubbed ‘spam’. Different governments have announced that they are considering the implementation of regulations against spam; the EU has already published a directive, to be implemented by national states before the end of 2003.

Regulating spam is a tricky proposition, because it is an international phenomenon. When one country creates regulations against spam, it does not affect the senders of spam in other countries. But a potential side effect of spam regulation could be that mandatory e-mail filters are installed by providers which also filter legitimate e-mail. It is highly unlikely that national anti-spam regulations will prevent bulk e-mail from being sent to its citizens. It may not be sent from that same country but from a safe haven abroad where the sending of spam is not illegal.

Another important consideration is that spam filtering systems should by necessity be voluntary for the end-user, and may never be involuntarily forced upon the user, because no filter is foolproof. Filtering will always result in the loss of some legitimate e-mail messages, and it is only the users who can decide what risks they would like to take in that area.

It might be better to fund public initiatives that develop anti-spam measures and technologies, instead of implementing regulations. There is a variety of ways in which end-users can protect themselves against spam. Government regulation is not needed as a protective measure, nor does it work: national jurisdiction is at odds with the international character of the Internet. But what does work is enabling end-users to install software that will help them deal with the problem. Some quite effective anti-spam filters are available on the

Internet. Another development is the rise of the concept of challenge response e-mail, where a recipient has to approve the sender in order to receive e-mail from that address now and in the future.

The conclusion that many advanced Internet users have drawn is that government regulation of the Internet is an inherently negative development: on the one hand it simply doesn’t work and threatens cultural differences, while on the other hand it causes collateral damage and hampers the proper development of Internet technologies. Industry self-regulation is even worse than government regulation: it suffers from obscure methodology without offering the possibility of public scrutiny. Apart from that, it is unheard of to give any industry the power to enforce regulation, and thus censorship, upon citizens.

What is the situation of Freedom of the Media and the Internet in the OSCE region?

Christian Möller

Introduction

The Situation of Freedom of the Media and the Internet in the OSCE Region

At first sight the Internet is a global infrastructure that is operating regardless of state borders or different cultures. But in spite of its global nature, national laws are adopted that influence the exchange of ideas and information through decentralized digital networks in one way or another. For participating States of the OSCE that are also members of the EU or Council of Europe these supranational bodies are also in the process of regulating various aspects of the Internet, for example with the Cybercrime Convention of the Council of Europe or the Copyright Directive (EUCD) of the EU.

But it is not only on a regulatory level that differences can be seen throughout the OSCE region. Technical advancement and the development of the technical infrastructure – telephone or broadband lines, the number of Internet service providers (ISPs) or the penetration with personal computers – likewise shows a lot of variation in the 55 OSCE States between Vancouver and Vladivostok.

According to statistics from the International Telecommunication Union (ITU), in 2002 there were more than 5,000 Internet users per 10,000 inhabitants in the Netherlands, Norway or Sweden. By contrast, there were only 243 users per 10,000 citizens in Bosnia and Herzegovina, 136 in Moldova and 119 in the Ukraine, just to pick some random examples. The estimated penetration of PCs per inhabitants in the whole of Europe is 20 per cent, but while this amounts to 44.17 per cent in Finland, 51.73 per cent in Luxembourg or 30.06 per cent in Slovenia things look different in other States, for example in Bulgaria (3.46 %), Romania (3.57 %) or Albania (0.76 %).[1]

Besides technical accessibility it is the costs that might prevent people from participating in the digital world. While in 2001, for example, in the US the cost of 40 hours of Internet access at peak times was 23.20 PPP dollars[2] or in Finland 33.70, it was 150.40 in the Czech Republic or even 171.80 in Hungary. The EU average for 40 hours was 62.50 PPP dollars.[3]

The above shows that although in principle everybody is free to communicate through the Internet, gather information from it or publish their own content the degree of technical development and the costs of access may hamper the actual use in many regions. But even if technology and access are provided, regulation and legislation may still be obstacles to unrestricted access to information or unfettered publication of content.

It must be admitted that criminal content can be found on the Internet, although this also applies to other media or information exchange infrastructures. However, the discussion on this topic often fails to differentiate between clearly illegal and just unwanted or so-called unsuitable or harmful content, which ranges from erotic depictions, left and right wing propaganda or copyright protected material to explicit pornography or violence. Besides this impreciseness in the discourse another problem is that legislation and cultural values differ throughout the region. While the explicit depiction of nudes, for example, might be considered offensive in the US or the United Kingdom, nobody would complain in the Netherlands or Scandinavia. On the other hand, what is considered illegal propaganda in Germany might be perfectly legal under the First Amendment in the US. There is only agreement when it comes to clearly abhorrent and criminal content, like child pornography. Although the dangers of misusing this new infrastructure are outweighed by the benefits of a global network by far, illegal content must be prosecuted and legislation in the respective countries of origin applied resolutely. But the Internet as such must not be made responsible for the content that is distributed through it.

Even in serious cases of hate speech, anti-Semitism or discrimination of minorities, suitable ways of proper policing, ISP hotlines and comprehensible notice and takedown procedures as well as the fostering of Internet literacy among users should be developed instead of blocking content. Not only are these technical measures 'undereffective' and cause 'overblocking'[4] but they also interfere seriously with the technical basis of the Internet. For example, the district government of the federal state of North Rhine-Westphalia ordered Internet service providers to impose blocking mechanisms or filters to prevent citizens from accessing sites like 'Nazi Lauck NSDAP/AO' (http://www.nazi-lauck-nsdapao.com/) or stormfront.org. While these sites are considered illegal by German local authorities they are protected by the right of freedom of expression in the US. Nevertheless, in order to obey government decisions German ISPs, including some universities, are using proxies,

[1] ITU Statistics, *Internet indicators: Hosts, Users and Number of PCs* (2003) <http://www.itu.int/ITU-D/ict/statistics/at_glance/Internet02.pdf>

[2] PPP dollars: adjusted with the help of a purchasing power parity (PPP) conversion factor. The PPP conversion factor shows the number of units of a country's currency required to buy the same amount of goods and services in the domestic market as one dollar would buy in the United States.

[3] See OECD, *Measuring the Information Economy 2002*, p. 57.

[4] See Maximilian Dornseif, *Government mandated blocking of foreign Web content*, 22 July 2003 <http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf>

packet filtering or even tamper with the Domain Name System (DNS), something like the telephone book of the Internet, in order to prevent their users from downloading the abovementioned contents.

Without entering into the discussion here about whether citizens should themselves be able to decide what content they wish to download, it should be explained that imposed blocking can not only be easily circumvented by the average skilled Internet user but also poses a threat to the technical framework of the Internet itself. Studies have revealed that obstructing the DNS to prevent the mapping of domain names into IP numbers might not only prevent access to the very page that the user wants, but also interfere with e-mail traffic or other Internet services.[5] It must not be forgotten that there is more to the Internet than the World Wide Web (WWW) and that all interferences on the technical level might influence much more than had been intended.

Packet filtering of data from certain IP addresses is also problematic, because it might prevent access to *all* pages from a certain address, even if the majority would not be incriminated. In the case of some webspace providers even web pages from many different authors could be filtered and blocked without justification. With packet filtering the user does not even know why access to the requested site is impossible. All in all, these immature technical measures affect the communication infrastructures themselves more than the authors of questionable pages.

Yet attempts to avert access to unwanted sites are not only to be found in Germany. In Kazakhstan it is also quite common to block opposition websites and independent newspapers like the online newspaper *Navigator*, which was blocked by the country's main ISP, the state-owned Kazakhtelecom in April 2003.[6]

Regardless of these technical problems of effectively and adequately filtering unwanted content from the World Wide Web, legislation in nearly all States tries to develop methods of regulating content on the Internet. However, while regulation might be justified in classic media with scarce resources, e.g. radio frequencies, a close look must be taken at similar endeavours for the Internet, as the above-mentioned technical examples show. The knowledge that some hackers or experienced users will find ways of circumventing censorship measures must not lead to unconcern about legislative developments.

In the following chapter Yaman Akdeniz, Mindaugas Kiskis, Jelena Surculija and Mikko Valimaki will report on the situation of freedom of the media and the Internet in Turkey, Serbia and Montenegro, Lithuania, and Finland. The choice of these four countries was made partly at random, and partly because they all serve as interesting examples of similar developments in different regions. However, the fact that these particular countries are combined in this book does not necessarily mean that they provide an especially good or an especially bad example.

[5] See Maximilian Dornseif, *Government mandated blocking of foreign Web content*, 22 July 2003 <http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf>

[6] Reporters sans frontières, *The Internet under Surveillance* (Paris, 2003).

Yaman Akdeniz

Internet Governance and Internet Freedom in Turkey

Introduction. This article will provide an overview of the legislative attempts to regulate Internet content in Turkey and will also offer a survey of the application of certain provisions of the Turkish Criminal Code to Internet publications and websites. Obviously, there may be varying approaches to the growth of the Internet in different societies and the impact of the Internet on different nation states may have diverse results. Different nation states present varying levels of economic development, respect for rights, transnationality and technological sophistication. While Turkey may be considered to be at a developing stage with respect to the Internet, others may be far more sophisticated with regard to Internet access, use and penetration. Inevitably, this will be reflected in the policy-making process and approaches to the governance of the Internet. But the Turkish approach to Internet governance can only be described as emerging. Internet governance has not been a top priority within the government agenda, and its transition to a 'knowledge society' has been slow with major concerns about the development of the infrastructure for Information Society services in Turkey.[1]

[1] See generally Republic of Turkey Ministry of Transportation (TUENA), Turkish National Information Infrastructure Masterplan, Final Report (Ankara: TUENA, October 1999), at <http://www.tuena.tubitak.gov.tr/pdf/tuenafinalreport.pdf>. See further the Turkish Industrialists and Businessmen's Association report, *Information Society and eTurkey Towards European Union*, T/2001-07/304 (Istanbul: TUSIAD, 2001). This report is available through <http://www.tusiad.org.tr/> and the author contributed to its preparation. See further Approaches to eEurope+ initiative in Turkey at <http://www.bilten.metu.edu.tr/eEurope+/>.

Because of cultural, historical and socio-political diversity, there will inevitably be divergent approaches to the growth and governance of the Internet in different European societies.[2] For example, while the German[3] and French Governments[4] have political fears and sensitivities about the use of the Internet by neo-Nazis, the United Kingdom takes a more relaxed attitude to the dangers of racism but conversely has a long cultural tradition of curtailing the availability of sexually explicit material. On the other hand, the Turkish Government may be more concerned about defamatory statements made about state officials and politicians, and the dissemination of racist and xenophobic propaganda.[5]

Legislative attempts to regulate Internet content in Turkey. The Turkish Constitution refers to freedom of expression and dissemination of thought in Article 26, which states that ‘everyone has the right to express and disseminate his thoughts and opinion by speech, in writing or in pictures or through other media, individually or collectively.’[6] Article 26 further states that these rights may be restricted, for example for the prevention of crime[7] but this provision ‘shall not preclude subjecting transmission by radio, television, cinema, and similar means to a system of licensing.’[8] Turkish law and court judgments are also subject to the European Convention on Human Rights (ECHR) and are bound by the judgments of the European Court on Human Rights and there are several cases involving Turkey and Article 10 of the ECHR.[9] More recently, in August 2000, Turkey also signed the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights.[10]

The Turkish Government adopted a hands-off approach to regulation of the Internet until 2001. However, during 2001, the Government introduced a parliamentary bill with the intention of regulating Internet publications according to the same rules that govern the mass media.[11] This prompted strong protests[12] and it was thought that:

'the bill was aimed at stifling the independence of a few aggressive Internet news portals, which have been publishing stories about corruption and politics that the mainstream media – firmly tied to the establishment – consider too hot to handle.'[13]

[2] See generally C. Walker & Y. Akdeniz, 'The governance of the Internet in Europe with special reference to illegal and harmful content', *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the Internet (1998), pp. 5-19.

[3] Criminal case of Somm, Felix Bruno, File No: 8340 Ds 465 JS 173158/95, Local Court (Amtsgericht) Munich. An English version of the case is available at <http://www.cyber-rights.org/isps/somm-dec.htm>.

[4] *League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France,* Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November 2000; Y. Akdeniz, 'Case Review of the Yahoo! Case', *Electronic Business Law Reports*, 1/3 (2001), pp. 110-20.

[5] Report of debates of the Second Part of the 2001 Ordinary Session on the Draft Cybercrime Convention, Council of Europe, Parliamentary Assembly (Assembly Spring Session, 23-27 April 2001), 24 April 2001.

[6] Note the recent changes within the Turkish Constitution in relation to Article 26. Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinin Degistirilmesi Hakkında Kanun, No: 4709, Kabul Tarihi: 3.10.2001, T.C. Resmi Gazete, No: 24556 (Mukerrer) 15 October 2001.

[7] Note that restrictions on the exercise of this right, such as 'national security, public order, public security, the fundamental characteristics of the Republic and the protection of the indivisible integrity of the State with its territory and nation', are added to the second paragraph of Article 26. See further Republic of Turkey Prime Ministry Secretariat General for European Union Affairs, *An Analytical Note on the Constitutional Amendments*, Ankara, 4 October 2001. This document is available through <http://www.abgs.gov.tr/>.

[8] The Constitution of the Republic of Turkey at <http://www.turkey.org/politics/p_consti.htm>.

[9] Among others see: *Erdogdu and Ince* judgment of 8 July 1999, Reports 1999, *Sürek and Özdemir* judgment of 8 July 1999, Reports 1999, *Okçuoglu* judgment of 8 July 1999, Reports 1999, *Zana* judgment of 25 November 1997, Reports 1997 – VII.

[10] European Commission, Regular Report on Turkey's progress towards accession, November 2000, p. 11, at <http://europa.eu.int/comm/enlargement/turkey/>. Note also the November 2001 progress report from the same pages. It should also be noted that under its MEDA programme for Turkey, the European Commission committed more than 70 million ECU in 1997 to strengthen civil society and human rights within Turkey. See EU Press release, Working together to strengthening civil society and human rights in Turkey, Brussels, 30 January 1998, DN: IP/98/109.

The bill was vetoed by Ahmet Necdet Sezer, the President of Turkey in June 2001. Sezer at the time stated that[14]:

'The most important aspect of Internet broadcasting, which is like a revolution in communication technology, is that it is the most effective area for freely expressing and spreading ideas and for forming original opinions... Leaving the regulation of the Internet to public authorities completely and linking it to the Press Law does not fit with the characteristics of Internet broadcasting.'[15]

This, however, proved a pyrrhic victory for the opponents as the sponsors of the bill were successful the following year. In May 2002, parliament approved the Supreme Board of Radio and Television (RTUK) Bill (No. 4676). The bill regulates the establishment and broadcasting principles of private radio and television stations and amends the current Turkish Press Code. It includes provisions that would subject the Internet to restrictive press legislation in Turkey. Although it attempts to apply only some aspects of the Press Code (such as to do with publishing 'lies'), the vague provisions are open to various interpretations. Critics maintain that the rationale behind these provisions would appear to be the silencing of criticism of the members of the Turkish Parliament and to silence political speech and dissent.[16] In general terms strong criticism is acceptable in Turkey. But, as noted by a Human Rights Watch report:

'Such freedom, however, ends at the border of a number of sensitive topics. Alongside the arena of free discussion there is a danger zone where many who criticize accepted state policy face possible state persecution. Risky areas include the role of Islam in politics and society, Turkey's ethnic Kurdish minority and the conflict in southeastern Turkey, the nature of the state, and the proper role of the military.'[17]

It should be noted, however, that to date no action has been taken in relation to any Web publications under the provisions of the legislation.

Control of cybercafes. Apart from this widely discussed and opposed legislation,[18] the only notable Internet-related regulation exists in connection with cybercafes in Turkey.[19] The regulation is mainly concerned with location (for example, cafes may not open near schools) and requires cafes to be licensed, like gaming places. Minors under the age of 15 are not to be allowed into such cafes and access is prohibited to illegal sites (such as pornography[20] and national security). The regulations do not specify, however, whether the cafes should use filtering software or how they should achieve blocking.

[11] Section 27 of the proposed legislation would bring the Internet within the ambit of the 5680 numbered Press Law. Radyo ve Televizyonların Kurulus ve Yayınları Hakkında Kanun, Basın Kanunu, Gelir Vergisi Kanunu ile Kurumlar Vergisi Kanununda Degisiklik Yapılmasına Dair Kanun Tasarısı, T.B.M.M. (S. Sayısı : 682), Dönem : 21 Yasama Yılı : 3.

[12] The bill was so thoroughly ridiculed that no agency admitted drafting or introducing it and no member of parliament acknowledged voting for it: 'Turkey in a Tangle over Control of Web; President Vetoes Bill Curbing Internet as Concern about Free Speech Grows', *The Washington Post*, 21 June 2001.

[13] 'Turkey in a Tangle over Control of Web; President Vetoes Bill Curbing Internet as Concern about Free Speech Grows,' *The Washington Post*, 21 June 2001.

[14] Presidential Statement in relation to proposal to amend the Press Law, 18 June 2001, at <http://www.cankaya.gov.tr/ACIKLAMALAR/18.06.2001-1159.html>. See further J.W. Anderson, 'Turkey in a Tangle over Control of Web', *The Washington Post*, 21 June 2001.

[15] Ibid. See further 'Turks Face Strict Censor in Internet Crackdown,' *The Times Higher Education Supplement*, 31 August 2001.

[16] See further Statement by Dr. Yaman Akdeniz in relation to the Internet-related provisions of the Turkish Supreme Board of Radio and Television (RTUK) Bill (No. 4676), 15 May 2002, at <http://www.cyber-rights.org/press/tr_rtuk.htm>. Note also 'Press group slams Turkish moves on the media', *Agence France Presse*, 5 June 2001.

[17] But note that even when writing on sensitive topics, a wide latitude holds sway, and different realities exist for different individuals. See further Human Rights Watch, *Violations of Free Expression in Turkey*, February 1999 <http://www.hrw.org/reports/1999/turkey/>.

[18] See websites such as <http://www.birlik.com/english.htm>

A handful of criminal prosecutions involving Internet publications. There have been three reported cases involving Internet-related prosecutions and attempts at censorship involving the Turkish Criminal Code. However, to date these are still isolated cases and each has been heavily criticized. Each case centred on Article 159(1) of the Turkish Criminal Code which states that:

'Whoever overtly insults or vilifies the Turkish nation, the Republic, the Grand National Assembly, or the moral personality of the Government, the ministries or the military or security forces of the State or the moral personality of the judicial authorities shall be punished by a term of imprisonment of one to six years.'

The details of each case are outlined below.

Emre Ersoz Prosecution. Emre Ersoz, 18 years old, received a ten-month suspended sentence for 'publicly insulting state security forces' after comments he made in June 1998 in an online forum operated by one of Turkey's ISPs.[21] Insulting state authorities and the police is a criminal offence in Turkey, under section 159(1) of the national criminal code. Ersoz was taking part in a debate over allegations of rough police treatment of a group of blind protesters who were complaining about potholes in the nation's capital, Ankara. After saying he believed that the national police had beaten the protesters, Ersoz repeated the allegation in a posting on a current events forum provided through Turknet, an ISP. As it turned out, Ersoz was mistaken: the protesters had been beaten by municipal officers, not by the national police.

Ersoz, who signed off using his real name and e-mail address, was reported to authorities by another person on the Turknet forum. State prosecutors then asked Turknet for Ersoz's full address, and the ISP complied. At 3:30 a.m., Ersoz's home was raided by a special anti-terrorism police squad, and he was taken into custody and held by the police for two days. The public prosecutor of the Beyoglu municipality in Istanbul brought the charges and demanded a sentence of one to four years. Ersoz pleaded not guilty, claiming his writings were not in the public domain. In the trial, he testified that his online comments could not be construed as public because the forum was open only to Internet users. Ersoz's ten-month sentence was suspended on the condition that he is not convicted of similar charges during the next five years.

Coskun Ak Prosecution. Coskun Ak, a former moderator of various forums operated by Superonline, one of the largest ISPs in Turkey, was sentenced to 40 months in prison due to a particular message about human rights abuses in Turkey sent to a Superonline forum by an anonymous poster. The message that triggered a prosecution under Article 159 of the Turkish Criminal Code was sent anonymously in May 1999.

The court decided to sentence Ak for insulting and weakening the Republic of Turkey, the Military Forces, the Security Forces, and the Ministry of Justice, to one year in prison for each insult, totalling four years. Later, the good conduct of the accused in court was taken into account and his sentence was reduced to ten months for each insult, totalling 40 months.

[19] Regulation B.05.1.EGM.011.03.05, dated 01/03/2000.

[20] It should be noted that under the Turkish law, 'provision' (or distribution) of obscene publications to children is criminalized rather than 'possession' of such content.

[21] See further Y. Akdeniz, 'Turkish teen convicted for Web postings', *Freedom Forum*, 8 June 1998, at <http://www.freedomforum.org/templates/document.asp?documentID=11277>. Note also K. Altintas, T. Aydin, V. Akman, 'Censoring the Internet: The Situation in Turkey', *First Monday*, May 2002, at <http://www.firstmonday.dk/issues/issue7_6/altinta/>.

In an interview about his trial, Coskun Ak said that he tried to explain to the prosecutor what the Internet was and what these forums were about, but he could not make him understand:

‘At the end of two hours, the prosecutor asked me, “Are you the Godfather of the Internet?”’[22]

On 14 November 2001, the Supreme Court reversed this ruling. It was decided that Ak’s case should be reconsidered, once experts selected from universities had analysed the situation.

On 12 March 2002 Istanbul Criminal Court No. 4 passed a second verdict against Coskun Ak. The sentence of 40 months’ imprisonment was commuted to a fine of TL 6 million (app. $4). On 24 April 2003, this second sentence was quashed by the Court of Appeal.

Ideapolitika.com Prosecution. In December 2001, a court in Istanbul ordered the closure of the website ideapolitika.com (site of the magazine *Idea Politika*) for insulting and degrading the armed forces under Article 159 of the Turkish Criminal Code.[23] This ensued from the initial prosecution of the magazine itself which featured articles that were deemed to be illegal under Article 159. However, despite various court cases, ideapolitika.com continued to be available on the Internet through a foreign server outside Turkey carrying the banned issues of the magazine. It should also be noted that it is possible to access ideapolitika.com in Turkey and the public prosecutors took no action to block access to this website from within Turkey.

Closure of Subay.net. Subay.net was a Turkish website which was critical of the administration of the Turkish Armed Forces (TSK). The website, which invited members of the Turkish army to air complaints about the military, was taken off the Internet in

February 2001, after rousing the ire of the powerful Chief of General Staff according to *Turkish Daily News*.[24] The site, which was thought to have been established in September 2000, had a forum entitled 'Free Fire' for soldiers to sound off on army life and share jokes about superiors. Some of the visitors to the forum defended the TSK while others criticized it, trading insults with one another as they left notes on the site. One of the messages on the website was: 'The biggest obstacle to Turkey's development is the TSK. From now on remain in your barracks.'[25]

However, the website was threatened with a prosecution under Article 159 of the Turkish Criminal Code as the pages were thought to be insulting to the military.[26] More than 18,000 Internet users visited the website within four days of a story about it being published in *Milliyet*, a popular Turkish daily newspaper.[27]

Filtered websites. A small number of websites are being filtered by Turkish Internet service providers following court orders. These websites generally include allegations of corruption within the Turkish Government and army. However, this handful of websites are still accessible through Turkish Internet service providers by using anonymous proxy servers, and access is also possible through anonymizer.com.

[22] 'Turkey in a Tangle over Control of Web; President Vetoes Bill Curbing Internet as Concern about Free Speech Grows', *The Washington Post*, 21 June 2001.

[23] BBC News, 'Turkey: RSF Deplores "Repressive" Amendments of Media Law', 17 May 2002.

[24] 'February: Political Row Sparks Unprecedented Economic Crisis, TL Floated Against $', *Turkish Daily News*, 5 March 2001.

[25] 'Turkish Press Scanner: Big Fight over Subay.net', *Turkish Daily News*, 10 February 2001. See further 'Turkish Website Takes Jabs at Powerful Military: Subay.Net Includes a Forum Called "Free Fire", Where Soldiers Sound Off on Life in the Army and Share Jokes about the Top Brass', *Turkish Daily News*, 8 February 2001.

[26] 'Website Under Fire', *The Independent* (London), 18 February 2001.

[27] 'Turkish Press Scanner: Big Fight over Subay.net', *Turkish Daily News*, 10 February 2001. See further 'New Website – Topic of the Day at the General Staff', *IPR Strategic Business Information Database*, 14 March 2001.

Impact of international developments on Turkey. Turkey is a member of the Council of Europe, United Nations, the OECD and the OSCE and has adopted a ‘wait and see’ approach while policies have been fostered at the international level. It has also respected its international obligations on at least one occasion by starting the ratification process for the implementation of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography[28] into the Turkish legal system.[29]

Turkey has not signed or ratified the Cybercrime Convention nor its additional first protocol as of August 2003. But it remains to be seen what approach will be adopted by the new Turkish Government. A major communications congress took place at the end of February 2003 in Ankara and representatives of the Government, academia, NGOs, and the Internet industry discussed the way forward and what regulation – if any – should be introduced in Turkey.

At the same time, membership of the European Union in the future will also have a major impact upon the governance of the Internet in Turkey. The development of the Internet and a regulatory framework for it within the European Union is directly relevant and important for the Internet’s development in Turkey. In December 1999, Turkey was recognized as a candidate country for full membership of the European Union and it is therefore crucial to align Turkish Internet policy with regulatory initiatives within the European Union.[30]

Future membership could shape Turkish policy even though there has not been prior alignment of its policies with the European Union as far as Internet governance is concerned.[31] However, as a candidate country Turkey has since June 2001 been included in the *eEurope+ 2000* Action Plan programme of the European Commission[32] which mirrors the priority objectives

and targets of the eEurope programme for the EU member states.[33] The overall aim of the Commission is to make the whole of Europe 'the most competitive and dynamic knowledge-based economy in the world'.[34] For this purpose:
'positive action on the basis of a strong, political commitment is needed to ensure that the EU Candidate Countries use the full potential offered by the Information Society and avoid a further digital divide with the EU.'[35]

The targets will have to be met by the candidate countries by the year 2003. These include accelerating the putting in place of the basic building blocks for the Information Society;

[28] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, New York, 25 May 2000, Fifty-fourth session (97th plenary meeting), Agenda item 116 (a), Distr. General A/RES/54/263, 26 June 2000. Not yet in force (the Optional Protocol will enter into force three months after the date of deposit of the tenth instrument of ratification or accession with the Secretary-General of the United Nations, in accordance with its Article 14).

[29] TBMM Proposal for legislation and the report of the Foreign Office Commission on the Optional Protocol, No: 690, 31 May 2001, at <http://www.tbmm.gov.tr/sirasayi/donem21/yil01/ss690m.htm>.

[30] Paragraph 12 of the conclusions of the Helsinki European Council stated that 'The European Council welcomes recent positive developments in Turkey as noted in the Commission's progress report, as well as its intention to continue its reforms towards complying with the Copenhagen criteria. (DN: PRES/99/999, Helsinki, 10 and 11 December 1999, Presidency Conclusions).

[31] But note, EU and Turkey open contacts on harmonising Turkish law, DN: IP/00/649, Brussels, 22 June 2000; EU Presidency Conclusions, DN: PRES/99/999, Helsinki, 10 and 11 December 1999.

[32] See eEurope+ 2000: A co-operative Effort to implement the Information Society in Europe, Action Plan, prepared by the Candidate Countries with the assistance of the European Commission, June 2001. See generally <http://europa.eu.int/information_society/international/candidate_countries/index_en.htm>. Note also the press release, Commission welcomes eEurope+ initiative of EU Candidate Countries, Brussels, 16 June 2001, at <http://europa.eu.int/comm/gothenburg_council/eeurope_en.htm>.

[33] eEurope 2002 – An Information society for all – Draft Action Plan prepared by the European Commission for the European Council in Feira – 19-20 June 2000, COM/2000/0330 final; Communication from the Commission to the Council and the European Parliament – eEurope 2002: Impact and Priorities A communication to the Spring European Council in Stockholm, 23-24 March 2001, COM/2001/0140 final.

[34] eEurope+ 2000: A co-operative Effort to implement the Information Society in Europe, Action Plan, p. 2.

[35] Ibid, p. 1.

providing a cheaper, faster, secure Internet; investing in people and skills, and stimulating the use of the Internet (including the promotion of e-commerce).[36] If these targets are met, Turkey could in theory start implementing some of the more specific EU policies such as those provided within the Electronic Commerce Directive[37] and the Electronic Signatures Directive.[38]

Furthermore, in general terms Turkey is already making progress towards EU membership and its national programme for the Adoption of the Acquis[39] includes the preparation of a legal infrastructure for 'data security and the use of data by taking into consideration technological developments and the development of electronic commerce, and for allowing public access via the internet to information produced by the public and private sector, bearing in mind the need to protect personal data and national data security.'[40]

Although there is no deadline set up for achieving these goals, the document outlining the national programme suggests that this will be achieved in the medium term.[41]

Conclusion. With the Adoption of the Acquis programme,[42] the Turkish Constitution and relevant provisions in other legislation are under revision in order to enhance the freedom of thought and expression in the light of the criteria referred to in Article 10 of the European Convention on Human Rights and Fundamental Freedoms, including those concerning territorial integrity and national security. This review is undertaken on the basis of the fundamental principles of the Turkish Constitution, particularly those concerning the secular and democratic character of the Republic, national unity and the unitary state model.

Content regulation remains a politically sensitive area within Turkey and elsewhere but it should also be remembered that the great appeal of the Internet is its openness. Efforts to restrict the free flow of information on the Internet, like efforts to restrict what may be said on a telephone, could place unreasonable burdens on well-established principles of privacy and free speech.

It is to be hoped that there will be no further amendments to Turkish laws to restrict freedom of expression on the Internet and that Turkey will continue to relax its laws under the Adoption of the Acquis programme.

[36] Ibid, p. 3.

[37] 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, Official Journal of the European Communities, vol 43, OJ L 178 17 July 2000, p. 1.

[38] Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 013, 19/01/2000 P. 0012 – 0020.

[39] Republic of Turkey Prime Ministry, The Secretariat General for EU Affairs, Turkish National Programme for the Adoption of the Acquis (NPAA), Ankara, 19 March 2001, p. 387. See generally <http://www.abgs.gov.tr>.

[40] Ibid, para 4.20, Telecommunications, p. 387.

[41] Ibid.

[42] See generally <http://europa.eu.int/comm/enlargement/turkey/pdf/npaa_full.pdf>.

Mindaugas Kiškis

First Steps in Internet Regulation in Lithuania

There is uniform agreement among legislators and academia internationally that the Internet provides an unmatched milieu for nourishing the fundamental values of democratic society, such as freedom of speech or freedom of opinion. On the other hand, the Internet is increasingly becoming a means for unlawful activities and a challenge to democratic rights such as privacy, and is providing a new environment for conventional crime and modern forms thereof. These reasons lead governments worldwide to introduce certain regulations for Internet media.

In a young democracy, such as Lithuania, the Internet provides unique tools for encouraging pluralism, increasing transparency and efficiency of public services, and facilitating access and exchange of information. Lithuania also faces an increasing need for regulation of the Internet, owing to noticeably unjust or even criminal usage of the Net, e.g. for facilitating human trafficking, distributing child pornography or intellectual property infringements. Fast paced EU enlargement also requires a leapfrog into the modern knowledge society, which may be assisted by up-to-date regulatory means.

In 2000-2003 Lithuania has seen an explosive growth in Internet penetration, with an annual growth of Internet users at approximately eight per cent and current Internet penetration at about 25 per cent. Although there is little reliable data, Internet misuse has also been rising significantly in Lithuania. Especially notable is the use of the Internet for intellectual property piracy, spreading racist and xenophobic ideas, abusing privacy or simply fraud. More latent ways of Internet misuse for facilitating human trafficking and child pornography are also present. Recent sociological research also shows that the Lithuanian public have little trust in Internet products and services. All these circumstances are not unique to Lithuania and all speak for the need for a certain degree of Internet regulation.

The challenges of Internet regulation were recently rather courageously met by the Lithuanian Government through a series of enactments. Three recent initiatives of the Lithuanian Government deserve to be mentioned in particular:

1) 5 July 2002 Law on Telecommunications of the Republic of Lithuania No. IX-1053;
2) 10 September 2002 Law on Protection of Minors from the Harmful Impact of Public Information No. IX-1067;
3) 5 March 2003 Resolution No. 290 of the Government of the Republic of Lithuania 'On procedures for the control of harmful information and distribution of restricted information in publicly accessible computer networks'.

The above regulations also rely heavily on the Law on Public Information of the Republic of Lithuania of 2 July 1996, which has had 15 revisions since enactment, with the most recent major overhaul in 2000, as well as cornerstones of the Lithuanian legal system in the form of the Civil Code, Criminal Code and the Code of Administrative Violations.

Specific issues that are important in Internet regulation in Lithuania relate to the Internet industry, as well as the need to protect Lithuanian cultural identity on the Internet. The Lithuanian Internet industry is relatively young and lacks social responsibility, unity and professional consciousness. These issues are demonstrated by the absence of any bodies which would unite the industry. As a result there are no common policies on privacy issues and user content, no self-regulation or content-rating systems, little co-ordination on unwelcome content, etc. The national Top Level Domain (TLD) administrator is hardly a good example for the Internet industry, with its notably non-democratic approach to domain name issues, as well as its lack of open governance of the TLD itself. It is hardly surprising that this has led to a lack of public trust in the Internet and the Internet industry.

In this situation, the Government is the only one capable of adopting industry-wide and mandatory regulations. This argument in favour of governmental involvement should not however be understood as encouraging the Government to ignore the value of self-regulation in the Internet industry. It is very important for the Government to introduce regulations, which would encourage the organization of the Internet industry, as well as its self-regulation. These objectives and means are supported in existing EU documents, such as the decision to adopt a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks of 1999, as well as the recommendation on Self-Regulation Concerning Cyber Content of 2001.

It is also rather obvious that the above-mentioned Lithuanian regulations are very recent, hence there is very little experience and empirical data relating to their application and effect. It is likely that there is no case law or administrative experience. The short time in which they have been in operation consequently means that their advantages and flaws cannot be fully assessed; hence only an overview of the existing regulations is provided below.

The general principle of the Law on Telecommunications is that Internet service providers are regarded as common carriers. The law eliminates any licensing for Internet service providers; however they are required to comply with rather straightforward notification procedures with the National Telecommunications Regulatory Authority. The law also contains provisions requiring Internet service providers to implement data retention measures for data transmissions (identificators and content) through common access telecommunications networks, and to provide this free of charge to criminal investigators and other authorities according to procedures established by the Government. Even before these provisions came into force (which had been set for 1 January 2003), they failed to survive the constitutionality challenge in the Decision of the Constitutional Court of 2002. The court found that such provisions are unconstitutional because they require unlimited and unpaid data retention. The court held that data retention measures which are necessary for ordinary business activities of Internet service providers, may be justified and reasonable. Thus, service provider's are effectively themselves entitled to decide on the scope and length of data retention, with due regard to data protection laws.

The Law on Protection of Minors from the Harmful Impact of Public Information attempts to define information which is considered harmful to minors, as well as establish the prohibitions and restrictions for distributing such information. The law embodying these provisions was passed only by overcoming the presidential veto. Key definitions on which the law relies remain rather vague and inconsistent, and thus somewhat jeopardize the benefits of this law. The definition of prohibited information is referenced to the Law on Public Information of the Republic of Lithuania and includes information that is xenophobic, criminal or that invades the privacy of an individual, especially if they are a minor. The definition of harmful information is even vaguer. An example of information that is classified as harmful in this law is pornography and sexual information, all kinds of violence, as well as information that causes fear and horror. The definitions rely on too many subjective considerations and appraisals to be effective.

The difficulties in classifying particular information as restricted or harmful may be demonstrated by the case of the Chechen website ‘Kavkaz-Center’ (http://www.kavkazcenter.net), which was hosted by the Lithuanian Internet service provider Elneta. On 20 June 2003 the provider was asked to shut down the website and the hosting server was seized by the Lithuanian authorities because of alleged accusations of hosting prohibited information, in particular information related to terrorism and the incitement of ethnic and racial discord. The presence of prohibited information was established by one expert and is questioned by a number of civil rights activists. The case is currently pending court trial.

The Government’s resolution on procedures for the control of harmful information and the distribution of restricted information in publicly accessible computer networks is designed to provide guidelines on how to enforce content control of the Internet. First of all it is not clear why such important issues were regulated in a resolution of the executive branch of Government, as opposed to the legislator. This governmental initiative clearly invades the territory of parliamentary jurisdiction, and hence is questionable *per se*.

The resolution attempts to regulate publishing on the Internet (including individual contributions to the Internet), and effectively extends the applicability of the current Lithuanian media laws to the Internet. Although the resolution cites that it is based on the European Parliament and Council Regulation of 1999, it hardly even mentions self-regulation and public involvement as a means of Internet regulation, and makes no provisions to encourage these two factors, which are prioritized in the European Parliament and Council documents. So far the Government takes on a sole regulatory role.

Electronic (or Internet) media is defined in this resolution as ‘web pages of media entities, providing public information, which is otherwise available by traditional means.’ However, ‘electronic media may be established by any juristic or natural person, under procedure established in the law, actively engaged or factually involved in media activities on the Internet’. Private web pages, which contain information on the author’s principles, data, works, products and services, etc., are not electronic media. It is unclear though whether private web pages containing information irrelevant to their owners, and especially web pages containing public forums, fall under the electronic media rules or not. This lack of a clear dividing line between private web pages and electronic media applies to most of the provisions of the resolution. Although electronic media are mandated to follow media ethics, it is not acknowledged that some operators of Internet pages, especially private individuals, are not always governed by such professional ethics.

Definitions of restricted and harmful information are not provided in the resolution, and are invoked from the Law on Protection of Minors from the Harmful Impact of Public Information, and the Law on Public Information. The general underlining principles of the resolution are to prohibit publication and/or distribution of restricted information on publicly accessible computer networks (i.e. the Internet), as well as to prohibit the free accessibility of harmful information. Harmful information is ruled to be subject to a mandatory rating system (to be introduced by the Ministry of Culture of the Republic of Lithuania).

The resolution further deals with establishing the mandatory content obligations for legal entities – web-page operators – who have to identify themselves clearly on the title page of their Internet pages, as well as liability principles for Internet content. As a general rule the operator of the Internet page is responsible for its contents. Hosting service providers are, however, responsible for the hosted content, as soon as they are aware of the existence of illicit content. The liability of non-professional operators of Internet pages, containing third party content (e.g. public forums) is not specifically regulated, and therefore may lead to improper treatment of such operators.

The resolution again attempts to introduce provisions requiring hosting service providers to log data and content and to provide them, along with the personal data about the individual and entities using the hosting services, to criminal investigators and other authorities free of charge. Although the obligation to provide logs is limited to those relating to normal business operations, it is still difficult to comprehend the democratic reasoning of these requirements, especially in view of the constitutional failure of similar provisions in Article 57 of the Law on Telecommunications of the Republic of Lithuania. Limiting this obligation to the provision of data necessary for normal business operations also relies on the sole discretion of the service providers.

The resolution suggests that the Ministry of Culture rates the information. There is no suggestion to involve the general public in this or in assessing alleged violations. The authority to investigate violations is vested in the Ministry of Interior, which shall also maintain an e-mail and hotline service for people to report such violations. The Information Society Development Committee at the Government of the Republic of

Lithuania has been assigned to make sure that these provisions are fulfilled. This committee should also foster the development of the industry and Internet users associations, codes of conduct and filtering means. Thus, the industry and the Internet public are excluded from the current resolution, yet at least their involvement has not been ruled out in the future.

The resolution does not provide any remedies to deal with the violation of the new rules, except for demands to block access to Internet service providers and hosting service providers. To a certain extent the Government may rely on the remedies provided in the Law on Public Information, as well as other laws (Criminal Code and Code of Administrative Violations). Unfortunately, many of these solutions are impractical or hardly applicable to electronic media, especially to individuals. Finally, and inevitably, the resolution provides no clear guidelines on the means of enforcement outside the reach of Lithuanian jurisdiction.

Even this brief insight into current Lithuanian Internet regulation proposals indicates that there are tendencies towards excessive and inconsistent regulation, which have already been found to compromise democratic values. Alternatives to governmental regulation, such as self-regulation of the industry, have also not yet been recognized by the Lithuanian Government. An overall analysis of the above regulations leaves a feeling of a rather desperate attempt to stretch traditional media rules to cover the Internet. This impression becomes especially viable in view of the global nature of the Internet. Even now, many websites providing harmful and prohibited content are hosted outside of Lithuania. Moreover, the prohibitions formalized in these governmental resolutions were effectively present in the moral leanings of most Lithuanian Internet service providers.

The above-mentioned findings suggest that the regulations, as they currently stand, may not serve the desired purpose. They may need to be reworked, and designed not to regulate Internet content directly but to provide a legal backing for self-regulation. It may also be suggested that a broader regional/ international framework is needed in order to balance out regulation and protection of democratic values on the Internet. Such a framework may assist national governments in shaping democratic regulations for the digital domain. It would provide a model for national Internet regulation, ensure a degree of cross-border uniformity, and finally facilitate enforcement, extending the capabilities to address the global aspects of the Internet. Existing regional initiatives do not provide a sufficient framework and are not fully comprehended by national governments, especially in young democratic countries.

It is important to acknowledge that these conclusions on current regulatory attempts are not unique to Lithuania. Other countries in Central and Eastern Europe, and even some EU countries, are undergoing similar experiences. In view of the pending enlargement of the EU it is increasingly important that these issues are addressed.

References:

Internet research news. Lithuanian IT industry association INFOBALT <http://www.infobalt.lt/main.php?s=42&r=475>

Information Society Development Committee at the Government of the Republic of Lithuania <http://www.ivpk.lt>

News reports on 'Kavkaz-Centre':
<http://www.delfi.lt/archive/index.php?id?2723808> <http://www.kavkaz-center.com/russ/article.php?id=9185>

Ruling of the Constitutional Court of the Republic of Lithuania on 23 October 2002, On the compliance of Article 8 and Article 14.3 of the Law of the Republic of Lithuania on Provision of Information to the Public with the Constitution of the Republic of Lithuania // Official Gazette *Valstybes Zinios*, 2002, No. 104-4675.

Jelena Surčulija

The Situation in Serbia and Montenegro

Serbia and Montenegro witnessed repression of the media and strong restrictions on freedom of expression during the 1990s, when the Internet became the alternative source of information. For example, Radio B92, which was closed down many times, launched the website where it started to broadcast its programme through live stream.[1] The Internet was not spared from the seizure – in December 1998 the Serbian University network set filters to prevent users from accessing the Open Net website, the Internet branch of Radio B92. However, after numerous Internet sites set up mirror sites to host Open Net, filtering of most of the Open Net websites stopped.[2]

The B92 website has done a great deal to alert the world to what was happening in Serbia, while at the same time keeping Serbian citizens informed about what was going on in their own country.[3] Unfortunately, only a small number of people were privileged enough to have access to the Internet and to enjoy the basic freedom of receiving information.

Institutional framework for Internet service providers and users. There was no law in Serbia that regulated the Internet before April 2003. Telecom Serbia, having exclusive rights until 9 June 2005, took advantage of the loophole by

[1] Radio B92 can be listened to at <www.b92.net>. Daily news is also available on the website.

[2] For more details, see the Human Rights Watch report on censorship of the University network <http://www.hrw.org/press98/dec/kos1221.htm>.

[3] The news is available in four languages: Serbian, English, Hungarian and Albanian.

trying to unite new technologies under its umbrella, which was considered illegal by private providers, sub-providers and users. The Law on Telecommunications has been in its ‘final phase’ for almost two years. Article 33, which provided for the monopoly, was an integral part of the draft law, but the problem was that – at the time – in Serbia there was no organized opposition to the monopoly. Internet service providers (ISPs) were trying to have an influence individually without adopting a common stand. Providers were competitors and in constant dispute with one another. As a result, the OSCE Mission to Serbia and Montenegro (OMiSaM) initiated the founding of the Yugoslav Association of Internet Service Providers[4] (YUISPA), which was finally established in September 2001. Despite constant competition with one another, 90 per cent of ISPs from both Serbia and Montenegro were present at the founding assembly and joined the association. The OMiSaM has continued to advise YUISPA on self-regulations, providing them with examples, legal texts and other documents and information.

At the same time, Internet users were also trying to become involved in the process of Internet regulation.[5] The OMiSaM Media Department was once again active and proposed creating a users’ institution. The final result was the founding of the Center for Internet Development in November 2001 with the aim to provide citizens with equal opportunities to access the Internet and to guarantee the unobstructed flow of information from and to the user.[6] The OMISaM has provided legal assistance to the Center, especially regarding the Law on Telecommunications and reform of the ‘.yu’ top level domain, among other things. One of the main projects of the Center has been the Global Internet Policy Initiative[7] (GIPI), which was started in June 2002 in co-operation with Internews[8] and the Center for Democracy and Technology[9]. Through GIPI, the Center has offered consulting services and organized visits of the European Internet Service Providers Association[10] (EUROISPA) to YUISPA, after which YUISPA was invited to become an associate member of EUROISPA. The latest project under the auspices of the Center and GIPI was founding the Telecommunications Users' Group (TUG) on 31 May 2003.

In the meantime, the international community was trying to point out the problems within the draft Law on Telecommunications[11], such as the fact that generally accepted telecommunications definitions needed to be clarified. Pressure exerted from both sides resulted in moving the article concerning the monopoly to the transitory provisions and at the same time removing Internet and multimedia services from Telecom Serbia's exclusive rights.

Internet service providers' dispute with Telecom Serbia. For some time, a certain number of ISPs had been offering Voice over Internet Protocol[12] (VoIP) services in Serbia. Telecom Serbia obstructed operations of ISPs that provide VoIP by reducing

[4] On <http://www.isp.org.yu> members of the association are listed and there is news related to the Internet or telecommunications in Serbia and Montenegro as well as a mailing list to which anyone can subscribe. The website is in Serbian only.

[5] Individually and/or through Internet forums e.g. <www.internodium.org.yu> or <www.elitesecurity.org> – very popular, but without any wider impact on the public at large.

[6] <www.cdt.org>

[7] <www.gipiproject.org> has a very good archive of documents related to Internet rights and freedoms.

[8] <www.internews.org>

[9] <http://www.cdt.org>

[10] <http://www.euroispa.org>

[11] See Dr. Katrin Nyman-Metcalf's report on the draft Law on Telecommunications at <http://www.plac-yu.org>.

[12] Voice over Internet Protocol (VoIP), also known as Internet telephony, is defined as 'a generic term for the conveyance of voice, fax, and related services, partially or wholly over packet-switched IP-based networks' according to the ITU Report of the Secretary General on IP Telephony, issued on 9 March 2001. VoIP is much cheaper than a standard circuit-switched call for consumers, because they use only their local line from both sides and do not reserve the entire international line.

their leased capacities from February until June 2002, when the group of ISPs were simply disconnected by Telecom Serbia from the public switched telephone network (PSTN) services. This was done without prior notice, warning, or consent. The affected ISPs brought their cases to the Commercial Court in Belgrade and the Inspector of the Ministry of Transport and Telecommunications of the Republic of Serbia, which both ruled in favour of the ISPs. These decisions also ordered Telecom Serbia to fully restore the disconnected services to ISPs and to stop any practices of this sort. To date Telecom Serbia has refused to comply with these decisions.

Vecernje Novosti, one of the major daily newspapers in Serbia, suddenly lost its Internet connection provided by its ISP, Memodata, on 11 February 2003. Both *Vecernje Novosti*'s and Memodata's IT units reported this to Telecom Serbia's support service, which reported back that there was no problem at all. The Memodata team found out that the line was not disconnected, but that the fast lines did not function. Telecom Serbia's final explanation was that everything was in order because even for high-speed links Telecom could guarantee only 9,600 bps. On 15 February 2003, Telecom Serbia offered to provide *Vecernje Novosti* with the connection. *Vecernje Novosti* had to accept the offer, not only because of its frequent use of e-mail and Internet, but also because its European edition is printed in Frankfurt for which the high-speed Internet link is necessary. *Vecernje Novosti*'s official explanation was that they have chosen the better Internet service provider. However, Memodata was the first ISP that was completely disconnected and lost all its leased lines, which affected thousands of Internet users in Serbia.[13]

Current Internet regulation in Serbia and Montenegro. **SERBIA.** Within the present legislative framework, the Internet is divided into Internet content (regulated as a media outlet) and Internet service (defined as a telecommunications service).

According to the Law on Public Information,[14] 'Media outlets comprise newspapers, radio programmes, television programmes, news agency services, Internet and other electronic editions of the above-mentioned media outlets and other public information media that use words, images and sound to publish ideas, information and opinions intended for public dissemination and an unspecified number of users.'[15] This definition raises many questions and concerns when considering the further implementation of this law with regard to the Internet and to online publications of media outlets. According to Article 17 of the law, 'the competent district court may upon a motion by the public prosecutor ban the dissemination of a piece of information if it establishes that such a prohibition is necessary in a democratic society to prevent calls for a violent overthrow of the constitutional order, the undermining of the territorial integrity of the Republic, prevent propagation of war, incitement to immediate violence or racial, ethnic or religious hatred representing incitement to discrimination, hostility or violence, and that the publication of such information would directly result in a serious, irremediable consequence that could not be prevented in another manner.' As mentioned above, Serbia had already experienced the banning and filtering of websites in the last decade, although this was never entirely successful since the Internet is a powerful tool that can host various contents in different locations, thus evading national legislation.

[13] SEEMO released the protest letter regarding this issue on 7 March 2003.

[14] Law on Public Information, 'Official Gazette of the Republic of Serbia', 43/03, 22 April 2003.

[15] Article 11 of the Law on Public Information.

The law prescribes that every media outlet must publish an imprint and a summary imprint[16] while ‘a distributor has the right to refuse to distribute a media outlet lacking an imprint’.[17] A fine of YUM 100,000 to 1,000,000 (EUR 1,500 - 15,300) for a violation shall even be imposed upon the legal person who established a media outlet if this fails to publish the imprint.[18] It is easy to find and hold liable a distributor of print or electronic media, but who is a distributor of an online publication? There is also an obligation prescribed by the law that every media outlet must have a responsible editor.[19] A fine shall be imposed upon the founder (legal person) of a media outlet if a responsible editor has not been appointed. The editor-in-chief does not simultaneously have the status of responsible editor, nor can a person who enjoys immunity from responsibility or whose residence is not in the Republic of Serbia be appointed responsible editor.[20] What shall we do with a media outlet that exists only online and that is founded by a natural person? It seems that this law, although a pioneer in regulating the Internet despite mentioning it only once, has a lot of loopholes that can lead to misinterpretations by courts. This should be taken into consideration in future amendments of this law.

The Law on Telecommunications[21] is the first law that regulates Internet services in Serbia. According to the Law on Telecommunications, ‘Internet service is a public telecommunications service realized by applying Internet technology’,[22] and ‘public telecommunications service is a publicly available telecommunications service provided by a public telecommunications operator.’[23] The Telecommunications Agency, once established, shall issue a general authorization to any person who intends to operate a public telecommunications network or provide public telecommunications services under this regime, provided that this person has met or agreed to meet all requirements prescribed for that network or service. General authorization shall be issued particularly for Internet services.[24] The Law on Telecommunications prescribes that 'Telecom Serbia, the operator of the public fixed telecommunications network, which has an exclusive right until 9 June 2005, at the latest, shall provide to users in the Republic of Serbia all existing and future types of fixed telecommunications services (including local, national, long-distance and international fixed telecommunications services, services of public switched telecommunications network [PSTN], other fixed services of voice mail, data transmission, telematic services, value-added public telecommunications services, integrated services digital network [ISDN], intelligent networks services, fixed satellite services, services based on the DECT [digital enhanced cordless telephone] standard, and leased lines), to build, own and operate any and all types of the existing and future fixed telecommunications infrastructures and networks (including wireline and wireless fixed facilities) in the territory of the Republic of Serbia, to provide directory services (including 'White Pages' and 'Yellow Pages') and to provide information, over the telephone or in electronic form, on subscriber numbers used in fixed telecommunications services for which it

[16] Articles 26 – 28 of the Law on Public Information.

[17] Article 29 of the Law on Public Information.

[18] Article 93, Paragraph 1, Point 1 of the Law on Public Information.

[19] Article 30 of the Law on Public Information.

[20] Article 93, Paragraph 1, Point 2 of the Law on Public Information.

[21] Law on Telecommunications, 'Official Gazette of the Republic of Serbia', 44/03, 24 April 2003.

[22] Article 4, Point 30 of the Law on Telecommunications.

[23] Article 4, Point 10 of the Law on Telecommunications.

[24] Article 38, Paragraph 1 and Paragraph 9, Point 4 of the Law on Telecommunications.

has exclusive rights and shall retain this right until the stated date unless the agreement under which this right has been acquired is amended.'[25] This exclusive right does not include the Internet, multimedia services or any other radio and television or cable television services that can be provided freely and under equal conditions according to the provisions of the law.[26]

Although Internet services are *de jure* excluded from the exclusive rights, they are *de facto* still under the monopoly regime. For example, Internet service providers need leased lines to provide their services and if Telecom Serbia does not have enough resources available, they will not be able to operate. In addition, forced to use Telecom's leased lines, ISPs from Subotica, a city near the Hungarian border, have to use Telecom's link to Belgrade and then from Belgrade to Hungary, instead of having their own direct leased line to Hungary.

Upon completion of the legal framework, the next and very important step will be the proper implementation of these laws.

MONTENEGRO. The situation in Montenegro is quite different from Serbia. Internet service is regulated by the Law on Telecommunications[27] which states that the existing operator of the public fixed telecommunications network (Telecom Montenegro) or its legal successor shall have the exclusive right up to 31 December 2003 to provide public fixed telephone services, telex and telegraphy, public payphones and to lease lines to users in the Republic. It also has the exclusive right to construct, own and exploit the public fixed telecommunications network, as well as to organize or provide a 'call-back' and voice transferring service through the Internet in the Republic. During the specified period, the right to perform the services of public payphones belongs also to the Post Office of Montenegro Ltd., or its legal successor.[28] This provision brings Montenegro closer to market liberalization and foreign investments in the telecommunications sector after 1 January 2004.

The Agency for Telecommunications was founded by the Government of Montenegro in 2001.[29] It has issued four general licences to Internet service providers so far, of which Internet Crna Gora (Internet Montenegro) is the biggest and covers 95 per cent of the Montenegrin market. Forty per cent of it is owned by Telekom Crna Gora and 60 per cent by private owners. It has around 50,000 users, although only 35,000 registered dial-ups.

SERBIA AND MONTENEGRO. According to statistics from the International Telecommunications Union (ITU)[30], Serbia and Montenegro had 400,000 Internet users in 2000, while in 2002 that number significantly increased by more than 50 per cent to 640,000 users. While there were 376 users per 10,000 inhabitants in 2000, this number almost doubled in 2002 to approximately 600 users per 10,000 inhabitants. In 2000, Serbia and Montenegro had 2.26 PCs per 100 inhabitants and this increased to 2.71 in 2002. The European average was 20.01 PCs per 100 inhabitants in 2002, ten times higher than in Serbia and Montenegro. Although there has been enormous statistical progress in the past two years, it is apparent that access to the

[25] Article 109, Paragraph 1 of the Law on Telecommunications.

[26] Article 109, Paragraph 2 of the Law on Telecommunications.

[27] Law on Telecommunications, ‘Official Gazette of the Republic of Montenegro’, 59/00, 27 December 2000 and 58/02, 1 November 2002.

[28] Article 27 of the Law on Telecommunications.

[29] Decision to found the Agency for Telecommunications, ‘Official Gazette of the Republic of Montenegro’, 10/01, 28 February 2001. Further details regarding the work of the Agency can be obtained at its official website: <http://www.agentel.cg.yu/english/index.htm>.

[30] <http://www.itu.int/ITU-D/ict/statistics>

Internet, as a prerequisite for access to any information online, is still the main problem. The existing monopolies in the telecommunications sector may slow down the process of market liberalization, which is necessary for further convergence towards the European Union.

The Constitutional Charter of the State Union of Serbia and Montenegro recognizes the supremacy of international law[31] and states that 'ratified international agreements and the generally accepted rules of international law shall have precedence over the law of Serbia and Montenegro and over the law of the member states.'[32]

Article 19 of the Universal Declaration on Human Rights[33] states that: '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 Charter on Human and Minority Rights and Civic Liberties of Serbia and Montenegro guarantees freedom of expression and freedom of the media in Serbia and Montenegro. One would hope that the citizens will be brave enough and have the strength to fight for this, that the Government will respect freedom of expression and freedom of the media and that the international community will call for the full implementation of these basic human rights in practice.

[31] Article 16 of the Constitutional Charter of the State Union of Serbia and Montenegro, 'Official Gazette of Serbia and Montenegro', No. 1, 4 February 2003.

[32] The International Covenant on Civil and Political Rights (ICCPR) was ratified by the Socialist Federal Republic of Yugoslavia (SFRY) on 4 February 1971 ('Official Gazette of SFRY', 7/71).
The state union of Serbia and Montenegro became a member state of the Council of Europe on 3 April 2003 and on the same day signed the European Convention on Human Rights (ECHR) that has not been ratified yet.

[33] The Universal Declaration on Human Rights was adopted and proclaimed by the General Assembly resolution 217 A (III) of 10 December 1948.

Mikko Välimäki

Defending the Freedom of Speech in an Advanced Information Society: The Finnish Story

Introduction: Myyrmäki bombing 2002. Freedom of speech online became a hot topic in the Finnish news in autumn 2002. 'Finland's Minister of the Interior Ville Itälä (Nat. Coalition) ordered the establishment of a police working group which is to consider the need for possible controls on the content of Internet message boards in light of the recent events. At least one message board devoted to explosives was shut down on Sunday.'[1]

A college student had exploded himself and five other people in a Helsinki suburb mall. Allegedly the student had learned bomb making from a local Internet discussion forum. Another youngster running the discussion group was consequently arrested. His computers were retained and all message board archives were searched for possible evidence.[2]

A public debate followed. Electronic Frontier Finland (EFFI) had been founded to defend civil rights and individual freedoms on the Internet just before the September attacks in 2001. In spring 2002 EFFI gave Finland's first Big Brother awards and had gained mainstream media attention. Now, EFFI was needed to defend the uncensored Internet. Within a week after the Myyrmäki bombing, EFFI board members commented on the case and its possible online implications more than five times in different talk shows and news broadcastings.

[1] 'Police detain youth in connection with shopping mall bombing – flags fly at half staff all over Finland', *Helsingin Sanomat*, 15 October 2002 <http://www.helsinki-hs.net/news.asp?id=20021015IE9>.

[2] 'International Edition coverage of the Myyrmäki bombing', *Helsingin Sanomat*, 22 October 2002 <http://www.helsinki-hs.net/news.asp?id=20021022IE4>.

New law on free speech online. One of the major achievements of EFFI has been the amendments to a new law on the use of freedom of speech online in early 2003. The legislative process had bad timing since all the Myyrmäki news was still fresh in people's memories. At one extreme, the Christian party demanded more censorship of the Internet claiming that 'at least all web pages in Finnish should be cleared'.

The first proposal of the law which came out in 2001 was definitely worrisome. It fundamentally restricted the freedom of speech online and additionally required the logging of practically all Internet traffic. To be precise, the law didn't aim at regulating the freedom of expression but merely the liabilities and responsibilities of those who use their freedom of speech as stated in the constitution.[3] Similar kinds of problems with new Internet-related laws can probably be found elsewhere:

- Definitions are ambiguous. While the Finnish law proposal perhaps targeted large websites of traditional printed media with staff editors, in the first version it could be read to mean any web page out there – including interactive message forums and chat rooms.
- Unnecessary and overbroad retention requirements. The first version of the proposal had a six month requirement, which dropped to two to three months in the second version and ended up as three weeks in the final law. This is a positive change, but is does not remove the fundamental problem. Why is it necessary to store web publications in the first place?
- Logging requirements are also too broad. In the first version of the law, logging covered practically all possible communication. It required system operators (or responsible editors-in-chief) to log e.g. IP addresses and message headers of all communications. Fortunately, this requirement was dropped from the final law.

- Monitoring requirements are too heavy. The Finnish law proposal first required that all web publications would need an 18-year-old editor-in-chief responsible for even third party publications to some extent. One can only count how many immigrants a country of 5.5 million people like Finland would have needed in order to fulfil this requirement.

Electronic Frontier Finland, local ISPs and the International Chamber of Commerce were the main opponents of the law. With co-ordinated effort these were able to change the law substantially at the parliamentary hearings. A constitutional law committee did a very careful new drafting and accepted almost all the requested amendments. As a result, the Finnish parliament finally passed the law on 17 February 2003 in a substantially changed form.[4]

Intellectual property and the freedom of media. Debate on justified intellectual property rights is today global. Different grass-roots organizations and political parties alike discuss quite heatedly on the topic. We have had a share of the discussion also in Finland.

The discussion fired up again when a new copyright law proposal based on the EU copyright directive (EUCD) was dismissed in parliament in early 2003.[5] One of the main reasons was that it didn't take conflicting constitutional rights into account.

[3] <http://www.effi.org/sananvapaus/>

[4] See 'Finland rewrote the Internet censorship law', EFFI press release, 16 February 2003 <http://www.effi.org/julkaisut/tiedotteet/pressrelease-2003-02-16.html> and 'Finnish companies oppose law to censor Internet', International Chamber of Commerce statement, 6 February 2003 <http://www.iccwbo.org/home/news_archives/2003/stories/finnish.asp>. Since this law is enacted in the so-called constitutional legislative process it needs another accepting vote to be effective. The vote is expected soon and the changing of the wordings is impossible at this stage.

[5] 'Finland kills EUCD – for now', EFFI press release, 31 January 2003 <http://www.effi.org/julkaisut/tiedotteet/pressrelease-2003-01-31.html>.

Take the freedom of speech as an example. The freedom to obtain, use and disseminate information uncensored fundamentally conflicts with the idea of restricted copying and dissemination of copyrighted works.

The problem is that the new copyright rules limit the role of copyright exemptions granted e.g. for citation, private use and education. If works are technically protected (with so called digital rights management) even a citation may result in copyright infringement.[6] The unlucky Finnish law proposal – interestingly written by the chairman of the 1996 WIPO meetings that later resulted in EUCD – stated that: 'This proposal does not include anything that would require constitutional law review.' Once again, the parliamentary hearings changed the tone of the discussion.[7]

Where is Scandinavia going? One area in need of increasing observance is the corporate environment. Our freedom to use the Internet and new communication media depends on different intermediaries. Most ISPs have traditionally been proponents of the free Internet. However, there are also alarming counter-examples where the company power has been used against the principles of free communications.

We recently stressed corporate responsibility at the annual Finnish Big Brother 2003 awards on 4 June in Helsinki. The most prestigious award was given to the largest Finnish Telco, a partly government-owned company called Sonera (as of now TeliaSonera). In October 2002, an unusually extensive privacy breach was reported. It all started when the Finnish newspaper *Helsingin Sanomat* printed allegations that Sonera employees had violated communications secrecy during 2000 – 2001.

The top management of Sonera had ordered surveillance of over fifty phone records in order to find out who leaked classified company information to reporters.[8] Sonera was among those ISPs who miscalculated during the dot-com boom and invested in the next generation mobile network licences all over Europe, later to find out that the investments almost took them into bankruptcy. Understandably, at the time of the phone surveillance, the company's management was very alarmed about the company's stock quote (essential in licence bidding and acquisitions) and related news reporting.

Manuel Castells and Pekka Himanen identify three types of advanced information societies: the Silicon Valley model (US style free markets), Singapore (Asian authoritative model) and Finland (Scandinavian welfare state).[9] Interestingly, online civil rights movements have started from the free market environment and only recently arrived in welfare states. In authoritative states they are a far cry away from this as recent Chinese examples show.[10]

People in welfare states seem to trust in government officials and consumer protection agencies even in information policy matters. Rules are obeyed to the extreme – and we have seen that the new proposed rules do not always serve the best interests of society as a whole. Our Finnish example should encourage other online civil liberty activists to start contacting law makers and influencing actual public policy. We can really make a difference if we just want to. There are reasons to believe that further action will be seen in other Northern European countries, too.[11]

[6] See Article 6 of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.

[7] A new copyright law proposal is expected in early autumn. While a year ago Finland seemed to be one of the first to implement EUCD, we are now safely behind the EU average in the process.

[8] See e.g. 'Police arrest former Sonera CEO Kaj-Erik Relander', *Helsingin Sanomat*, 27 November 2002 <http://www.helsinki-hs.net/news.asp?id=20021127IE1>. This wasn't the first case in Sonera. See also 'Sonera managers charged with data privacy invasion over e-mail snooping', *Helsingin Sanomat*, 2 December 1999 <http://www.helsinki-hs.net/today/021299-01.html>.

[9] Manuel Castells and Pekka Himanen, *The Information Society and the Welfare State. The Finnish Model* (Oxford University Press, 2002).

[10] On the other hand, authoritative states may have quite liberal practices towards e.g. restrictive property rules, which may balance out some of the potential freedom of speech problems beforehand.

[11] Currently Norway has a strong online civil liberties organization called Electronic Forpost Norge <http://www.efn.no/>, which gained attention with the recent DVD copy protection case. In Denmark, there is Digital Forbruger Danmark <http://www.digitalforbruger.dk/> and Digital Rights <http://www.digitalrights.dk/>. Sweden has EF-Sverige <http://www.efs.se/>.

Regulation of decentralized networks: a problem or a necessity for freedom of expression?

Páll Thórhallsson

The Freedom of Expression Regime in Europe: Coping with the Net

I. Introduction

The Internet brings with it new opportunities for enhancing freedom of expression and information. Every individual with access to the Internet can potentially reach the rest of mankind with his/her message. All kinds of information sources are proliferating.

But, there are not only opportunities, there are also risks. Child pornography and racist speech on the Internet, unsolicited commercial e-mail (SPAM): these are examples of the kind of abuse of freedom of expression which calls for an answer. There is no reason why we should abandon the regulatory framework for public communications, simply because violations are more widespread than before or because it is becoming more difficult to provide answers.

In the following, I would like to give an overview of the main characteristics and principles of European public communications law and review them in the light of the challenges posed by the Internet.

II. How does the freedom of expression and information regime in Europe cope with the Internet?

Constitutional framework: Article 10 of the ECHR.

The constitutional framework for freedom of expression and information in Europe is to be found in Article 10 of the European

Convention on Human Rights.[1] According to this provision freedom of expression and information may be subject only to those restrictions which are prescribed by law, are necessary in a democratic society and serve certain legitimate purposes. In other words, freedom of expression is not absolute; limitations must be allowed in order to protect other rights and interests. The conditions for allowing limitations have been defined in more detail in a number of cases before the European Court of Human Rights.

Since this provision is already technology neutral, there does not seem to be any need to revise it to take account of the Internet. This is emphasized to some extent in Principle 1 of the recently adopted Declaration on freedom of communication on the Internet: 'Member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery.'[2]

It is also telling that the EU Charter of Fundamental Freedoms, drafted after the Internet became a household word, does not invent anything as regards freedom of expression and information to cope with the technological changes – there is no need to!

No censorship. The freedom of expression regime is liberal in the sense that people are entitled to say or write what they think, only afterwards will there be a control of whether the expression was in accordance with the law or not. Prior restrictions can only be tolerated in very exceptional cases. This is reflected in the fact that censorship in the sense of prior administrative control of publications has been abolished in all Council of Europe member States.[3]

The Internet makes it both more difficult and easier for repressive governments to exercise censorship. It is more difficult in the sense that the amount of publicly available information is much more than before and there are potentially a much higher number of information providers than before. On the other hand it may be technically easier to control the flow of information across borders when this takes place in cyberspace compared to books, newspapers, radio and television. It suffices to have control of the Internet access points, the national service providers. Technology may also enable governments to collect information on how people are using the Internet, something which was much more difficult in former times with respect to media such as radio or books.

This situation is addressed in Principle 3 of the CoE Declaration dealing with when and under which circumstances public authorities are permitted to block access to Internet content. The Declaration states first of all that public authorities should not employ 'general blocking or filtering measures' in order to deny access by the public to information and other communication on the Internet, regardless of frontiers. With 'general measures', the Declaration refers to crude filtering methods which do not discriminate between illegal and legal content. This principle, which is quite broad in its scope, does not prevent member States from requiring the installation of filtering software in places accessible to minors, such as libraries and schools.

Member States still have the possibility, according to the Declaration, to block access to Internet content or to order such blockage. There are, however, several conditions which

[1] There are other important characteristics of the European freedom of expression regime which derive less directly from Article 10 of the ECHR. Thus, it can be argued that States have the duty to protect, and if need be, take positive measures to safeguard and promote media pluralism. The public service broadcasting model can also be said to be a characteristic of the European freedom of expression regime. It is enshrined for example in Recommendation (96) 20 of the Committee of Ministers. I will not dwell on these issues here.

[2] Declaration of the Committee of Ministers of the Council of Europe on freedom of communication on the Internet, adopted on 28 May 2003. Available at <www.coe.int/media>.

[3] In some of them very recently, in others centuries ago.

need to be fulfilled: a) the content has to be clearly identifiable, b) a decision on the illegality of the content has to have been taken by the competent national authorities and c) the safeguards of Article 10, paragraph 2, of the European Convention on Human Rights have to be respected, i.e. a restriction has to be prescribed by law, aim at a lawful purpose and be necessary in a democratic society.

As stated in the Explanatory Note to the Declaration, Principle 3 is in particular aimed at situations where state authorities would block access by its population to content on certain foreign (or domestic) websites for political reasons. At the same time it outlines under which exceptional circumstances, blockage of content may be considered acceptable, a matter which is or will be relevant to all member States.

Regardless of frontiers. Freedom of expression and information is borderless. This is highlighted in Article 10 of the ECHR where it says that the right to these freedoms shall be respected ‘regardless of frontiers’. This has been taken to mean, for example, that the reception of broadcasting from abroad enjoys the protection of Article 10. Parties to the European Convention on Transfrontier Television commit themselves to allowing such free reception on condition that programmes from abroad respect certain basic content standards.

The Internet has developed as a network which knows no national borders. It has a huge potential to bring nations closer to each other and enhance mutual understanding between peoples. The Internet is the first truly global medium. Any legal solutions which may be found to the problem of implementing standards should take these phenomena into account. It would be a pity, for example, if it became the general rule, that information providers would be obliged to follow the law of every jurisdiction where their information could be consulted. That would mean either the victory of the lowest common denominator, thus stifling fresh thoughts which would risk being at odds with any particular legal system, or alternatively that technical solutions would have to be invented to make content only available to users in certain countries, something which would amount to splitting the Net up into national systems.

Content standards. What then are the legal standards that we apply to expressions disseminated publicly? Article 10 of the ECHR provides the general framework for the kind of standards which are accepted. The details are provided by national law and comparisons show that there are some common trends.

Some standards apply to every kind of public expression. Statements must for example not be defamatory, racist or in violation of privacy rights or intellectual property rights. These rights are protected by national civil or criminal law and constitute in principle, subject to several conditions, an acceptable ground to limit freedom of expression according to Article 10 of the ECHR and the case law of the EurCourtHR.

There is no reason to think that these standards should not apply to the Internet. What happened with the Convention on Cybercrime and its Additional Protocol, however, was that a common agreement was found on only a limited number of issues, namely child pornography, copyright violations and racist and xenophobic speech. That doesn't mean that the others aren't relevant. The fact is that they may be enforced primarily through civil law and therefore did not have their place in this particular convention.

Other standards are more sector-specific, such as those applicable to broadcasting. Here, I refer for example to the prohibition on certain types of advertising or to rules which prohibit the broadcasting of content harmful to minors at certain hours of the day (watershed rules).

Here we come to the really difficult part. Should we assimilate online public communications into standards for broadcasting, newspapers, expressions in public spaces or none of these? It seems rather evident that broadcasting standards should apply when the Internet is used for direct retransmission of broadcast programmes. But apart from that? Is there reason to try and uphold the same standards? These questions are being thought about within both the EU and the Council of Europe. A recent CoE study suggests that some standards, such as limiting the amount of advertising, do not lend themselves to being maintained. Others, such as separation of editorial content and advertising, are very well suited.[4]

As regards harmful content, the Council of Europe has adopted a recommendation on self-regulation concerning cyber-content no. (2001) 8. The recommendation suggests ways to deal with harmful Internet content through developing rating and filtering systems, replacing watershed rules with means to empower users to avoid certain types of content.

Specific liability rules for media content. These rules differ from one country to the other, but in many countries there are systems which confer responsibility for publications on a particular person, which is not necessarily the author. This enables, for example, anonymous articles in newspapers. If there were ordinary liability rules police authorities or prosecutors could start enquiring who the real authors of articles were or even who had given information to the media. That might be a serious threat to the free expression of information.

In the offline world the focus has been on the legal responsibility of journalists vs. media companies. In the online world new questions arise. What about the responsibility of service providers? There are different types of service providers.[5] Answers to some of these questions are given in the e-commerce directive but also in the Cyberconvention and the CoE draft declaration on freedom of communication on the Internet. Basically, the level of liability depends on the awareness of the service providers of the illegal nature and of their ability to control access to the information.

There is a particular dilemma here, namely how to avoid private censorship? The CoE Declaration on freedom of communication on the Internet emphasizes that when defining under national law what level of knowledge is required of service providers before they become liable, '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.'[6]

The questions which are addressed here are currently widely debated, for example in the context of defamatory remarks on the Internet. The Explanatory Note underlines that questions about 'whether certain material is illegal are often complicated and best dealt with by the courts. If service providers act too quickly to remove content after a complaint is received, this might be dangerous from the point of view of freedom of expression and information. Perfectly legitimate content might thus be suppressed out of fear of legal liability.'

[4] See <www.coe.int/media>

[5] In the Convention on Cybercrime a service provider is defined as 'any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service.'

[6] Declaration, Principle 6, para. 4.

Remedies. Remedies to abuse of freedom of expression can be mild ones, such as the right of reply, or more severe ones, such as fines or imprisonment. The right of reply is a particular European remedy found in many national laws and also in Article 9 of the European Convention on Transfrontier Television. In principle there is not much to say about the range of remedies, they should all apply equally to violations online as well as offline. One of them is tricky though, namely the right of reply. Traditionally an obligation to publish a reply from a person whose personality rights were at issue only rested with the press and then later also with radio and television. Should this remedy now be extended to everyone who makes a public communication, even through personal websites? An expert group within the Council of Europe has been looking at this question.[7]

Implementation. The implementation of the above-mentioned rules and standards has traditionally been mainly in the hands of national authorities. The role of self-regulation has also been recognized for a long time. Principle 2 of the Declaration encourages States to allow self-regulation and co-regulation as regards content on the Internet to develop as an alternative to outright state regulation. This is considered to be more respectful of freedom of expression but also a necessity in a very complicated field where other actors than the State must be encouraged to act responsibly.

Conclusion. The Declaration on freedom of communication on the Internet is a timely addition to the legal arsenal of the Council of Europe in the field of public communication. Some of its principles may sound rather self-evident to people from most member States. It should however not be forgotten that the situation within the Council of Europe is very varied and some state authorities may have a tendency to subject expression on the Internet to excessive control.

In practical terms it will also be useful as a point of reference for Council of Europe experts when giving advice on draft legislation in member States.[8] The Declaration contains European standards in a new field where there is still no case law from the European Court of Human Rights to refer to.

[7] See the work of the group of specialists on online services and democracy, <www.coe.int/media>.

[8] The expert opinions on draft broadcasting laws, draft freedom of information laws etc. are now as a general rule published on the Council of Europe´s website, see <www.coe.int/media>.

Tarlach McGonagle

Practical and Regulatory Issues Facing the Media Online

This chapter explores some of the issues concerning the role, activities and regulation of the media in an online environment. It does not set out to be exhaustive in its treatment of relevant issues; rather its aim is merely to raise a selection of issues for discussion and further probing.

The media and democracy. One of the profound paradoxes of democracy is that if it functions well, criticism of it will thrive. Criticism should pervade throughout society, but it is rooted in the media and, increasingly, civil libertarian and other non-governmental organizations. It is not without reason that many people have come to regard the media as the Fourth Estate; a would-be extra pillar in a radical reworking of Montesquieu's tripartite division of powers.

The centrality of the (mass) media to the dynamics of democracy has been recognized time and again by the European Court of Human Rights, having ascribed to the media the 'vital role of public watchdog'.[1] The Court has stated that it is incumbent on the media to impart information and ideas on all matters of public interest. It has also consistently held that '[n]ot only do the media have the task of imparting such information and ideas: the public also has a right to receive them'.[2] In light of this function of the media (corrective, supervisory,

[1] *The Observer & Guardian Newspapers Ltd. v. United Kingdom*, Judgment of the European Court of Human Rights of 26 November 1991, Series A, No. 216, para. 59.

[2] *The Sunday Times (No. 1) v. United Kingdom*, Judgment of the European Court of Human Rights of 26 April 1979, Series A, No. 30, para. 65.

stabilizing – call it what you will), the Court has tended to carve out a zone of protection for the media's right to freedom of expression that is even greater than that of ordinary individuals.

One hallmark of the expanded zone of the media's freedom of expression is the notion of journalistic independence. Importantly, this independence filters from the editorial level down to coal-face journalism and reporting. A key pronouncement in this regard reads: 'the methods of objective and balanced reporting may vary considerably, depending among other things on the medium in question; it is not for the Court, any more than it is for the national courts, to substitute its own views for those of the press as to what techniques of reporting should be adopted by journalists.'[3] This commitment to the autonomy of the media in a democratic society goes a long way to guaranteeing operational latitude for journalists. Moreover, this operational latitude stretches to include 'possible recourse to a degree of exaggeration, or even provocation'.[4] However, alongside the enjoyment of journalistic freedom – as defined by the Court – are concomitant duties and responsibilities[5] (discussed below).

The growth and maturation of the European Court's attitude towards the media can largely be attributed to their function to serve the aforementioned public interest through the provision of information. The Court's attitude would appear to be premised at least in part on the point-to-multipoint nature of mass media communications; on the understanding that information purveyed and disseminated by the mass media will reach a larger section of society than communications between ordinary individuals. The contiguous considerations of impact and influence are key to this conception of the role and activities of the media.

Could or should this state of affairs under which the media enjoy preferential status change in the online world (as broadly defined)? Or, in other words, in a world where the barriers to mass communication are drastically diminished? Or in a world where communications services are becoming increasingly customized, personalized and individualized? Or in a world where the 'proliferation of niche markets, the waning of public reliance on general interest intermediaries and the growing incidence of advance individual selection of news sources are all serving to insulate citizens from broader influences and ideas';[6] cutting them off from the rough and tumble of democracy; denying them the formative experience of being confronted with unwanted ideas; denying them exposure to situations where tolerance has to be learnt? Or, more poetically, in a world with a diminished incidence of 'serendipitous encounters'[7]?

Some of these highlighted trends can contribute to the erosion of shared, collective experience and the reduction of common reference points; thus negatively affecting participatory democracy and engendering social fragmentation.[8] The net result of these trends and tendencies is that individuals are increasingly cocooning themselves in informational and communicational universes of their own creation; potentially leading to a Hall-of-

[3] *Bladet Tromso & Stensaas v. Norway*, Judgment of the European Court of Human Rights of 20 May 1999, Reports of Judgments and Decisions, 1999-III, para. 63, drawing on *Jersild v. Denmark*, Judgment of the European Court of Human Rights of 23 September 1994, Series A, No. 298, para. 31.

[4] *Prager & Oberschlick v. Austria*, Judgment of the European Court of Human Rights of 26 April 1995, Series A, No. 313, para. 38.

[5] See Article 10(2) of the European Convention on Human Rights.

[6] T. McGonagle, 'Changing Aspects of Broadcasting: New Territory and New Challenges', *IRIS plus* 2001-10, p. 5. For a more expansive treatment of these issues, see generally, C.R. Sunstein, *Republic.com* (Princeton, N.J.: Princeton University Press, 2001).

[7] A.L. Shapiro, *The Control Revolution* (USA: Public Affairs, 1999), p. (xvi).

[8] See further, C.R. Sunstein, op. cit., especially Chapter 1, 'the daily me', pp. 3-22.

Versailles type of effect where their own views are merely mirrored on all sides and distorted somewhat by virtue of excessive amplification. This stark prognosis is one of the arguments frequently invoked in favour of prohibition of websites and chat-groups dedicated to the propagation of hate speech and other types of extremist activities, for example.

Its starkness should not, however, be exaggerated. Filtering trends and proclivities towards self-insulation in the comforting surrounds of like-minded opinions are age-old practices and tendencies respectively. The Internet, like all of its forerunner communications technologies, will take some getting used to. It is typical for pioneering technological changes to set a blistering pace; for regulatory responses to lag somewhat behind this *peloton,* gasping for breath, and for cultural changes to remain largely out of the picture, with much ground to make up. Familiarity with the workings and potential of the online world will eventually harness much of the awe and apprehension that have characterized the debate thus far.

Quo vadis, then, for the media? First, is the cherished freedom of expression of the media – as staked out by the European Convention on Human Rights and the European Court of Human Rights – likely to be transposed *en bloc* to the online world? This is by no means sure. Crucially, though, the enjoyment of relevant freedoms by media actors in the offline world has always been contingent on the simultaneous exercise of certain duties and responsibilities (including, first and foremost, that journalists obey the ordinary criminal law,[9] and also that they act 'in good faith in order to provide accurate and reliable information in accordance with the ethics of journalism'[10]). There is nothing to suggest that such a proviso would not (or does not already!) apply online as well. This line of analysis begs further questions: for instance, in the online world, where it is much easier for individuals to engage in mass communication, are the above-mentioned distinctions between media actors and ordinary citizens *qua* communicators still valid? On what grounds could such distinctions then be sustained? Would the rationales of impact, influence and service of the public interest, discussed above, be able to survive the transition to the online world?

The second line of analysis is more oriented towards the practice of journalism in an online environment. With the ease of direct access to original sources of information, including official information and in any case the information which shapes the news of the day, there may be less of a role to be played by media professionals according to traditional conceptions of straight reporting. However, not everyone will invest the time and effort in checking original sources. Those who do will have to re-examine their approach to the intake and digestion of news and information available online. This need is prompted not only by the explosion of information caused by the advent of Internet-technology, but also by various qualitative features of that information: anonymity of, or lack of information about, the provider; lack of traditional intermediaries processing/providing the information; resultant difficulties in assessing the credibility of the information, especially when it originates in foreign or unfamiliar institutions, organizations or cultural contexts.[11]

[9] *Fressoz & Roire v. France*, Judgment of the European Court of Human Rights of 21 January 1999, Reports of Judgments and Decisions, 1999-I, para. 52.

[10] *Bergens Tidende & Others v. Norway*, Judgment of the European Court of Human Rights of 2 May 2000, Reports of Judgments and Decisions, 2000-IV, para. 53, drawing on *Goodwin v. United Kingdom*, Judgment of the European Court of Human Rights of 27 March 1996, Reports of Judgments and Decisions, 1996-II, para. 39.

[11] See further, A. Vedder, 'Misinformation through the Internet: Epistemology and Ethics', in A. Vedder (ed.), *Ethics and the Internet* (The Netherlands: Intersentia, 2001), pp. 125-132, at p. 128.

A particular role could perhaps be envisaged here for public service broadcasters if they were to assume the role of intermediaries or trustees by pointing the public towards other online material (extraneous to their own sites) to which they would have awarded a sort of ‘seal of approval’. By doing so, they would vouch for the reliability of content on other websites as being of the same high standards as on their own websites. Such a public-service kite-marking initiative could develop to become a useful navigational tool in the online world; enabling the website of the broadcaster to become a portal which would confer credibility on external content.[12] This ‘reliability-enhancing’[13] initiative would lead any reputable public service broadcaster to be identified as a ‘beacon of trust’[14] in the online world.[15]

Overall, the media will have to take on a more intermediary role; place greater emphasis on analysis and interpretation; counter the self-interest agenda of organizations providing information; help to sift facts from rhetoric and comment on the extracted matter. This is no mean challenge for a sector which arguably bears the most responsibility for ‘the triumph of idiot culture’ (i.e., the rise of a media culture in which serious journalism is eclipsed by an obsession with sensation and scandal).[16] This is a call for the media to rediscover their roots; their informative, dissident tradition. They will have their work cut out for them.

An interesting corollary question is often overlooked: what is the likely impact of the inexorable rise of Internet-related communication on the more traditional, offline media? Will Darwinistic theories apply? Will adaptation solely within the confines of the offline world prove possible? Or will virtually all (mass) media concerns have to reinvent themselves in such a way as to secure footholds in the off- and online worlds?

Possible role for regulation? Having 'developed by accretion, as piecemeal responses to new technology', contemporary media regulation can be considered 'complex and unwieldy'.[17] Different regimes often apply to different media and each regime is characterized by its own specificities. In consequence, it can prove difficult to identify or achieve consistency in these different regimes. The reality of ongoing and projected technological changes has already precipitated fresh thinking about the best (regulatory) means of attaining desired objectives; of honouring specific values. This is particularly true in light of trends of convergence and individualization.[18]

Such is the global and complicated nature of information technology and the modern media in general, that a multitude of additional regulatory difficulties (many of them unprecedented) has arisen. As concisely stated by Lawrence Lessig: '[R]elative anonymity, decentralized distribution, multiple points of access, no necessary tie to geography, no simple system to identify content, tools of encryption – all these features and consequences of the Internet protocol make it difficult to control speech in cyberspace.'[19] Coupled with this detailed observation is the fact that the innovative features of new information technologies have heightened the exposure of the traditional shortcomings of already-existing regulatory structures.

[12] Ibid., p. 130.

[13] Ibid., p. 131.

[14] D. Docherty, 'Empires and evolution: public service content in the new media', 27 *Intermedia* (Issue No. 2, May 1999), pp. 20-23, at p. 23.

[15] See further, T. McGonagle, 'Changing Aspects of Broadcasting: New Territory and New Challenges', op. cit., pp. 6-7.

[16] C. Bernstein, in E. Hazelcorn & P. Smyth (eds.), *Let in the Light: Censorship, Secrecy and Democracy* (Dingle, Ireland: Brandon Book Publishers Ltd., 1993), pp. 17-25, at p. 20.

[17] T. Gibbons, *Regulating the Media* (2nd Edition) (London: Sweet & Maxwell, 1998), p. 300.

[18] See further, T. McGonagle, 'Co-Regulation of the Media in Europe: The Potential for Practice of an Intangible Idea', *IRIS plus* 2002-10, p. 2.

[19] L. Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), p. 166.

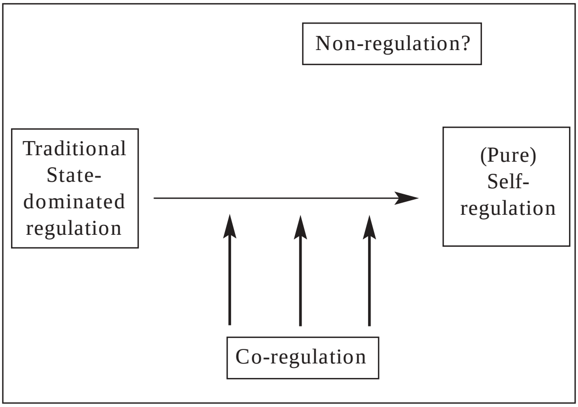
It is at this juncture that the notions of self- and co-regulation (S&CR) have been introduced into the debate.

Another impetus for the emergence of the notions of S&CR has been the current debate on, and quest for, better governance at the European level.[20] In this context, the European Commission's White Paper on European Governance has enumerated five key principles of good governance: openness, participation, accountability, effectiveness and coherence.[21] S&CR have been mooted as suitable means of helping to honour these principles in practice.

As demonstrated elsewhere,[22] the notions of S&CR are characterized by their fluidity. This definitional dilemma has been compounded by a lack of consistency in interpretations of the relevant (and other proximate) terms. (Pure) self-regulation is widely regarded as the 'control of activities by the private parties concerned without the direct involvement of public authorities'.[23] Co-regulation, for its part, refers to the 'control of activities by a combination of action from private parties and public authorities'.[24] Another term, coined to embrace as wide a selection of co-regulatory practices as possible, is 'regulated self-regulation', which describes 'a form of self-regulation that fits in with a framework set by the State to achieve the respective regulatory objectives'.[25] Another variant on the co-regulatory terminology is 'audited self-regulation',[26] a term which tends to enjoy greater currency in the US than in Europe. The least that can be stated with certainty is that the terms indicate 'lighter-touch' forms of regulation than the traditional State-dominated regulatory prototype.

It is imperative, however, that one avoids getting bogged down in definitional minutiae. What *is* important, though, is that one grasps that the principle of co-regulation implies a novel approach to regulation, by virtue of its in-built potential for involving an increased number of interested parties (to a greater or lesser extent) in a flexible regulatory process. It might be useful if one were to conceive of regulation in terms of a continuum stretching from the traditional State-dominated model through co-regulation to self-regulation.

Figure 1: Regulatory continuum



[20] See, in this connection, European Governance: A White Paper, Commission of the European Communities, 25 July 2001, COM(2001) 428 final; Mandelkern Group on Better Regulation Final Report, 13 November 2001; both of which were welcomed by the Laeken European Council, 14-15 December 2001.

[21] White Paper on European Governance, op. cit., p. 10.

[22] W. Schulz & T. Held, *Regulated Self-Regulation as a Form of Modern Government* (United Kingdom: University of Luton Press, 2003 – forthcoming); T. McGonagle, 'Co-regulation of the Media in Europe: The Potential for Practice of an Intangible Idea', op. cit.; C. Palzer, 'Co-Regulation of the Media in Europe: European Provisions for the Establishment of Co-regulation Frameworks', *IRIS plus* 2002-6; W. Schulz & T. Held, 'Regulated Self-Regulation as a Form of Modern Government', study commissioned by the German Federal Commissioner for Cultural and Media Affairs, Interim Report (October 2001).

[23] Mandelkern Group Report, op. cit., p. 83.

[24] Ibid., p. 81; see also, ibid., p. 17.

[25] W. Schulz & T. Held, forthcoming, op. cit., p. 85. The coiners of the term elaborate on its flexibility in the following manner: 'Thus, all means of governmental influence on self-regulatory processes can be described and phenomena referred to as co-regulation in other contexts are covered as well.'

[26] Audited self-regulation has been described as: 'the delegation by Congress or a federal agency to a nongovernmental entity the power to implement laws or agency regulations, with powers of review and independent action retained by a federal agency' – D.C. Michael, 'Federal Agency Use of Audited Self-Regulation as a Regulatory Technique', 47 *Administrative Law Review* (Spring 1995), pp. 171- 254, at p. 176.

The vagueness of what exactly co-regulation entails and the relative shortage of tried and tested models to examine have served to stymie its development, both as a concept and as a practice. While it is understandably difficult to conceive of and develop practical guidelines for co-regulation *in abstracto*, some recent research is likely to make a significant contribution to the concretization of relevant discussions.[27] This research examines a variety of S&CR models from different jurisdictions and from that starting point, has come up with a 'toolbox' of appropriate instruments for 'the regulation of self-regulation'. A related and perhaps self-evident observation is that some areas and cultural/legal contexts are better suited to S&CR than others.[28] But the vagueness that has characterized – and to an extent hampered – the debate on co-regulation so far should not be perceived uniquely in a negative light. It is precisely the same vagueness or intangibility that enables the notion to offer so much potential for milking.

The advantages of a committed co-regulatory system are numerous: greater representation and participation would result in the guiding documents commanding the confidence of all parties; the channelling of industry expertise into the regulatory drafting process would lead to greater sensitivity to the realities of the media world; an efficient system of sanctions, again elaborated multilaterally, would also enhance the credibility of the system (unlike State-devised equivalent structures which have traditionally tended to elicit resistance from industry players); procedural efficiency and expeditiousness; regulation would be more flexible, more easily and swiftly adapted to changing realities ushered in by technological and societal developments.

At the European level, there are increasing indications of a cautious consensus favouring the exploration of S&CR techniques specifically in relation to the media. As regards the

European Union, for instance, the ongoing review of the 'Television without Frontiers' Directive has listed the possibility of S&CR as one focus of its attention.[29] In addition, both the Directive on electronic commerce (Article 16)[30] and the Data Protection Directive (Article 27)[31] have stressed the importance of codes of conduct; an approach which represents a tentative move away from traditional regulatory techniques and arguably in the direction of co-regulation.

As regards the Council of Europe, while a formal review of the European Convention on Transfrontier Television has yet to be announced, a recent report[32] concludes with a consideration of the architecture of future regulation, including S&CR as possible options. There has been a guarded willingness to countenance S&CR at successive European Ministerial Conferences on Mass Media Policy (e.g. Prague, 1994; Thessaloniki, 1997; Cracow, 2000). The prospect has also been broached in the Committee of Ministers' Recommendation on

[27] W. Schulz & T. Held, op. cit.

[28] For a fuller discussion of the possible thematic ambit of S&CR (including with respect to the independence of journalists; tackling hate speech; the protection of minors; advertising, and technical standards), see T. McGonagle, 'Co-Regulation of the Media in Europe: The Potential for Practice of an Intangible Idea', op. cit. See also, *IRIS Special: Co-Regulation of the Media in Europe* (Strasbourg: the European Audiovisual Observatory, 2003).

[29] Fourth Report from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the application of Directive 89/552/EEC 'Television without Frontiers', COM (2002) 778 final, 6 January 2003.

[30] 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), OJ L 178, 17 July 2000, p. 1.

[31] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995, p. 31.

[32] Report by Dr Andreas Grünwald on possible options for the review of the European Convention on Transfrontier Television, Standing Committee on Transfrontier Television of the Council of Europe, Doc. T-TT(2003)002, 24 April 2003.

self-regulation concerning cyber content;[33] the Standing Committee's Statement on human dignity and fundamental rights of others,[34] and most recently and perhaps also most explicitly, the Council of Europe's Submission to the 2nd Preparatory Committee for the World Summit on the Information Society[35] and the Committee of Ministers' Declaration on freedom of communication on the Internet.[36]

The level of politico-legal support for S&CR as sketched above seems to be growing independently of any accompanying attempts to define its scope. This has predictably fuelled the criticism that passing textual references to S&CR are no more than lip-service on the part of governmental and intergovernmental organizations in their purported quest to attain high-minded principles for the enhancement of participatory practices in their decision-making processes. It has also fuelled scepticism about the practical appeal of S&CR. While this criticism is persuasive and this scepticism is not without foundation, neither should lead to the routine dismissal of S&CR as regulatory alternatives, without first attempting to engage meaningfully with the substantive issues involved.

Remaining concerns. In the preceding section, a number of so-called regulatory alternatives have been canvassed. Another, more fundamental question, is obviously whether there should be regulation at all. Or more aptly, whether there should be additional regulation, for much time and effort have thankfully been spent debunking the all-too-frequently recurring misperception that the online world is unregulated. In regulatory matters, reflex should be replaced by reflection. It is only once the need for specific regulation has been convincingly established that its possible mechanics should be considered. There is a certain unease among critics of S&CR about the sharing (or partial transfer) of regulatory responsibilities that have traditionally been the preserve of the State. The fear that S&CR bodies would lack the authority, accountability and a host of other (procedural) safeguards necessary for ensuring the public service role they would be expected to fulfil is also very palpable.

In response to these concerns, it ought to be pointed out that co-regulation should not be perceived as a result-driven phenomenon. One of the most attractive features of co-regulation is that its structures are designed to optimize quality of governance and it attaches paramount importance to process values. Greater representation and participation in regulatory structures is one of the first of these process values that comes to mind; an inclusiveness of a greater selection of parties. In the same vein, responsiveness to the public and an ability to serve the stated interests and needs of diverse societal groups is another prerequisite. The process should remain transparent and easily accessible to the public. Structures should be in place ensuring user-friendliness as regards complaints and appeals mechanisms, with the possibility of ultimate recourse to an independent arbiter or the courts. Co-regulation offers a structural framework that is particularly conducive to guaranteeing these – and other – process values.

[33] Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), 5 September 2001.

[34] Statement (2002)1 on Human Dignity and the Fundamental Rights of Others, Standing Committee on Transfrontier Television of the Council of Europe, 12-13 September 2002. For a fuller discussion of the relevant provisions of these texts, see T. McGonagle, 'Co-Regulation of the Media in Europe: The Potential for Practice of an Intangible Idea', op. cit.

[35] Democracy, human rights and the rule of law in the Information Society, Contribution by the Council of Europe to the 2nd Preparatory Committee for the World Summit on the Information Society, Doc. WSIS/PC-2/CONTR/32-E of 9 December 2002.

[36] Adopted by the Committee of Ministers of the Council of Europe on 28 May 2003.

Operational autonomy for the co-regulatory body is also crucial, and adequate, independent financing is a *sine qua non* for the same if the body is to be insulated from powerful political and commercial interests. A co-regulatory system's accountability to the public could be safeguarded by structured evaluation processes (e.g. governing the start-up phase which would include the drafting of codes, guidelines, etc., and equally once the system is up and running and the codes, etc., are being implemented). An earnest espousal of these principles – which could be set out in the enabling legislation that would set up the co-regulatory system – would go a long way towards meeting some of the ideals of good governance as set out in the European Commission's White Paper, such as the creation of 'a reinforced culture of consultation and dialogue'.[37]

An increasing openness to the potential of S&CR is now very much a feature of the regulatory *Zeitgeist*. For co-regulation to establish itself as a viable regulatory model, it will need to bridge the gap between theory and practice; a gap of considerable scepticism and resistance. In order to do so, its drivers will have to keep a resolute focus on the primary goal to be achieved: to ensure a more equitable type of regulation which would enhance opportunities for freedom of expression, not curtail them.

[37] Op. cit., p. 16.

Sandy Starr

Putting Freedom Back on the Agenda: Why Regulation Must be Opposed at all Costs

Introduction. The argument against regulation of decentralized networks is simple: regulation of decentralized networks should be categorically opposed, on the grounds that it restricts the democratic freedoms exercised over those networks.

But this argument is frequently sidelined, in favour of one of two alternative arguments – each of which was endorsed by several speakers at the OSCE 'Freedom of the Media and the Internet' conference:

- Those who favour regulation tend to argue that far from restricting freedom, regulation is necessary to *guarantee* freedom over decentralized networks.
- Those who do not favour regulation tend to argue that decentralized networks *cannot* be effectively regulated, because the technology involved is inherently resistant to regulation.

In this paper, I take issue with each of these arguments, and then I conclude with a critique of the 'Amsterdam recommendations' that came out of the OSCE conference (and which are included at the end of this volume).

Is regulation necessary to guarantee freedom? The prevailing assumption that informs Internet regulation – and that, increasingly, informs policy and law more broadly – is that individuals are weak, vulnerable to the myriad ills of the world, and in desperate need of protection. At the heart of most discussions about Internet freedom and Internet regulation is the presumed weak individual, who requires external intervention before they can exercise any freedom.

This conception of the weak individual was given a new legitimacy by the terrorist attacks of 11 September 2001, which reinforced a false counterposition between freedom and security. After 11 September, governments with a long-standing interest in prying into our lives were allowed to present such intrusion as being in our interests, necessary to prevent future terrorist attacks.[1] The distrust of the state which traditionally underpinned principles of freedom was turned on its head – so that rather than people seeking to protect their freedom from the state, the state purported to protect people's freedom from other people.

But it isn't just the threat of terrorism that looms large in justifications for Internet regulation. Increasingly, the very act of communication – through words, images and sounds – is characterized as something that can do injury to others and cause trauma. Increasingly, the distinction between communication and action is being erased in law and policy.

It is falsely assumed that communication is directly harmful to its recipients, that communication impels its consumers to act, that communication is equivalent to the abuses it describes and depicts. In cases involving child pornography, such assumptions have culminated in the bizarre legal notion that an individual can be complicit in an act that originally took place without their knowledge or involvement.[2]

Perhaps the best example of the assumption that communication can cause direct harm is the category of 'hate speech', which has unfortunately become widely recognized in national and international law. When, at the OSCE 'Freedom of the Media and the Internet' conference, speakers such as myself and Yaman Akdeniz of Cyber-Rights & Cyber-Liberties UK questioned the validity of 'hate speech' as a category, OSCE Representative on Freedom of the Media Freimut Duve was outraged. Duve argued that 'we don't have a single conflict at the moment that is not based on the use of speech to encourage people to kill each other', and that 'the conflicts of tomorrow will not be conflicts of interest, but conflicts of hate speech'. Certainly, speech and the media are used in conflicts to promote the interests of opposing sides – indeed, it would be odd if this were not the case. But to conclude from this that it is necessary to prohibit communication, as a pre-emptive measure to prevent future conflicts, betrays a deeply patronizing view of the citizens of sovereign states.

This patronizing attitude is characteristic of the way that regulators view Internet users. Take the way that children are used as a moral shield for regulation – to listen to today's regulators and legislators, you would think that our entire society should be reorganized so as not to traumatize minors. The UK Government, for example, has done everything in its power, including manipulating statistics, to characterize the Internet as a dangerous place for children.[3]

Meanwhile, child pornography is the issue that provokes the greatest moral outcry and call for Internet regulation worldwide, and is seen as the ultimate justification and benchmark

[1] A recent report notes that erosions of privacy following the 11 September 2001 terrorist attacks were not 'necessarily new; the novelty is the speed in which these policies gained acceptance, and in many cases, became law'. Sarah Andrews (ed.), *Privacy and Human Rights: An International Survey of Privacy Laws and Developments 2002* (Washington/London: Electronic Privacy Information Centre/Privacy International), p. 27 <http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf>.

[2] See Barbara Hewson, 'Fetishising images', *spiked*, 23 January 2003 <http://www.spiked-online.com/printable/00000006DC06.htm>.

[3] See Sandy Starr, 'Are you the one in four?', *spiked*, 27 March 2001 <http://www.spiked-online.com/printable/00000000553F.htm>; Sandy Starr, 'We scare because we care', *spiked*, 7 January 2003 <http://www.spiked-online.com/printable/00000006DBBF.htm>; Sandy Starr, 'Shevaun and the scaremongers', *spiked*, 5 August 2003 <http://www.spiked-online.com/printable/00000006DEAA.htm>.

for Internet regulation. But child pornography is also the least understood or rationally evaluated problem on the Internet. Even the director of the Combating Internet Paedophiles in Europe project admits that ‘it is difficult to find another area of substantial policy development that has been based on such little empirical evidence’[4].

Early champions of Internet freedom were often utopian and idealistic[5], but in their aspiration for a sphere where people can mingle and exchange ideas without interference or censure, they differed significantly from the Internet’s current evangelists. Their aspiration didn’t patronize people by presuming to help them use the Internet to empower themselves – it merely asked that decentralized networks be preserved as a place where people can communicate and associate freely.

Today, by contrast, we have touchy-feely discussions of ‘edemocracy’, ‘social inclusion’, and the problem of the ‘digital divide’ – discussions that, properly speaking, have nothing to do with individual freedom, but instead are about the wellbeing of victim figures. Information technology is widely characterized, not as a tool that can be used for progressive ends, but as a crutch for the victim. Such attitudes go beyond traditional regulation, and extend to areas such as trusted computing (an initiative to make computing more ‘trustworthy’, endorsed by Compaq, Hewlett-Packard, IBM, Intel, and Microsoft[6]) and social software (software championed by technologists as the solution to declining levels of political participation[7]).

All of this is bad enough, but it is positively disastrous when it means that the state becomes characterized as a benevolent actor, proactively enforcing our freedoms on our behalf. The state is explicitly conceived in these terms within the framework of human rights, as codified in international (and latterly, national) law since the Second World War.[8] Instead of prescribing limits to state power in order that individual freedom may flourish, human rights legislation directly prescribes the rights that individuals are entitled to exercise. Where the First Amendment to the US Constitution begins 'Congress *shall make no law*...'[9], Article 1 of the European Convention for the Protection of Human Rights and Fundamental Freedoms begins 'The High Contracting Parties *shall secure to everyone*...'[10].

Regulation of decentralized networks can only be self-perpetuating, once the state is given such licence to step in and 'secure' our freedom from, say, the practices of unscrupulous companies such as Microsoft. This is because such a 'freedom' is a myth. Our privacy from the marketplace is always qualified, because as long as we consume goods and services, then to some extent our private pursuits occur within the marketplace. On the other hand, we can, and should, aspire to comprehensive privacy from the state.

The compromise of freedom bound up with the framework of human rights was epitomized by my fellow panellist at the Amsterdam conference, Páll Thórhallsson, legal officer

[4] Max Taylor, 'Child Pornography and the Internet: Challenges and Gaps', Combating Internet Paedophiles in Europe, December 2001 <http://copine.ucc.ie/attachments/challenges.pdf>.

[5] For example John Perry Barlow, with his infamous 'A declaration of the independence of cyberspace' of 1996 <http://www.eff.org/~barlow/Declaration-Final.html>.

[6] See the Trusted Computing Platform Alliance <http://www.trustedcomputing.org> website.

[7] See Leander Kahney, 'Web antidote for political apathy', *Wired News*, 5 May 2003 <http://www.wired.com/news/print/0,1294,58715,00.html>. For a comprehensive overview of the field of social software, see William Davies, *You Don't Know Me, But...: Social Capital and Social Software* (London: Work Foundation, 2003) <http://www.theworkfoundation.com/pdf/1843730103.pdf>.

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

[9] Amendments to the Constitution of the United States of America, Article I, my italics <http://www.house.gov/Constitution/Amend.html>.

[10] Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocol no 11, Council of Europe, Article 1, my italics <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.

in the Council of Europe Directorate General of Human Rights. For every statement of ‘no censorship’, Thórhallsson put forth a statement of ‘balance between freedom of expression and other rights’, ‘remedies (right of reply, fines, damages, imprisonment)’, and ‘encouraging responsibility by private actors: self-regulation/co-regulation’.

Such ‘balance’, ‘remedies’, ‘responsibility’ and ‘self-regulation/co-regulation’ are not means of guaranteeing freedom, but are in fact insidious new restrictions on freedom. It is these new restrictions, and the invisible effect that they have upon the Internet, that give the lie to the assumption that decentralized networks cannot be effectively regulated. To this we now turn.

Can decentralized networks be effectively regulated? In an otherwise accurate and comprehensive outline of the global state of Internet regulation given at the OSCE ‘Freedom of the Media and the Internet’ conference, my colleague Felipe Rodriquez, founder of the Internet service provider XS4ALL, succumbed to a common fallacy. He argued that on the Internet, ‘any censorship can, and will, be defeated’[11].

From such an assumption comes the lazy belief that free expression on the Internet will be protected by technical default, rather than as a result of principled conviction and argument. This is entirely wrong. It may be difficult to regulate decentralized networks, but experience tells us that wherever such networks *can* be regulated, they *will* be regulated. However insignificant such regulation may initially appear, it is likely to have an insidious effect, as dangerous precedents are set.

As Internet usage became more popular in the 1990s, the regulatory authorities found themselves frustrated by decentralized networks, and up against the limits of what traditional forms of media regulation can achieve. Their response was to introduce methods of regulation that mimicked the decentralization of the network, notably self-regulation – the exporting of the government's regulatory tasks to the marketplace, where regulation disappears from public view, and from the court of public opinion.

One popular method of self-regulation is the imposition of ambiguous liabilities upon ISPs, which makes ISPs regulate not according to any clear legal principle, but out of a generalized fear. When regulation mimics the decentralization of networks, and devolves into self-regulation, such quaint principles as the presumption of innocence, the right to free speech, and the fair use of creative works are dismantled.[12]

Such invisible regulation is difficult to resist. If you're a techno-literate activist and your ISP removes something from your website, then perhaps you can kick up a stink. But if you can't be bothered to contest the removal of content from your website, or if you don't understand that the content might have been removed wrongfully, then that means that nobody else in the world will ever see that content – or even know that it existed. Self-regulation has a chilling effect upon free expression for *all* Internet users, not just content providers and customers of ISPs.

Another level at which freedom in decentralized networks might be undermined is the purely technical. Just because hackers and crackers always seem to be able to find a way to get around encryption and evade the authorities, is no reason to assume that subtle changes can't be made, at the level of

[11] Felipe Rodriquez's speech was adapted from his paper 'Burning the village to roast the pig: censorship of online media', Felipe Rodriquez, *From Quill to Cursor: Freedom of the Media in the Digital Era*, (Vienna: Organization for Security and Co-operation in Europe, 2003), p. 108 <http://www.osce.org/documents/rfm/2003/04/41_en.pdf>.

[12] For an extensive debate on the merits and demerits of self-regulation for online copyright infringement, see '*spiked*-IT debate: Copyright in the digital age', *spiked*, 29 August – 4 November 2002 <http://www.spiked-online.com/copyright>.

technology, that result in a less free Internet overall. Besides, hackers and crackers are a techo-literate minority – while their activities might be significant, they are not a reliable barometer of the freedom generally exercised on the Internet.

There's not even any reason to assume that the most fundamental standards and protocols that enable the Internet to function couldn't be changed in some way, to work against freedom. These standards and protocols are neither eternal nor God-given – somebody had to make them, and somebody can unmake them. Just because the Internet Engineering Task Force and related standards-developing organizations are international communities, open to any interested individual, doesn't mean that the gulf that separates them from the exercise of political interest can't be traversed – or hasn't been traversed in some way already.[13]

Another fallacy harboured by those who believe that decentralized networks cannot be regulated is the notion that civil disobedience is equivalent to a proper political debate. Civil disobedience can be important to politics, and I'm the last person to denigrate it. But unless civil disobedience is accompanied by informed and principled political debate, there is a danger that it will result merely in an escalation of cynicism on both sides of a dispute, and will encourage the authorities to respond in an even more authoritarian manner – as has occurred with the Napster/Gnutella/KaZaA controversies of recent years, where large numbers of people have, strictly speaking, flouted copyright law by downloading files for free.

Ultimately, the notion that decentralized networks *cannot* be regulated is just as inimical to freedom as the notion that decentralized networks *should* be regulated. It is vital that regulation is met with concerted opposition – and not just in the form of civil disobedience, which lets the authorities off the hook by failing to engage with them intellectually.

Conclusion: taking the 'Amsterdam Recommendations' to task.

The 'Amsterdam Recommendations' issued by the OSCE, that came out of the proceedings of the Amsterdam conference, are an accurate reflection of the event's uneasy mixture of firm principle and fearful compromise. Some of the recommendations – 'technology as such must not be held responsible for any potential misuse'; 'access to the public domain is important for both technical and cultural innovation'; 'there is no need for new legislation'; 'new forms of censorship must not be developed' – are welcome.

But other recommendations muddy the waters, by confusing issues of individual freedom with the imposition of various forms of responsibility. For example, recommendations that 'access to digital networks and the Internet must be fostered', and that 'the right to disseminate and receive information is a basic human right', go beyond guaranteeing freedom, and suggest that there should be some kind of intervention by the authorities in order to get people online.

Of course, people should have the wealth at their disposal to get online if they choose, and telecommunications infrastructure should be extended to deprived areas. But beyond that, whether people get wired up or not is entirely their own business. To make a moral good out of people using the Internet is to invite intervention into their lives, and actually runs contrary to the principles of freedom embodied in the more progressive Amsterdam Recommendations.

The concluding Amsterdam Recommendation, which encourages 'values of professional journalism...to guarantee a free and responsible media in the digital era', is perhaps the most troubling of all. The wonderful thing about the Internet

[13] See the 'Internet Engineering Task Force overview' section of the Internet Engineering Task Force website <http://www.ietf.org/overview.html>.

is precisely that just about anybody can publish on it, and it is up to the individual reader to assess what is 'professional journalism' and what is not. Internet journalism already has to prove its 'professional' credentials in the court of public opinion – no additional guarantee of quality, in the form of the OSCE encouraging 'values of professional journalism', is necessary.

The two words that really jar in this final Amsterdam Recommendation are 'free' and 'responsible'. Calls for Internet freedom at the 'Freedom of the Media and the Internet' conference were a welcome riposte to the growing tide of global Internet regulation. Calls for responsibility, on the other hand, strengthened the regulators' hand, and expressed a diminished view of the Internet user.

Internet users are quite capable of deciding for themselves what to read, watch, listen to and download, and whether they think it's any good to boot. The imposition of new responsibilities, in order to safeguard users, can only insult their intelligence and undermine their freedom.

Peter Noorlander

Freedom of Expression and Internet Regulation

Introduction. Over the last decade, the Internet has become a key instrument for the right to freedom of expression. It allows for the dissemination of opinions and ideas that would not normally find their way to a mass-audience and provides a near-instant means of communication for millions. The diversity of content on the Internet is enormous; as the US Supreme Court famously noted, 'content on the Internet is as diverse as human thought.'[1]

However, in its diversity the Internet also attracts considerable criticism. To many, the Internet is an anarchic entity in need of regulation. In some countries, it is demonized as a safe haven for paedophiles, terrorists and copyright pirates, while in others, less than democratic regimes see the ability of the Internet to give voice to dissident voices as an unacceptable political threat. In response, legislation is being passed in countries around the world to 'control' online activity – for example by requiring all web users to register, or by implementing laws that authorize monitoring of online activity. These initiatives are additional to existing laws of general application, such as regarding defamation, that apply to all publications – online or offline.

This paper indicates the extent to which these various forms of regulation impact on the exercise of the right to freedom of expression online. It examines various different forms of state regulation as well as the many self-regulatory initiatives that have sprung up over the last few years. On the eve

[1] 521 US 844 (1997), under I.

of the World Summit on the Information Society,[2] this paper finally examines what steps should be taken to make the right to freedom of expression online a reality for everyone.

Controlling the net. The growing importance of the Internet means that access has become an important public issue, in terms of both restrictions as well as measures to promote and even provide access. In some countries, such as the United Kingdom, the Government has pledged to provide computers to all low income families to prevent exclusion from the 'information society'. The same issue is at stake internationally, where the growing poverty-gap between 'information-rich' and 'information-poor' countries means that concerted action is necessary to bridge the international 'digital divide'.

However, while the international community is working to address the 'digital divide', in a number of countries public policy actually has the effect of limiting Internet access, for example by requiring users or Internet service providers (ISPs) to obtain a licence or to register. In both Italy and Spain, recently passed legislation requires everyone with a website to register with central authorities[3] while in Armenia, all ISPs need to obtain government registration.[4]

Under international law, such requirements constitute an 'interference' with the right to freedom of expression and must be very carefully scrutinized. The International Covenant on Civil and Political Rights, an international treaty signed by 149 countries,[5] requires that no State should interfere with the right to freedom of expression unless the interference is provided by law, pursues a legitimate aim and can be considered 'necessary in a democratic society'.[6]

Under this test, outright restrictions on access such as by prohibiting the possession of a modem or other communications equipment constitute an illegitimate restriction on the right to freedom of expression.[7] Licensing[8] of individual Internet users or Internet service providers is likewise illegitimate;[9] and any registration requirements,[10] for users as well as for service or content providers, are of very doubtful legitimacy. In a March 2000 case, the UN Human Rights Committee considered a law which required all publishers, no matter how small their publication, to register with central authorities. The Committee considered that requirement to establish 'such [an] obstacle as to restrict the author's freedom to impart information'.[11] As there was no evidence that the measure was necessary for the protection of public order or for the protection of the rights of others, the requirement constituted a violation of the right to freedom of expression. This merely concerned a registration scheme for media publishers; a scheme for all Internet users to register would pose an even greater restriction on the right freely to receive information as well as exerting a serious chilling effect on the right to disseminate information.

[2] <http://www.itu.int/wsis/>

[3] In Spain, this is enforced through Law 34/2002, 11 July 2002, 'de Servicios de la Sociedad de la Información y Comercio Electrónico'; in Italy, the applicable law is Law No. 62 of 7 March 2001, 'Nuove norme sull'editoria e sui prodotti editoriali e modifiche alla legge 5 agosto 1981, n. 416.', published in the Official Gazette No. 67 of 21 March 2001.

[4] Law on Licensing: <http://www.internews.am/legislation/english/Law-on-Licensing.zip>.

[5] UN General Assembly Resolution 2200A(XXI) of 16 December 1966, in force 23 March 1976.

[6] Article 19(3), ICCPR. The implications of this will be considered in further detail below.

[7] *Autronic AG v. Switzerland*, 22 May 1990, Application No. 12726/87 (European Court of Human Rights).

[8] By 'licensing' we refer to a system whereby a user or provider needs to obtain governmental authorization in order to be able to carry out online activities.

[9] For a full discussion of the human rights implications, see the Inter-American Court of Human Rights' decision in *Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism*, Advisory Opinion OC-5/85 of November 13, (Series A) No. 5 (1985).

[10] By registration, we refer to a system whereby a user or provider is required to notify central authorities of their online activities.

[11] *Laptsevitch v. Belarus*, 20 March 2000, Communication No. 780/1997, para. 8.1.

Similarly, any regulation of Internet content, whether Internet-specific or imposed through laws of general application, must not fall below the standards set by international human rights law and must take into account the special nature of the Internet. In Europe, North America and Australia, there has been a considerable backlash against government attempts to regulate Internet content. Content restrictions are often seen as censorship and the US Supreme Court has struck down various legislative proposals to restrict the availability of 'obscene' or 'indecent' material for this reason. For example, there is no 'scarcity of frequencies' on the Internet that would justify the kind of overarching regulation found in the broadcast sector. With regard to obscene materials, because the Internet is not like a bookstore, where the top shelf can be designated for certain titles, or like television, where certain material can be broadcast only after 9 pm in the evenings, it cannot be regulated in the same way as those media. While from a theoretical perspective, the same laws apply – what is obscene offline is also obscene online – the rules often cannot be enforced in the same manner.

Another problem with nationally-imposed content regulation is that different countries all attempt to enforce their own national laws over the global Internet. Crudely put, this leads to the danger that the entire Internet might succumb to the standard of the least tolerant regulator. Already, cases are being decided that point in this direction, including the case of a Zimbabwean judge asserting jurisdiction over the British newspaper *The Guardian* on the basis that it can be accessed by any Zimbabwean who knows how to operate an Internet browser (although at trial, the prosecutor first could not find an Internet connection that worked and, after the whole court had relocated to an Internet cafe, then discovered that a clever someone at the *Guardian*'s technical department had removed the offending article from the server),[12] the infamous Yahoo!

auctions case in France[13] and the ongoing Gutnick saga in Australia.[14] While the Zimbabwean example can arguably be ignored, the Australian and French cases are more difficult to reconcile since although US, French and Australian laws differ in how they strike the balance between competing interests such as the protection of reputation or anti-racism considerations and freedom of expression, all are broadly compliant with international human rights standards.[15]

Other problems with regard to regulation of Internet content concern the question of who can be regarded as 'publisher' – Can an ISP be held liable for content put online by their customers?[16] Can a person be held liable for the content of pages linked to?[17] – and the question how long material published in online archives remains actionable – Should it be possible for someone to file a lawsuit for defamation with regard to an article that was published years before the user came across it on a website?[18]

[12] Although the Court held that it could exercise jurisdiction, the defendant journalist was eventually acquitted on other grounds. Days later, he was deported from Zimbabwe: <http://media.guardian.co.uk/zimbabweandthemedia/story/0,11522,755688,00.html>.

[13] Yahoo! was sued by French anti-racism groups to remove Nazi memorabilia from the auctions section of its site. A Californian court eventually ruled that a French court order to this effect could not be enforced as it was incompatible with the First Amendment: *Yahoo!, Inc. v. La Ligue Contra Le Racisme et L'Antisemitisme*, 145 F. Supp. 2d 1168 (N.D.Cal. 2001): <http://www.cand.uscourts.gov/>.

[14] This concerns an Australian businessman who is suing Dow Jones for an article describing various of his business practices that originally appeared in a magazine published in the United States, but that was also available to online subscribers in Australia. Mr. Gutnick sued in Australia, where defamation laws are in his advantage. The defendants have taken the case to the UN Human Rights Committee.

[15] See, for example, *Lehideux and Isorni v. France*, 23 September 1998, Application No. 24662/94 (European Court of Human Rights).

[16] For an overview of the legal situation regarding this in the US, see: <http://www.bitlaw.com/internet/isp.html>.

[17] E.g. <http://www.eff.org/br/20030807_eff_pr.php>.

[18] In *Tranchant v. Bardin*, Arrêt no. 6374, 16 October 2001, the French Cour de Cassation applied a strict limitation period to online content. However, in *Loutchansky v. Times Newspapers* [2001] ECWA Civ 1805 the English Court of Appeal held that an Internet publication must be considered to be published anew every time it is accessed.

Because of these problems, 'self-regulation' has been hailed by some as the preferred alternative to state regulation. Initially, this focused on the development of blocking and filtering software to enable 'parental control'. However, when this software began to show promise it was quickly co-opted by governments around the world. Countries like China have bolted it on to their national points of access to filter out Amnesty International, Google, the BBC and other 'subversive' sites while in countries such as the UK or the US it is now often installed as mandatory on terminals in public libraries. The former example is clearly illegitimate, but the latter is problematic also.[19] Given that many of the software packages filter on the side of caution, blocking for example websites discussing gay and lesbian issues alongside sites offering porn, this seriously restricts the right to access to information of those who rely on those terminals for access – often the poor.

Other forms of self-regulation, including the operation of 'hotlines' for undesirable content and the development of a 'global ratings mechanism' have been criticized as representing government censorship in a corporate guise. A good example is the establishment of the Internet Watch Foundation (IWF) after the Metropolitan Police sent a letter to all United Kingdom ISPs, notifying them of a number of newsgroups that contained sexually explicit material and reminding them that the publication of obscene material is an offence in the UK. The IWF was subsequently established with a wide brief to halt the spread of child pornography on the Internet.[20] Similar industry organizations have now been established in other countries. While the prevention of serious crime online is an important goal, it is undesirable that ISPs act on behalf of the police as censors for two reasons. First, ISPs are not judicially qualified to determine whether a certain website might contravene the law or whether an individual user might be likely to publish something that is considered to be illegal. When faced with a borderline case, they are likely to err on the side of caution and decide not to host the site. Second, there are no safeguards to ensure that ISPs do not abuse their powers and there is no system to call ISPs to account. This is problematic, particularly since the ISPs' actions will have an important impact on the right to freedom of expression of those who they decide to refuse access, as well as the right of others to receive information. Users whose access rights are summarily restricted by a private party typically have no legal redress whatsoever.

Finally, in discussing forms of Internet 'control' the issue of online snooping must not be overlooked. Surveillance and monitoring practices have a serious inhibiting effect on online expression. If an Internet user suspects that his or her online movements are monitored, he or she will exercise caution with regard to statements made or sites visited. Technology can provide some solace; anonymity and encryption tools are constantly being improved. However, their success in doing so has meant that governments have tried to restrict the use of such software.

States implement surveillance systems for different reasons. In countries such as China, law enforcement agencies are alleged to engage in wide-scale monitoring activities to prevent individuals within their jurisdiction from discussing politically damaging issues. In countries such as the United Kingdom or the Netherlands, monitoring takes place for law enforcement

[19] Although the US Supreme Court in *United States et al. v. American Library Association, inc., et al.*, 000 U.S. 02-361 (2003) saw no First Amendment issues in the linking of federal subsidies for libraries to the installation of filters on public terminals.

[20] As described by Ruth Dixon, former Deputy Chief Executive, Internet Watch Foundation, in 'Co-operative forms of regulating the Internet' <http://www.humanrights.coe.int/media/cyberforum/rep-dixon.rtf>.

or national security-related purposes and interception warrants are granted only for these purposes. Since the events of 11 September, many countries have enacted new legislative powers in this field and it may be assumed that such activities are now on the up. The Council of Europe's much-maligned Cybercrime Convention[21] can be seen as a related development, as can the ever-increasing data-retention demands on ISPs. In addition, states such as Zimbabwe and Belarus have now started using the language of 'fighting terror' to justify the various measures they take to restrict freedom of expression, online as well as offline.

There can be no doubt that it is legitimate that law enforcement agencies should have the appropriate tools to prevent, detect and prosecute crime, online and offline. However, the balance to be struck between the interests of privacy and free expression on the one hand, and the interests in preventing and detecting crime on the other, is a delicate one, as has been stressed time and again by courts including the European Court of Human Rights.[22] Legitimate concerns have been expressed that as currently framed, many surveillance laws leave executive agencies too much leeway while providing too little protection for human rights.

Realizing freedom of expression online: the World Summit on the Information Society. In December 2003 and again in 2005, the World Summit on the Information Society will take place in two rounds, in Geneva and in Tunis. As the first global summit meeting to discuss communication issues, this presents a unique opportunity to formulate an international strategy to make the right to freedom of expression a reality for everyone rather than a lofty aim to be achieved at some point in the future.

As a starting point, it is crucial that the Declaration and Action Plan to be developed are firmly grounded in international human rights law. The international standard on freedom of expression is laid down in Article 19 of the Universal Declaration of Human Rights, and further elaborated in the International Covenant on Civil and Political Rights, also at Article 19. This recognizes that freedom of expression is not an absolute right and that states have a legitimate interest in proscribing, for example, child pornography on the Internet. However, it requires that any measures taken should be provided by law and necessary in a democratic society in pursuit of a legitimate aim.[23] This test is a very strict one: a state cannot merely pass a law restricting Internet content and justify this by stating that it is 'reasonable in light of recent terrorist events': the state will also have to point to some pertinent and relevant facts justifying the measure, showing that it is 'necessary' rather than 'useful' or 'appropriate'.[24] In addition, the law itself will have to provide guarantees and safeguards against abuse. Similar standards must be applied to surveillance legislation: a monitoring operation may be instituted only if this is truly 'necessary' for national security or crime prevention purposes.[25]

Moreover, under international law the right to freedom of expression also has a positive component, requiring states to take active steps to ensure that all persons within their jurisdiction can exercise the right.[26] This means that states are

[21] Adopted in Budapest, 23 November 2001, ETS No. 185.

[22] E.g. *Klass and others v. Federal Republic of Germany*, 6 September 1978, Application No. 5029/71 (European Court of Human Rights).

[23] See Article 19(3) of the International Covenant on Civil and Political Rights.

[24] E.g. *Sunday Times v. the United Kingdom*, Judgment of 26 April 1979, para. 59 (European Court of Human Rights).

[25] See *Rotaru v. Romania*, 4 May 2000, Application No. 28341/95 (European Court of Human Rights).

[26] E.g. the European Court of Human Rights' judgment in *Vgt. Verein gegen Tierfabriken v. Switzerland*, 28 June 2001, Application No. 24699/94, para. 45.

under an obligation to provide a climate within which all can have access, but also that states should take action to prevent restrictions imposed by private actors. In the context of online freedom of expression, these two overarching principles have important consequences for access as well as content regulation, and for all activities that may have a ‘chilling effect’ on the right to freedom of expression.

But in order for WSIS to be a success it will have to go beyond these general principles. Concrete rules and minimum standards need to be formulated to make online freedom of expression a reality for everyone. At a minimum, these should include the following:

- States, acting jointly as well as individually, should take active steps to abolish the digital divide;
- Measures that tend to restrict access to the Internet, including all licensing and registration requirements, should be abolished;
- Legislation limiting Internet content should be in line with the standards laid down in Article 19(3) ICCPR;
- As a general rule, states should not seize jurisdiction over content uploaded in another country;
- ISPs should not be held liable for material uploaded by third parties, and no-one should be liable for material linked to;
- In defamation and related cases, the single-publication rule should be applied to all Internet content;
- Internet users should have judicial recourse against the decision of an ISP not to host ‘objectionable’ material or to remove certain content;
- The choice to install blocking and filtering software should be left to the end user;
- Monitoring and surveillance operations should only be undertaken where they are absolute necessary to achieve a

legitimate aim, and then on the basis of transparent legislation that provides for accountability of the agency involved.

The WSIS should work to create a legal framework that facilitates rather than hinders freedom of expression online. A failure to implement standards along the lines suggested in this paper will mean that it has been a missed opportunity.

The technical and economic framework: How are code and companies influencing Freedom of the Media on the Internet?

Christian Ahlert

Technologies of Control: How Code Controls Communication

You can‘t take something off the Internet – it‘s like taking pee out of a pool.
(US News Radio 1995)

As computers are increasingly used for manifold human transactions – from simply sending e-mails, to commercial activities such as banking online, and, surely more importantly, also for conducting political campaigns and the dissemination of political information in general – we face the classic political question of deciding how control over communications in the digital realm should be governed.[1] The question of who regulates, and perhaps censors, the content of communications is not a new issue. But, because of 1) the less transparent way in which networked digital systems are indeed regulated, by 2) a variety of highly effective control methodologies, in conjunction with 3) often naïve and confusing conceptions of self-regulation, corporations and specific Internet organizations rather than elected officials are deciding what can be communicated in the digital world.

Against this context this paper offers a *tour d’horizon* about the relationships among networked digital communication (mainly the Internet), current regulatory strategies, their political costs, and the technical characteristics of digital media. It is also an attempt to analyse the complex interrelationship between standards, protocols and software code on the one side, making

[1] Compare also Keohane and Nye (1998) who asked a similar question, but, as the paper will suggest, a definitive answer has not been found as of yet, but rather a wrong and potentially dangerous regulatory ideology has become consensus.

up the Internet, and communication and control on the other. Firstly, I argue that the interrelationships between 'Digital Code', 'Law' and 'Politics' need to be better understood if we want to make certain that those who regulate digital content are accountable to the regulated. Second, I argue that the existing forms of content control rely on private intermediaries to censor undesirable content, a system of control that poses significant political, ethical and legal issues. Finally, I conclude with a critique of current self-regulatory strategies as a form of Internet content regulation.

Technology and control in the digital paradigm. There are a number of misconceptions about the relationship of technology and control in networked digital media.[2] First, that the Internet by design is inherently good for the freedom of the media and expression, and second that no government can single-handedly control the net, meaning that nobody controls the Internet. Secondly, this has led to a misguided understanding of who is building and how in the digital communication chain – making up what we call the Internet – and how this affects the regulation of communication. But, surely, we will only understand if and how freedom of speech and expression is being constrained and subsequently if and how it can be protected online if the underlying technology of the Internet is understood. It is undeniably true that the Internet is a great medium for free expression, because of the way it has been built and designed. But this will not necessarily be the case in the future. The Internet has matured, and so have strategies and concepts to control, censor and regulate it. Hence we have to look carefully at where the architecture of the Internet is vulnerable to censorship and where parts of the Internet that make the 'control of communication flows' difficult are being rebuilt to regain control.

Control in the sense of regulating what is *on the Net* is by and large determined by the architecture of the Internet, as will be described, which in turn is made out of standards and protocols and written into the software code of our computer programs. It is built into the backbones, servers, routers and the computers we use to constitute the Internet. To understand then how regulation works on the Internet, it is important to examine how different levels of digital communications interact with each other, as Yochai Benkler (1998) has explored in his logical layers models.

I rather like to think that the Internet and the distribution of and access to digital content is composed like a pyramid. The foundation is made out of the basic infrastructure, let's call it the **network** level, which consists of telephone cables, optic fibre, satellites and so forth. The networks are owned by physically existing entities, the owners of the communications networks. These owners provide for the foundation of the digital pyramid, and can make decisions regarding the price of access, or to what extent they will not give certain parties access at all. Then there is a more obscure – because it is less visible – but nevertheless influential layer in the communications pyramid: **standards and protocols** such as the Transmission Control Protocol and the Internet Protocol (TCP/IP), which form the next level. They determine how data is routed across these networks. This characteristic aspect of Internet technology is particularly crucial for understanding communication regulation, because it decouples applications from the underlying transmissions, either via cable or satellites. The following level is made up of the **hardware**: the chips and hard drives constituting the computer**.** And finally there is the **software** and **applications** level. Applications such as Internet Explorer and Netscape determine how the information in Internet transactions is displayed and can be used.

[2] Christian Ahlert, 'The Party is Over', in Rötzer, Maresch (ed.) *Cyberhypes* (2001), p. 138-54.

The software, such as operating systems, determines, by and large, what one can do on the computer itself. Interaction between these layers is necessary, because for example standards and protocols determine how the different levels of information technology relate to each other. Therefore, they can be seen as a form of regulation, affecting for example the competitiveness of the market, but also the usability of software, intellectual property rights and a variety of public interest goals such as privacy, access, security and reliability.

So on each of these different layers of the communication pyramid decisions are being made and rules being built. Yet the reader might say – so what? – nothing of political or legal novelty has happened. Network owners were always, and still are, regulated by states, bi- and multilaterally. Within this regulatory framework their business decisions affected how we could communicate – for example if telephone calls became cheaper, or not. And standards were being used by industry to lock in consumers, dominate markets or to allow for network effects. So what is the difference? The difference lies in the simple fact: it's digital not analogue, it's global not national. The Internet is digital. On the Internet the rules that enable, or restrict, our capability to communicate, receive, distribute and share information are written into 'Code' (software code) as Lawrence Lessig (2000) has put it. And this software code not only makes our computers work, it also tells our computers how they work. And at different but interconnected levels in the computer environment rules can be written into this 'code'. While the current design of the Internet infrastructure makes file sharing possible and copying easy, all this could be different, and will also be written into the rules of that medium. It is therefore crucial to understand whether a new protocol for the Internet makes censorship easier, or whether it might add to the erosion of privacy when communicating online.

Digital control. The understanding of digital control becomes even more crucial because this year marks the first time in the history of communication that more digital than analogue communication devices will be sold. More pictures, books, music and personal communication will be digital and distributed online than ever before. And as more and more communication and other forms of social transactions are performed online and digitally an enquiry into the characteristics and extent to which 'Computer Code' controls communication, and how we should then control the producers of this Code, becomes important when discussing the freedom of speech and the media. Similarly, studying the effects of the Internet on society cannot be separated from how technological choices affect what we can do in the digital communication environment. So whereas freedom of expression was traditionally mainly constrained by governments using the law or brute force against publishers and journalists, and consequently protectionist measures focused on making better laws or protecting journalists, I will argue that decisions are now being made on the 'infrastructure' and other layers of the Internet regulatory framework which are becoming issues of concern.

At the same time we like to think that we are in control of the way we communicate via our computers – at least most of the time. But imagine somebody would change the software and hardware of your computer so that you could not 'copy' and 'paste' any more. And there are examples supporting this argument: Intel the biggest chipmaker in the world is working on a recently renamed product called 'Trusted Computing Platform Alliance'. Intel claims that this is 'a new computing platform for the next century that will provide improved trust in the PC platform.' The other big player in computing Microsoft wants to incorporate into future versions of Windows a software feature called Palladium. The underlying rationale is fairly simple: more and more content is being distributed digitally and hence there is a desire by industry to be able to better control the distribution of that content. Hence computers using these technologies will include a digital encryption and signature device. In this way the computer can decide, based on the users' authentication, what data you can access, how and to whom you can pass it on. There are plans to use the same software structure for e-mail and documents – resulting in e-mails that may disappear in two weeks, or documents that can only be read on the computers in one company. You will not be able to turn this new functionality off, as it will also be built into your hardware. Some of the proposals even contain plans to monitor your computer, and when you download an illegal file, it will either be remotely erased, or your computer will be turned off.

Yet, the idea that computer code may be emerging as a meaningful instrument of political will and control remains one of the most evocative and poorly understood propositions in the study of law, politics and technology as Tim Wu (2003) puts it. Nonetheless, the effects of computer code have made it difficult to ignore the fact that code can be used to produce regulatory effects in a similar way to laws; but, as I will argue, code is also entirely different. Therefore we should change the perspective. In spite of the fact that 'Code is Law' has been a powerful metaphor and, as William Mitchell claimed in his seminal book on the *City of Bits* that 'out there on the electronic frontier code is law', this is in fact not true. Law is enforced ex post. In the real world, law is never a perfect regulator. The legal system leaves room for interpretation of rules. There is not only room for error, but perhaps more importantly for the 'non-observance-of-broken-rules'. One might even argue that the worst human nightmare is to live in a perfectly controlled environment – an environment where rules cannot be broken, bent or simply ignored. It will only be judged after a rule has been broken whether this was a severe disobedience, or if it was, under the given circumstances, acceptable. Law depends on judgement, and judgement on interpretation. What might be acceptable in state x, for person y, on day z might not be fair in state k on the same day. So when it comes to the digital world the question is not whether rules should be built into the hardware and software of our computers, but whether we want perfectly enforced rules? In addition, we also have to ask whether we want those rules to be built by private companies. We certainly rely on rules to decide hard cases, but otherwise we have to be tolerant, or we would live in a society of constant struggle. David Weinberger recently asked in *Wired* magazine (2003): 'What do computers do best? Obey rules? What do they do worst? Allow latitude? Why? Because computers don't know when to look the other way.'

From no control to unaccountable control. To put the above into perspective we have to take a detour, because there is a paradox when it comes to debates about Internet regulation. In spite of the observations made above – that computers (and the Internet) can be potentially more perfectly controlled than analogue communication – in the early 1990s, as the Internet experienced dramatic growth, the prevailing consensus was that the Internet was immune from control. John Gilmore famously claimed that 'the Internet interprets censorship as failure and routes around it.' This led, as I will argue, to a rather perilous mixture of technological determinism and judicial pessimism – resulting in the myth that the Internet is inherently immune against restrictions on speech (communications) imposed by a single state. Yet, more recently, and paradoxically given the statement above, as different strategies have emerged to regulate Internet communication, the OSCE and the Council of Europe (2003) have been pressed to point out that the new forms of censorship being imposed on digital communications would be found ‘intolerable in other forms of media’ – at least in democratic societies. These new controls, according to the Council of Europe, are ‘incompatible with international norms on freedom of expression and information’.[3] In short, given that the Internet is apparently not immune from censorship, one must ask, why are the strategies being used to control communications on the Internet intolerable?

To examine how the debate evolved from ‘no control’ to what the OSCE and the Council call unacceptable forms of control, I would like to start by briefly exploring the logic and history of Internet content regulation. I will not discuss other policy objectives, regulatory aims and strategies – such as privacy or security – because they are different in effect as well as in scope. Thus, I do not attempt here to discuss how the Internet as a whole is regulated, because this is surely a much larger task. Rather, I want to address the attempts that are being made to control communication flows. The decentralized, global character of the Internet in combination with its nearly zero transaction costs for dissemination, duplication and distribution of content appeared to amount to a regulatory *mission impossible* for the single state. The response by democratic governments around the world was to actively promote a hands-off approach,[4] as happened in the United States during the Clinton administration, or to resort to a new self-regulatory paradigm. Whereas the US implicitly facilitated self-regulation, by saying it does not intend to regulate, the European Commission has explicitly resorted to the promotion of a self-regulatory framework for the Internet. Confusingly, it is also said that the Internet as a whole regulates itself, or operates like a self-governing entity.[5] Moreover, what is not explicitly regulated is in the policy debate often seen to be within the remit of self-regulation. So in fact there are at least four different meanings to the term self-regulation with regard to the Internet. Even though they are obviously all quite different in their objective, they seem to commonly omit that self-regulation does not equal no regulation. It seems rather to be the case that self-regulation often means, at the end of the day, to refer regulatory responsibility, implicitly or explicitly, to either something as utterly undefined as 'The Internet' or as matter of fact as private companies. Moreover, as will become clear later, this mystifying array of different forms of *self-regulation,* combined with the underlying assumption that only regulation by the actors who are *on the Internet* can make regulation work, results in misguided understanding of who regulates what and how on the Internet.

Resorting to intermediaries in a self-regulatory context. Nonetheless, at first glance self-regulation seems like a sensible response. It is undeniably true that traditional regulatory strategies – laws, multilateral treaties, court orders – in the face of the Internet seem to be difficult to implement and enforce. John Gilmore was indeed right to hint at this: it is not easy via those means to control the Net. In particular when one considers that on the Internet illegal content, ranging from pirated software, movies and music to child porn and hate speech is widely available, this calls for some form of regulation.[6] And if option A – top-down control – seems impossible, because there is a *regulatory need*, option B – self-regulation – seems to be better than

[3] Council of Europe, 'Declaration on Freedom of Communication on the Internet', 2003.

[4] The White House, A Framework for Global Electronic Commerce, 1.7.1997, (Washington, 1997a) <www.whitehouse.gov/WH/New/Commerce/read.html>.

[5] Christian Ahlert, 'Global Governance im WWW', *Blätter für deutsche und internationale Politik*, no. 5 (2000), p. 531-34.

[6] One can also argue that the almost ubiquitous availability of content creates the need to control the flow of information, where it is deemed either highly dangerous for society, although societies heavily disagree about this, or where it conflicts with traditional legal rules such as copyright.

no regulation at all. But there is a potential flaw in the argument: if the Internet could not be controlled by the state making new laws, monitoring the net, and enforcing those laws, how could self-regulation control it? Or can self-regulation just control it a little bit better, somewhat better, or even more perfectly than traditional law ever could?

Given the short elaboration of the *regulatory nature* of digital control above, it seems not surprising that, in practice 'single points of content control' have been identified. Governments, companies, and to a lesser extent individuals, have learned to react to the new technology and devised a number of control strategies. Even though there are others, I have decided to present one of the most prominent strategies.[7] Everyone who wants to publish, post and propagate content on the Internet needs the services of an Internet service provider (ISP). They make access to the Internet possible and they host most of the content available on the World Wide Web as they are most often also hosting providers. Consequently they have been identified as the ones in the Internet's communication chain to be made responsible for removing illegal and harmful materials from the Internet, ranging from copyright infringement, to cases of defamation, racist websites and pornographic content.

This (self)-regulatory strategy can be seen as a response to the architecture of the Internet and has subsequently given rise to strategies exploiting the technical means available to an ISP. Most prominently so-called *notice and takedown procedures* have been developed, which rely on the fact that ISPs have to 'take down' material once receiving a 'notice' that it may be unlawful or harmful. So far this seems to be a perfectly reasonable strategy: the Internet has created a regulatory demand and ISPs can meet that demand technically. But this is not the problem.

In the same way that there are good laws and bad laws, self-regulation can be crafted in ways which are not compatible with traditional political and legal standards. Under this regulatory regime the unique, technological architecture of the Internet is utilized to induce technological control mechanisms by private parties, without duly considering their powers, interests and basic political standards. Under this arrangement ISPs have to assume the role of judge, jury and enforcer at the same time. They not only have to make a judgement about whether a website is illegal, or not, on the merits of the evidence gathered by themselves (something that directly contravenes basic principles of due process), but they also have to behave as enforcing agents with executive powers. The difference to established forms of media regulation is the private nature of the regulator and the power, which is otherwise clearly separated between branches of government, accumulated in one institution. Despite such basic concerns, once an ISP removes content it does so with such brute technical force that it can be called, without much exaggeration, the cyber-equivalent to the death penalty. When an ISP acts it can destroy a business, censor a political campaign, or eliminate criticism of a corporation made by an anti-globalization NGO so effectively that it makes access to the website for everyone on the Internet impossible.[8] Traditional strategies of ex post censorship in the analogue world were more difficult to enforce: once a book was published, one could not easily know where it was, so it was harder to censor it effectively.

[7] See also Jonathan Zittrain, 'Internet Points of Control', The Berkman Center for Internet & Society, 2003 <http://cyber.law.harvard.edu/publications>.

[8] Needless to say, that the whole operation is a potentially very costly responsibility for a business based on selling Internet connectivity and webspace, limiting in turn its incentives to perform the above-mentioned functions appropriately.

The above paragraph is not meant to expand in great detail on the desirability of ISPs being used to police content under the current self-regulatory framework, which differs significantly in Europe and the US. Instead it is intended to highlight that a) the Internet is *regulatable*, b) that intermediaries (such as ISPs) can be used to effectively police digital content and c) that this is being done under an inappropriate self-regulatory strategy. Not only can the Internet be regulated, as this example shows, but it highlights a notable characteristic of digital networked technology. It can be used in a way to eradicate communication and content in an instant, simply by a keystroke. The downsides of this regulatory approach should be quite obvious. A private actor is arguably keen on minimizing the costs of regulation, and therefore uses the least possible resources to exercise control. Nevertheless, almost no accountability mechanisms, or criteria defining the rights and duties of the ISP, the complainant and the content provider exist. This leaves the procedure open to abuse and creates serious doubts about its fairness, transparency and accountability and also raises questions about the desirability, and ultimately the legitimacy of self-regulation in this area.

The absence of norms: Why we don't see the problem of Internet self-regulation. To gain a better understanding of why *self-regulation* is not only promoted by governments, but also goes beyond what is implied by this promotion, leaving how to regulate how we can communicate online to the discretion of private actors, and why structurally the means of doing so are not transparent to us, I would like to tell a short story. It illustrates the absence of established norms and standards, which would guide us in differentiating between acceptable and unacceptable forms of communication control.

The story comes from a different medium, but it is a useful illustration of our problem with Internet regulation – no matter whether this is called self-regulation, or not. Let's imagine that everybody living in Amsterdam was suddenly not allowed to make telephone calls to the UK. Anyone who tried dialling a number in the UK would get a busy signal. Nobody gave you an explanation about why calls from across the channel were banned. In my example, British Telecom simply decided, without giving a public statement, that calls coming from Amsterdam will be unanimously blocked, so they would not reach BT customers. I think the citizens of Amsterdam would be outraged, and rightly so.

This telephone blocking is fortunately just the product of my imagination. Unfortunately the next story is not, and it illustrates how companies, which serve as intermediaries between individual users and the worldwide Internet, can in effect restrict the freedom of speech on the Internet. Recently every user of Oxford University's e-mail system was blocked from sending e-mails to anybody with an AOL e-mail address. When you sent an e-mail to an AOL user, it simply came back, leaving the impression that the e-mail address was wrong. But it was not the address that was wrong, it was AOL who had decided to block any e-mail coming from Oxford.

And in contrast to my imagined example almost nobody was outraged because it appeared to be a technical mistake. At the same time, communication was effectively blocked in between Oxford and the AOL community of 20-something million Internet users. So what can we learn from this example? It illustrates how effectively those who control the infrastructure of the Net can control the way we communicate and what we are allowed to say. In my example a private party had received spam from an Oxford address and decided unilaterally to block and punish all Oxford users. This amounts to a form of private censorship that is not tolerable in other media. It was not transparent to the user, in fact it was invisible to the user, and therefore he or she could not hold AOL accountable. It also illustrates another, perhaps even more important point about the regulation of the Internet and digital media. Whereas for traditional media we have established a set of implicit and explicit norms, standards and values regarding what a newspaper editor, a telephone company or a broadcaster should, or should not, be allowed to do, this does not seem to apply yet to networked digital media. What the example further shows is that Internet service providers, by controlling an important part of the Internet's infrastructure, can not only block e-mail, but also filter websites and monitor traffic. They can see who is surfing where, when and for how long; they can also take-down websites so that they vanish from the Web. In short, through technology they can control and substantially limit our freedom, and it seems questionable if this is what is usually meant by self-regulation.

Towards a positive re-regulation of cyberspace. Why does all this matter? After all digital computers in 'normal use play a purely deductive role in that they follow explicit instructions in operating on data that are fed into them' writes the Encyclopaedia Britannica citing a definition from 1957. Not a lot, might then be the answer. Computers are still our servants. They still obey the set of rules they have been programmed with, even though some might think otherwise when their tax form vanishes, or their beloved computer gets a virus.

On the other hand much has changed since 1957. Computers now form a central part of everyday life and communication. Increasingly all sorts of transactions from banking to chatting with friends can be performed digitally and online. In contrast, previous analogue media were either confined to a *receiver sender modus* making only one-way delivery of content possible – think of the postal services, TV, books, or radio – or to symmetric one-to-one communication. Any communication over the telephone for instance requires the parties wanting to engage in a discussion to be present at the same time. Against this context the transformation of the computer from a rather sophisticated calculator to a worldwide connected communication medium marks a fundamental change in the affairs of human conduct.

The differences are numerous so I will mention just a few here. Via the telephone, or the radio individuals could not engage in global communication without significant cost. Being on the Internet almost everybody can become a publisher, or even a radio station. The convergence of previously separated forms of media into one global medium marks an unprecedented degree of amalgamation of communication forms. So not only the degree to which we use digital devices to communicate is new, but also the degree to which we can communicate digitally is unprecedented. What traditionally necessitated manual labour, can now be performed at a keystroke, or what required personal interaction is now transformed into digital interaction. Entire companies are being built that only exist virtually. Analogue media users could not share music files, swap movies or perhaps even vote without leaving their homes. In brief it is still hard to grasp to what extent the combined effect of 'digitization' and 'neticization' transforms businesses, politics and individual behaviour, even though one can guess that it is profound. But if that is so, it indeed seems rather odd that the making of rules for computers, which happens at different layers in the computer communication chain, is rarely seen as a question worthy of systematic examination.

So what does this tell us? Technological choices regulate the way we can communicate via the Internet, and these choices are currently being made – on a day to day basis by ISPs and for the long run by the computer industry. At different levels in the infrastructure choices will need to be made about who can control the way we communicate and to what extent. And the problem is not whether this will happen, or not. The problem is that these 'regulations' are by and large built without public debate and that these seemingly technical regulators are not held accountable. So the future of the freedom of the media online will rely on the insight that when it comes to the Internet and digital media 'seemingly narrow technical choices can have a broad and lasting impact on public policy and individual rights – more so even than traditional policy processes'. And these choices are choices about digital technology that can potentially regulate communication far more perfectly than was ever possible in analogue media technology.

At the same time these seemingly technical decisions are not being made within governments and international organizations, but in private bodies – such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), or the Intel-led Alliance for trusted computing – that set technical standards for the computers we use and the Internet. But those and other key standards bodies operate largely outside the public eye and with little input from public interest groups or policy-makers. So let me then conclude with a perhaps boring, but important, point. Technical systems incorporate 'political properties' and the code and standards design and implementation processes for the Internet are 'regulative mechanisms' which have to be examined in detail in order to understand their various and subtle impacts on the way we are able to communicate online.[9] If we want to make the right choices about the regulation of digital media, we will need to understand that 'technological choices matter' and even more so in the digital than in the analogue realm.

In this context, we should remember the regulatory response that the EC, and other states, are advocating: self-regulation. It is not the case that self-regulation in itself is wrong, or even a bad regulatory system. But we should ask how a system that is run, maintained and enforced by private companies is appropriate, measured against the potential effectiveness of control measures available to them? To what extent do we want private actors to be in control of communication in the digital world? Whereas self-regulation might be in some cases the right answer, in others it might not be, but it should always be modelled in a way that contains sufficient safeguards for the protection of freedom of expression online. Just because the current design of the Internet makes some forms of control difficult there is no reason to leave that control outside the public eye, in particular in the digital age where control can be potentially far more perfect than in the analogue world of books, public broadcasters and newspapers.

Acknowledgements:
The author is thankful to the participants of the OSCE's Amsterdam Conference on Freedom of the Media and the Internet for their inspiring comments on this contribution to the debate. I am also grateful to Gail Saliterman of the Stanhope Center for Communication Research and Monica Arino Gutierrez, currently at Columbia University, for their combined intellectual rigour from which this paper logically profited.

[9] See also Zoe Baird, 'Governing the Internet', *Foreign Affairs*, 81/6 (Nov./Dec.2002).

Bibliography:

Ahlert, Christian, ‘Global Governance im WWW’, *Blätter für deutsche und internationale Politik*, no. 5 (2000), pp. 531-34.

Ahlert, Christian, ‘The Party is Over’, in Rötzer, Maresch (ed.) *Cyberhypes* (2001), p. 138-54.

Baird, Zoe, ‘Governing the Internet’, *Foreign Affairs*, 81/6 (Nov./Dec.2002).

Baldwin, R. and Scott, **C. et al.** (eds.), *A Reader on Regulation. Oxford Readings in Socio-Legal Studies* (Oxford: Oxford University Press, 1998), chapter 1.

Benkler, Yoshai, ‘Communications Infrastructure Regulation and the Distribution of Control Over Content’, *Telecommunications Policy*, 22 (3) (1998), pp. 183-96.

Council of Europe, ‘Declaration on Freedom of Communication on the Internet’, 2003.

OSCE, ‘Amsterdam Recommendations on Freedom of the Media and the Internet’, 2003.

Frieden, Rob, ‘Does a Hierarchical Internet Necessitate Multilateral Intervention?’, 2001, at <www.ssrn.org>.

Gillet and Kapor, ‘Self-Governing Internet: Coordination by Design’, in Brian Kahin and James H. Keller (eds.), *Coordinating the Internet* (Cambridge, Massachusetts, 1997), pp. 3-38.

Johnson, David R. and Post, David G., ‘Law and Borders. The Rise of Law in Cyberspace’, 1996a, <www.cli.org/X0025_LBFIN.html>, 8.9.97.

Keohane, Robert O. and Nye, Joseph S., ‘Power and Interdependence in the Information Age’, *Foreign Affairs*, 77/5 (1998), p. 82

Lessig, Lawrence, *Code and Other Laws of Cyberspace* (New York, 1999).

Lessig, Lawrence, *The Future of Ideas* (Random House, 2001).

Majone, Giandomenico, ‘Cross-National Sources of Regulatory Policymaking in Europe and the United States’, *Journal of Public Policy*, 11 (1991).

Mueller, Milton, ‘ICANN and internet governance, sorting through the debris of self-regulation’, *info*, 1. Jg. no. 6 (1999).

Sclove, Richard E., *Democracy and Technology* (New York: Guilford, 1995).

Scott, et al. (eds.), *A Reader on Regulation. Oxford Readings in Socio-Legal Studies* (Oxford: Oxford University Press, 1998).

The White House, A Framework for Global Electronic Commerce, 1.7.1997, (Washington, 1997a) <www.whitehouse.gov/WH/New/Commerce/read.html>.

Wu, Tim, ‘When Code isn’t Law’, *Virgina Law Journal*, 89/4 (2003)

<http://faculty.virginia.edu/timwu/When%20Code%20isn’t%20Law.pdf>.

Zittrain, Jonathan, ‘Internet Points of Control’, The Berkman Center for Internet & Society, 2003 <http://cyber.law.harvard.edu/publications>.

Jonathan Zittrain and Benjamin Edelman

Documentation of Internet Filtering Worldwide

A variety of organizations, institutions, companies, and countries seek to restrict Internet access from within their premises and territories. For example, companies may seek to improve employee productivity by restricting access to leisure sites; libraries and schools may seek to avoid exposing children to sexually-explicit content, or be required to do so; countries may seek to control the information received by their citizens generally. Common among nearly all these applications is the public unavailability of the filtering lists – that, by the design of filtering systems, users cannot and do not know the set of specific sites blocked. In some cases users might ask for a specific site and be told of its unavailability due to filtering, but in other cases such unavailability may be conflated with unremarkable network blockages – a website might be unreachable for any number of reasons, and the failure to view it at a particular moment cannot reliably be attributed to active filtering.

In a series of articles, we have sought to document and analyse a large number of web pages blocked by various types of filtering regimes, as well as to track trends in these filtering systems. We can thus start to assemble a picture not of a single hypothetical World Wide Web comprising all pages currently served upon it, but rather a mosaic of webs as viewed from respective locations, each bearing its own limitations on access. As various countries, companies and other entities employ or consider employing filtering software, documentation of the specific details, successes, and in some instances flaws of existing filtering efforts may prove helpful.

The remainder of this article provides summaries of selected articles we have published on these and related subjects. A current index of our publications on these subjects is available at http://cyber.law.harvard.edu/filtering . This URL also includes our publications as to filtering in countries outside the OSCE's focus area, including in China and in Saudi Arabia.

Localized Google search result exclusions: google.de and google.fr

This text describes research Zittrain and Edelman jointly posted to http://cyber.law.harvard.edu/filtering/google in October 2002.

To help understand the sorts of pressures placed upon intermediaries like search engines and their respective reactions, we have checked for search result discrepancies between results from google.com versus those from google.fr and google.de. We conducted this search by using a list of several thousand sites known or likely to be controversial, most for their inclusion of white supremacy or related content, including one site to which we had been alerted that discrepancies existed. For each site, we then searched google.com, google.fr, and google.de to determine the number of pages reported indexed respectively. Many such sites seem to offer neo-Nazi, white supremacy, or other content objectionable or illegal in France and Germany, though other affected sites are more difficult to cleanly categorize.

The implication of these results – confirmed in our subsequent searches on google.com versus google.fr and .de for the terms at issue – is that the French and German versions of Google simply omit search results from the sites excluded from their respective versions of Google, and that this anecdotally appears to be because of pressure applied or perceived by the respective governments. Of the sites excluded from Google results in France and Germany, some contain content known to be controversial, but the exclusion of others is less obvious. In subsequent work, researcher Seth Finkelstein points out[1] that some of these names may have been transferred from one registrant to another, resulting in a significant change in the content available; however, Google may have failed to update its filtering list to reflect such transfers. Seth also notes that Google's filtering systems seem to fail to remove all pages that specify a port number (www4.stormfront.org:81 for example), suggesting that the filtering may be a relatively simple end-of-process add-on attached to the ordinary Google search logic.

We note that Internet users in France and Germany need not use google.fr or google.de. While Google's geolocation systems typically automatically offer these sites to users in the corresponding countries, users retain the option to use the ordinary English-language google.com site. As a result, filtering of Google's .fr and .de sites poses a less serious and more easily circumvented difficulty than would be the case were use of these country-specific sites mandatory in the corresponding countries.

In our testing, every site found to be removed from German google.de results (65 sites in total) was also removed from French google.fr results. A further 48 sites were removed only from google.fr results. However, we found no sites blocked only in German results but listed in France. In subsequent testing, we have further found that google.ch (Switzerland) exclusions seem to match results in France.

In addition to the search result exclusions described above, google.com and google.de/.fr may differ in other respects also. The authors have confirmed that the images.google.de

[1] <http://sethf.com/infothought/blog/archives/000053.html>

advanced image search form fails to offer the user the option to enable or disable SafeSearch (filtering of sexually explicit images), while the corresponding images.google.com page lets the user choose whether or not to invoke this filtering. Sources in Germany suggest that all google.de image searches are performed with SafeSearch engaged to filter images thought to be sexually explicit. We note, however, that images.google.fr's images search does offer the user a choice as to the inclusion of sexually explicit images. We further note a divergence in results on images.google.com versus the .de and .fr sites. However, the cache feature of google.de and .fr seems to continue to provide archives even of the websites excluded from these versions of Google.

Websites sharing IP addresses: prevalence and significance

This text describes research Benjamin Edelman posted to http://cyber.law.harvard.edu/people/edelman/ip-sharing in February 2003.

In a survey of all .COM, .NET, and .ORG domain names, more than 87 per cent of active domains are found to share their IP addresses (i.e. their web servers) with one or more additional domains, and more than two-thirds of active domain names share their addresses with 50 or more additional domains. While this IP sharing is typically transparent to ordinary users, it causes complications for those who seek to filter the Internet, and restrict users' ability to access certain controversial content on the basis of the IP address used to host that content. With so many sites sharing IP addresses, IP-based filtering efforts are bound to produce 'overblocking' – accidental and often unanticipated denial of access to websites that abide by the stated filtering rules.

IP sharing. Websites are hosted on web servers, computers running specialized software that distribute web content as requested. Each server typically has a single IP address, a unique numeric identifier assigned to no other computer on the entire Internet. (Those servers that use multiple IP addresses are for purposes of this document effectively multiple servers. This treatment is appropriate because its distinct IP addresses could be filtered separately and independently by those who seek to restrict access to web content.) Websites are typically associated with domain names – textual strings like 'yahoo.com' that are easier for users to remember than numeric IP addresses.

Under the initial version of the HTTP specification that defines the transfer of web content, web servers receive from web browsers only the name of the requested file, without any supplemental information as to the website hosting that file. 'Give me the file /index.html', a browser might say to a server; if the server happened to host multiple websites, each with a file of that name, the server could not know which file to provide. As a result, under the initial version of HTTP, each domain name with web content needed its own IP address. If a server was to host several websites, each with its own domain name, the server would need that many IP addresses, and it would provide the appropriate files by tracking which IP address was the recipient of which requests.

In principle as many as four billion IP addresses might be available, but in practice the number of usable addresses is significantly less, causing a potential shortage of IP addresses. While the number of websites (and associated domain names) remains small in relation to the number of IP addresses, allocating a dedicated IP address to each site is seen as wasteful, especially when hundreds or even thousands of websites can in many instances share a single web server. In addition, reconfiguring a web server to add additional IP addresses is a relatively complicated task – one that, on many operating systems, temporarily disables network connectivity and temporarily renders existing websites unreachable.

Combining these administrative difficulties with concern as to a possible shortage of IP addresses and a perceived need to be more conservative in IP address allocations, the Internet's technical community devised a means of reducing the number of IP addresses required to host web content. Under version 1.1 of the HTTP specification (section 5.1.2), many websites can share a single IP address without facing the file confusion problems described above. This is possible because when a HTTP 1.1 browser sends a request to a web server, its request bears the name not only of the requested file but also of the requested website – not just 'give me /index.html' but 'give me the /index.html file on the server http://www.yahoo.com'. While this configuration is known by a number of names, including 'virtual hosting' and 'name-based hosting', the remainder of this document calls it 'IP sharing'.

Internet filtering. Although IP sharing has become standard practice, widely supported by all recent web browsers and web servers, it nonetheless interacts unpredictably with certain efforts to filter the Internet. This section provides an overview of filtering systems and their technical design, necessary to understanding the effect of IP sharing on the accuracy and granularity of Internet filtering.

Since the rise of widespread Internet use, a number of governments, companies, and private citizens have expressed concern as to certain controversial content available on the Internet. In the United States, controversial content often consists of sexually-explicit images. In Europe, hate speech is often of greatest concern. In parts of Asia, political speech is sometimes targeted. Concerned parties sometimes seek to remove such content from the Internet altogether, but when content is hosted on a server in a distant country, jurisdictional issues make enforcement impractical. Accordingly, some governments and private parties have implemented filtering systems – intended to block controversial content before it arrives at a user's computer.

In certain countries, Internet connections are designed in a way that passes all communications through central facilities, directly facilitating centralized filtering. For example, Saudi Arabia has designed its network in precisely this way.[2] This centralized filtering design allows the use of proxy servers which can review all web requests and block access to sites deemed unacceptable. Proxy servers can be designed to filter at the level of specific websites – even when multiple websites share IP addresses, as described above – and can even block particular pages on sites that otherwise remain accessible.

However, proxy-based implementations are less practical in the US and in Europe, where networks tend to be decentralized, featuring a multitude of links between ISPs. In this network design, it is less clear where to put a central proxy server, for the network does not create any obvious central point of control. Huge traffic volumes also make proxy servers less practical; hundreds or thousands of proxy servers would be required to filter a large network without a degradation in performance, but so many servers would be costly and burdensome to install and maintain. Accordingly, when governments order filtering in the US, the most obvious approach – with lowest cost and

[2] See also the author's prior work documenting specific sites blocked in Saudi Arabia <http://cyber.law.harvard.edu/filtering/saudiarabia/>.

fastest implementation time – is to configure network infrastructure (typically, routers) to deny requests on the basis of the IP address of the remote website.

Within the framework of filtering on the basis of website IP address, it is problematic for many websites to share a single IP address. If filtering is to operate at the level of IP address, all websites sharing that IP address will necessarily be blocked even if only a single site (or portion of a site, i.e. a particular page) is specifically targeted for filtering. This problem is known to affect filtering in China and in Vietnam.[3] In 2002, the state of Pennsylvania passed a law[4] that requires ISPs to filter designated websites found to distribute child pornography; ISPs have responded by implementing blocks on the basis of website IP address[5], and Pennsylvania (and, for many affected ISPs, their entire US or North American networks) has thereby begun to use content filtering by IP address.

Some web servers host hundreds of thousands of websites, and thousands of servers each host thousands of websites. With so many sites hosted on large web servers, it is desirable to separate servers into categories reflecting their usage and the types of content they respectively offer. The author suggests a four-step spectrum ordered according to the amount of unique content available on each site:

1 **'Under Construction' pages.** Some large web servers offer only 'Under Construction' or similar content on each of their many sites. For example, the 970,412 websites on 209.67.50.203 all provide Register.com's 'Under Construction' web page, making this server the largest of .COM, .NET, and .ORG servers, when measured via the total number of distinct domains hosted.

2 **Domains for sale.** Some large web servers host 'domain for sale' or similar pages operated by their respective registrants.

These registrants use their domain names to report and promote the availability of their domain names. For example, 208.254.3.130 hosts 123,011 domain names registered by Buydomains.com.

3 **Forwarding and redirects.** Second, some large web servers provide solely redirects to web content hosted elsewhere. Redirection services allow Internet users to combine the benefits of existing or free web space (often at a school, university, or existing ISP, or at Geocities or a similar service) with the conciseness of a domain name. For example, 216.136.232.176 hosts 73,811 domains configured with Yahoo! Domain's forwarding service. Though users' actual web content is hosted elsewhere, inaccessibility or blockage of the forwarding server would render the content unreachable by its domain name.

4 **Actual substantive content.** These are actual websites offering full-fledged web pages. Servers hosting many tens of thousands of domain names tend to offer smaller websites (with one or a few pages), while servers with somewhat fewer sites (typically, hundreds) offer large sites with hundreds or thousands of pages each. For example, 216.21.229.199 hosts 82,290 small sites ranging from gutter installation to sports cards to weight loss services. 216.205.146.137 hosts 1,962 larger sites, ranging from carpet care to management consulting to non-profit research centres.

Heterogeneity of sites sharing IP addresses. The practical effect of IP sharing on Internet filtering efforts depends on the heterogeneity of sites sharing IP addresses. If all sites on a given

[3] See the author's prior research, Empirical Analysis of Internet Filtering in China <http://cyber.law.harvard.edu/filtering/china>.

[4] <http://www.cdt.org/speech/030200penn7330.pdf>

[5] <http://www.politechbot.com/docs/worldcom.pa.reply.092402.pdf>

IP address provide similar or related content, then filtering of that IP address is less likely to mistakenly block non-controversial content than if sites on that IP address provide diverse content.

Within the four-prong categorization identified above, servers in categories one and two tend to offer limited content that is highly homogeneous. However, servers in categories three and four feature a broad mixture of content. The author conducted a limited manual review of sites hosted on these latter categories, concluding that these servers typically host a wide mix of content without any substantive unifying theme. Analysis suggests, and prior experience confirms, that it is not atypical for a single web server to host a mixture of sites that are sexually explicit and sites that are not.

The results detailed above reflect that sharing of IP addresses is prevalent – used by 87.3 per cent of active COM, NET, and ORG websites. In addition, IP sharing is substantial: More than two-thirds of active COM, NET, and ORG websites share their respective web servers with 50 or more other websites.

At the same time, filtering by IP address is also prevalent and seems to be increasing in usage. Such filtering is already used in China and Vietnam, and the author's prior research[6] indicates that IP filtering is one filtering method used by many commercial filters installed in libraries and public schools. Finally, under a 2002 law[7], the Attorney General of Pennsylvania has recently begun to order ISPs doing business in that state to 'disable access' to designated sites found to offer child pornography; most ISPs receiving such orders reportedly use router-level filtering to disable access to the affected IP address, even though that IP's server might contain scores of additional websites and thousands of specific web pages without child pornography. Related work by the Center for

Democracy & Technology considers the Constitutional and policy implications of this law,[8] and CDT in September 2003 filed suit to challenge the Pennsylvania law at issue.

Both prior experience and the analysis in this research suggest that filtering on the basis of IP address is bound to lead to overblocking – unintentional filtering of sites not targeted by filter operators. This is so for at least two distinct reasons: First, those who set filtering criteria typically cannot know what other sites share a web server with a site they deem unacceptable or, indeed, whether any other sites share that web server. Inconvenient as it may be, the Internet's domain name system simply is not organized in a way that makes it easy to obtain this information. The author's methods of making this determination are novel and, to the best of his knowledge, unique; filtering staff, be they in China or in Pennsylvania, are unlikely to have access to this information. Second, even if filtering staff knew what other content shared an IP address with controversial content, their technologically-imposed restriction to IP-based filtering means that a decision to block the targeted content *requires* blocking the other content on that IP address. Recognizing this problem, filtering efforts in China seem to be moving from IP-based filtering towards URL-based filtering. However, as discussed above, sophisticated filtering systems are particularly difficult to implement in a complex network design like that in the United States; Worldcom recently told the Pennsylvania Attorney General's Office that 'it is not technically feasible ... to block a site based on its URL.'

[6] <http://cyber.law.harvard.edu/people/edelman/mul-v-us>

[7] <http://www.cdt.org/speech/030200penn7330.pdf>

[8] <http://www.cdt.org/press/030220press.html>

Notwithstanding the overbroad blocking associated with IP-based filtering, those who dislike efforts at Internet filtering may find more focused filtering even more problematic. As the author describes in a recent op-ed in the *South China Morning Post*,[9] ‘These new filtering abilities alter the balance between ... censors and users. ... [T]raditional filtering methods were bound to provoke outrage since they led to over-blocking of popular websites. But ... more focused blocking may not elicit indignation or even notice. “China blocks 100 dissident websites” is a far less incendiary headline than “China blocks one million blogs.”’

Beyond their implications for router-based filtering, shared IP addresses can also present difficulties for commercial Internet filtering applications. While commercial proxy implementations are in principle capable of restricting access in a way that properly takes account of the many websites that may share a single IP address, extensive casual reports and the author’s prior research both reflect that some filters nonetheless fail to do so. This may reflect design errors, cost-cutting measures, or attempts to block all sources of sexually-explicit content even at the expense of blocking non-pornographic sites.

[9] <http://cyber.law.harvard.edu/people/edelman/pubs/scmp-012603>

Hans J. Kleinsteuber

The Digital Age: New Challenges after Three Hundred Years of Mass Media Experience

When Freimut Duve made his introductory statement, he defined himself as a Stone Age man in terms of the Internet. If you look at me, I am perhaps from the Copper Age. You should take this into consideration when I emphasize the point that our attitudes and behaviour in terms of media and freedom of information are very much still shaped by roughly three hundred years of mass media experiences with patterns that are totally different from what the digital age offers.

What I would like to emphasize is the following. The majority of media consumers are used to technologies that are one-dimensional, mass oriented, passive and based on a media monologue. The Internet offers totally new possibilities. Communication can be bidirectional, it can be individual or it can be peer-to-peer, it can be active or interactive and it allows dialogues. But the question is, How is this really handled in a real world where, for example, global media industries have been established or where governments have an interest in controlling political communication? What we can now observe is that features of the entertainment or fun industry are moving into the Internet; that things like entertainment in television, or marketing and advertising are becoming increasingly important; and that the potential of the Internet to create new spheres of information, to create public spheres where citizens can communicate with each other is not really being used.

So my question is: How does the Internet contribute to the development of the media landscape? If you look at the technologies of media, I think the most important application today is streaming technology, representing the digital convergence of old and new media that offers news portals including text, animated graphics, radio, television and even interactive features like instant referendum or sending back a letter to the editor or journalist. But this is just the potential of this technology. Before we go into that in depth, let's quickly see how media developed before the age of digitalization.

Here in Amsterdam is the place where the European institution – and there wasn't anything like this outside of Europe – of freedom of information started. Freedom of the press, freedom of the media began here even before it came to London and certainly much earlier than in other places in Europe. The reaction of the State at that time to this bourgeois power of creating public spheres was, of course, open censorship and this tradition of censorship still continues in non-democratic States. In a second stage of development open censorship has more or less vanished, due to the relationship between State and media in the broadcasting age. Again, we established a European tradition, the tradition of public service broadcasting, which is unique to our continent. But then another model, the commercial broadcasting model, was developed in the United States in the 1920s and internationalized in the 1980s. It moved over to Europe and if we talk about regulation, and this will be a central theme of the conference, we should keep in mind that regulation is an American experience. It is even mentioned in the American Constitution and it reflects the adoption of American models of organizing broadcasting media. However, if we transfer it into a new age of the Internet, we will see that it does not work because it reflects experiences of a more or less bygone age.

Let us now transfer our attention to the Internet. I think that it has been very clearly presented that any form of censorship or filtering does not work well in this field. The question is how to regulate problems of the Internet in the future – child pornography for example. I think the only model that we can offer, and I say this as a political scientist, is what we call global governance, which is a model that was developed around the United Nations conferences on environment, women, or health. There will be another UN conference in 2005 in Tunis on the Information Society. Global governance just means that the old state action does not work any more. Instead, we need some form of round table where government representatives, including the EU of course, people from industry and – very important – NGOs, representatives of an emerging world civil society, sit together, see where they have common interests and then follow a minimum strategy where they can then introduce measures jointly that might help in the worst fields where we need some global regulation. These global governance processes may not be democratic, even though I think that they may well be more legitimate than traditional processes in international policies. Yet, again, the Internet offers possibilities to organize elections as the example of The Internet Corporation for Assigned Names and Numbers (ICANN) shows. There we have role models about how to democratize these governance processes in the future and I think this is very necessary.

If I look at the global processes around the Internet at the current time, I see a kind of world struggle between those who support open and non-discriminatory architectures of the Internet and others who are trying to kind of privatize the Net – the software, the hardware, whatever – for their personal and usually economic interests. It seems very clear that the industries that now want to control the Internet are moving into the hardware field. They are trying to create chips that they control which might lead to a new form of censorship. This would not be state but industry censorship. There I see a clear conflict between the United States and Europe, for example in the field of software: Microsoft versus Linux, and certainly we should do everything to keep the development open.

In the United States, Microsoft, the world's largest software producer, started an alliance with AOL a few weeks ago. It would seem to me that they are jointly trying to introduce a system of Internet control that uses whatever technology is suitable. I think it will be predominantly hardware technology, trusted computing etc., which might in fact mean censorship. We should be very aware of this.

The US Digital Millennium Copyright Act and the European reactions to it – the Copyright Directive is currently under consideration in the European Parliament – were also mentioned. Again, I am very concerned about this process. In the United States, copyright law is already used to limit the free use of Internet material. Amazon.com, for example, successfully stopped all competitors from using a one-stop shopping software so that Amazon can, like Microsoft, create a de facto monopoly in a certain field. Or another example: recently an American law was passed that extends copyright protection for another twenty years. The law is called the Disney Law because it was lobbied for by the Disney Company in order to delay Mickey Mouse's entry into the public domain.

Let me finish with a few words on the opportunities that the Internet provides for journalism. Of course, online journalism is a new feature. You can read newspapers all over the world. Journalists have new sources for research and investigation, which is quite fascinating. We have new types of news portals, and much more. On the other hand, especially in the field of journalism, we also discussed the death of traditional media reporting simply because the Internet allows direct access to information for anybody, so you may bypass the journalist or the professional reporter, and the job may die out. There are even examples like Google News, which I would urge you to look at. Google now has a news portal and it works without a single journalist. They have their machines continuously monitoring all the English-language news portals of the world – and there are several thousands of these. Then they use their statistical parameters and the news features that are most often mentioned on those home pages are also the top stories in Google News. It is a parasite system, but it is still very interesting to see.

Still, with all these problems, I think that journalists become more important because of the information overflow and the unreliability of the Internet, and serve to protect against rumours and fakes. There will certainly be an increasing demand for navigation and selection and for this you need a new brand of professional media producer that, of course, requires different education from the old brand. Also the Internet offers an incredible variety of alternative sources of information – information that was previously issued in leaflets, radio stations, or news bulletins. During the Iraq War the mainstream media in the United States more or less sang the song of patriotism with very few exceptions. But if you went on Google and just wrote 'Iraq War' you would have been linked to dozens of home pages that offered the other stories, the non-reported facts or the number of dead bodies, or you would even have been linked to people in Iraq who were writing their war logs and giving their personal impression of what was happening during this war. The chance to have a counter public sphere, therefore, very much increases with the Internet, as does the opportunity for citizens, non-professionals, to become newsmakers – at least in extreme situations.

One last element that I would like to emphasize, which has to do with my activities with *Deutsche Welle*, is that I think that the technical side of the Internet and the quality of offering dialogues should also be transferred into a journalism of dialogue. In fact, the Internet offers incredible chances to connect cultures that are different in history, languages and experiences. It can even connect people in countries at war in a new way. I very much propose portals or websites that offer information from other parts of the world. Take for example the Arab world. We have lots of English-language information that has been discontinuously produced in the Arab world – radio, television programmes, newspapers that all offer news in English. If this were to be selected, sorted out, commented on and presented to us we would gain a much better image of the Arab world. The Internet also increasingly offers translating machines. Arab friends have told me that their language is too beautiful ever to be translated by a machine. But at least it is already possible to obtain raw translations from other cultures where we have no language access. Google offers this and I think that in a few years you should be able to read Arabic, or even Chinese or Japanese, newspapers on your computer. There are prospects for building bridges between cultures which deserve serious consideration. Again, here we have to develop new models so that the professional media producers, the journalists, are really able to handle these potentials of the Internet. Then we will have no problem in the process of the transfer of old media into new media and we will have the chance to take people who are, in their vast majority, still socialized in their old media, into the area of new media where all the qualities of the digitalized age can be truly fulfilled.

This article is adapted from a transcript of Mr. Kleinsteuber's speech held at the Conference on Freedom of the Media and the Internet in Amsterdam, 13 and 14 June 2003 organized by the OSCE Representative on Freedom of the Media.

Alberto Escudero-Pascual

Freedom of Information Builds Up in an Open and Affordable Network Infrastructure

The Organization for Security and Co-operation in Europe (OSCE) includes in the Helsinki Final Act of 1975 a set of guiding principles between participating States relating to Freedom of Information.[1] In the Act, the participating States commit to respect human rights and fundamental freedoms, including the freedom of thought, conscience, religion or belief, for all without distinction as to race, sex, language or religion.

As part of the Helsinki Final Act and followed later by different agreements in summits and meetings, the participating States made their aim to facilitate the freer and wider dissemination of information of all kinds and work towards the improvement of circulation of oral, printed, filmed and broadcasted information.

The work of the OSCE's Representative on Freedom of the Media focuses on specific cases of violation of freedom of expression and identifying problems that are characteristic of more than one State, such as, for example, censorship.

For historical reasons the work carried out by the OSCE has concentrated on the improvement of working conditions for journalists and traditional media like radio and television. But, with the growth of the Internet as a set of interconnected transport media and services, a new space for the dissemination of information is also developing. At the same time that traditional

[1] Freedom of Expression, Free Flow of Information, Freedom of the Media, Helsinki Final Act, 1975 <http://www.osce.org/fom/documents/files/commitments.pdf>.

media need to adapt to the challenges of a more decentralized technology, traditional approaches to combat censorship and promote freedom of information should also be reconsidered.

The Internet, which is commonly described simply as ‘a network of networks which transmit messages to one another using a common set of communications protocols’, has, among others, the property of being designed based on an ‘open architecture’ model. In the Internet the content (applications) is separated from the transport medium via a logical layer (TCP/IP). By contrast with traditional broadcasting media, the content delivery is completely dissociated from a broadcasting schedule and applications work independently of the transport media.

What seems to be a simple property in a technical design leads to a set of completely new scenarios.[2] Traditionally, by controlling (licensing) the use of a certain transport medium, controls were applied to the content. For example, radio stations or newspapers were required to obtain licences to broadcast a certain type of content and this could be monitored closely as it was broadcasted geographically at a certain time.

As a result of this transformation, the aim is to apply similar controls to the ‘transport media’ that are attached to any Internet gateway. For example, currently it is a common practice among telecommunication carriers to *lock* their customers to a given service as a requirement for obtaining access to a certain transport medium or some governments only provide Internet licences to service providers that do not host certain information.

The way that the Internet has been designed and deployed over the years challenges the traditional mechanisms that enabled control over content. The dissociation between transport media and content or the possibility of sending very different kinds of messages once having access to a transport medium make the Internet the most powerful communication tool today.

In countries where the transport media are under the control of a single governmental telecommunications operator, the physical transport media linked to an Internet gateway is a simple mechanism to control content. Based on the arguments presented before, we conclude that: 'full and affordable access to the "network" infrastructure (i.e. an Internet gateway) is a fundamental requirement to ensure freedom of information.'

In recent years a new technology, known as Wireless LAN, has enabled new actors (other than the national telecommunications operators) to deploy network infrastructure in metropolitan and rural areas.[3]

The following section describes some of the relevant aspects of Wireless LAN and reflects on the risks and opportunities of this new emerging technology. Rather than focusing on technological aspects, I will discuss how a new generation of open wireless standards can bring the Internet's open architecture to the wireless world.

Infrastructure based on IEEE 802.11 (Wireless LAN). One of the roles of the Institute of Electrical and Electronics Engineers (IEEE) is to promote industry standards. Participation in the IEEE standardization processes is open to any individual, independent of their industrial affiliation. The aim of the IEEE Standards is to represent a broad 'consensus' between various industry vendors and academics about how to implement different technical solutions. One of the motivations behind open standards is to reduce production costs by anticipating a wide, mass adoption of a certain technology while guaranteeing interoperability between different vendors.

[2] Chris Dibona, Mark Stone and Sam Ockman (eds.), *Open Sources: Voices from the Open Source Revolution* (O'Reilly & Associates, 1999).

[3] The IEEE P80211, The working group for Wireless LAN (Local Area Networks) <http://grouper.ieee.org/groups/802/11/>.

In 1997 the IEEE approved the first of a family of Wireless Local Area Network (Wireless LAN) standards. The first standard, IEEE 802.11, was soon followed by another IEEE standard called 802.11b in 1999. In order to guarantee interoperability between different implementations of the IEEE standard 802.11 a new organization called Wireless Fidelity (Wi-Fi) was also launched.

The IEEE Standard 802.11b was designed to operate in an indoor environment and to deliver a maximum of 11 Mbps using a technique called Direct Sequence Spread Spectrum (DSSS). The standard operates in 2.4 Ghz, in a frequency range that is normally allocated for the experimental Industrial, Scientific and Medical (ISM) radio band. The ISM Band is often unlicensed which means that a licence from the national government is not required to operate the radio equipment under certain power restrictions.

Although it was initially conceived as a short range, low power wireless technology for indoor use, it took very little time to see WLAN-based products in point-to-point (PtP) and point-to-multipoint (PtMP) outdoor solutions in both metropolitan area networks (MAN) and rural areas.

The possibility of using Wi-Fi to carry backbone Internet traffic, including data and voice, at a very low cost compared to the existing traditional Telecom equipment, drove vendors and users to find innovative approaches to overcome the IEEE 802.11b problems in outdoor environments. In a very short time, different vendors have already added extensions to the protocol to overcome the lack of performance in particular scenarios (e.g. polling extensions for multipoint solutions with the presence of hidden nodes, enhanced quality of service for voice over IP, etc.).

Wi-Fi-based solutions are spreading in the same way that happened with the revolution of open standards and the personal computer some twenty years ago. The truth is that while

Wi-Fi is far from being the best radio technology for long distance point-to-multipoint radio links, it represents for radio what open architecture represents for the personal computer. The reasons for the rapid growth of IEEE 802.11b as part of the basic data infrastructure in both developed and developing countries are as follows: the low cost of radio equipment due to its mass production, the possibility of easy integration with personal computers and operative systems, the existence of a certified interoperability between vendors (Wi-Fi) or the possibility of finding a very favourable regulatory framework in comparison with other radio technologies and related services.

In April 2002, another IEEE standard called 802.16 was approved. It focuses on broadband wireless access in metropolitan area networks (WirelessMAN).[4] The new standard is expected to bring low cost and more bandwidth efficient products for broadband outdoor wireless access in the next years. Time will show what will be the final role of IEEE 802.11b in indoor and outdoor environments, but what we cannot deny are the benefits and opportunities that it provides today.

For less than 2,000 USD it is possible to link two villages situated 10 kilometres away from each other and provide both data and voice services. This means that Wi-Fi is not only bringing new technical opportunities at a very low cost but it is also challenging the traditional telecommunication markets and their regulators.

Infrastructure investment generally consists of large capital-intensive projects that provide the backbone of the distribution system for the rest of the economy. Usually this includes roads, bridges, highways and airports that support the transportation of people but also the optical fibres and

[4] The IEEE P80216, The working group for Wireless MAN (Metropolitan Area Networks) <http://grouper.ieee.org/groups/802/16/>.

other communication equipment. There is a considerable risk of underestimating the need to invest in a long-cycled public fixed network infrastructure by trusting the private sector to develop its infrastructure by using short term solutions with bandwidth constraints as wireless links. This applies to many metropolitan and rural areas in developing countries where the new Internet service providers use technologies like Wireless LAN as a local loop, which hinders investments in the fixed infrastructure.

The benefits of market or user-driven wireless infrastructures like Wireless LAN should not undermine the government's role in investing, regulating and maintaining a country's infrastructure.

Summary. The open architecture of the Internet challenges the traditional mechanisms of control over content and communicating parties. The strong dissociation between the transport media and any given content has made the Internet a very powerful communication tool and has also reinforced the importance of having full operational access to an Internet gateway.

In the case of the Internet, the first effective mechanism of censorship before any other is to simply restrict access to physical transport media.

New emerging technologies, like Wireless LAN (IEEE 802.11), enable deployment alternatives to the monopoly of network infrastructure. Wireless LAN, while not being designed for outdoor use, has played a very important role in the decentralization of network infrastructure in both developed and developing countries.

Open wireless standards are not only providing new technical opportunities at a very low cost but also bringing the Internet model to an area that was restricted to traditional telecommunication operators. It is still uncertain if the growth of private investment in wireless infrastructure will slow down even more the required structural investments in fixed backbone networks.

In any case, keeping the network infrastructure open and affordable are necessary conditions to facilitate the freer and wider dissemination of all kinds of information.

How to ensure Freedom of the Media on the Internet in the OSCE region?

Sjoera Nas

The Future of Freedom of Expression Online: Why ISP Self-Regulation is a Bad Idea

Governments struggling with the abundance and speed of freedom of expression online have long cast flirting looks at service providers as the next best thing to central regulation. But most providers were not very keen on acting as policemen and refused to voluntarily accept liability for the content of their customers. Through the E-Commerce Directive governments have forced liability on ISPs anyway, hidden under a black veil of 'self-regulation'.

But what does such self-regulation entail? Let's take a look at the daily practice of Internet service providers. For obvious PR reasons, most providers don't publish statistics about takedown, but from my personal experience within XS4ALL I can provide some insights. XS4ALL, founded in 1993, was the first provider in the Netherlands to cater for the consumer market. Currently, it provides to both the consumer and the business market and serves about a 150,000 customers, most of which have a broadband ADSL-connection.

In the first six months of 2003, XS4ALL received a total of 750 serious copyright-related complaints, that is 31 complaints per week, or four and a half per day. The majority of these complaints are about straightforward infringements of copyright, and can be dealt with pretty easily. The remaining 10 per cent of the complaints however, demand a huge amount of time and attention from highly skilled legal professionals.

The majority of complaints originate from a few international right holders, like the MPAA, IDSA, Mediaforce, Microsoft and BSA, the Business Software Alliance. The Motion Picture Association of America represents most of the Hollywood film industry, while the Interactive Digital Software Association represents the international video and computer games industry. Another very active plaintiff is Mediaforce.

From January till July of this year XS4ALL received 265 complaints from the Motion Picture Association, 143 from the Interactive Digital Software Association, 110 from Mediaforce and 47 from the Business Software Alliance. On top of that, one specific right holder (Visualware) generated 125 complaints. So, out of the total 750 complaints, 681 stem from four large right holders, which amounts to about 90 per cent. Most of these complaints are about FTP servers, usually on ADSL-nodes, about Usenet postings and sometimes about websites and home pages.

In general, the complaints from the representative bodies of right holders are clear-cut and don't require much research. XS4ALL immediately forwards the complaint to the customer. Usually, the customer voluntarily removes or retracts the illegal content. In those cases, XS4ALL administers a virtual 'yellow card' to the customer; in case of a second wilful copyright violation that can be followed by a 'red card', i.e. disconnection. That seldom happens. Warnings are taken very seriously, since most customers are bandwidth junkies. Besides, the costs of disconnection and provider switch of a broadband subscription are very high.

Sometimes, copyright organizations complain about customers directly exchanging software amongst each other via IRC (chat-networks), or via peer-to-peer networks. Since providers have no way of verifying, tracing or influencing these alleged infringements, these complaints are usually ignored. As far as I know, Dutch providers have not been forced to hand-over personal data about customers to right holders, as was the case in Denmark and the USA, but the central collecting society is currently building up pressure, threatening to sue both providers and individual uploaders.

Back to the practice of dealing with complaints. Since mid-1999 XS4ALL has had a procedure for complaints about illegal content. This involves a questionnaire that has since become the standard model for all Dutch ISPs. The questionnaire enables right holders to describe their complaint clearly and precisely and protects the ISP against liability in case of wrongful take-down.

Most of the major right holders don't bother to fill in the questionnaire. Their complaints are largely generated automatically, and their reply-addresses often don't work, or answers are ignored. Often these complaints refer to North American legislation, the Digital Millennium Copyright Act, without any reference to the European E-Commerce Directive. Still, if such a complaint is serious and can be verified easily, most providers kindly act as postman, and forward the complaint to the customer. In most of these cases, the customer voluntarily removes the material. Life becomes difficult when the customer either doesn't reply at all, or replies with a sensible answer, creating reasonable doubt about the complaint. That only happens in 10 per cent of the cases, and those make life very difficult for ISPs. In those cases, the right holder is asked to complete the questionnaire. After that, the ISP has to make two difficult judgements. First of all, to determine the seriousness and validity of the complaint, and secondly to judge the quality of the response of the customer, when given.

The questionnaire to deal with complaints came out of a lengthy and very influential court case about the copyrights of the Church of Scientology. In 1995, XS4ALL servers were formally seized by a bailiff, assisted by a representative from

Scientology, for hosting the Fishman Affidavit on the home page of a customer. This affidavit, a court testimony from a former member, contained many quotes from documents that the church wanted to keep secret. Another customer of XS4ALL, Karin Spaink, put the document on her home page. When Scientology threatened to sue her and XS4ALL, many other people put mirrors on their home pages. In interim injunction proceedings in 1996, the court of The Hague declared all Scientology's claims against XS4ALL, Karin Spaink and 20 other defendants to be unfounded. Scientology appealed, but lost once again in 1999. However, this 1999 decision included a separate declaratory judgement stating that providers can be held liable if three conditions are met:

- first, the provider is notified;
- secondly, the notification leaves no reasonable doubt about the infringement of (copy-)rights;
- and thirdly, the provider does not take down or block the material.

The court at The Hague also ruled that providers might be held liable for hyperlinks and have to hand over the names and addresses of their customers under certain circumstances.

Again Scientology appealed. Early in September 2003, eight years after the initial complaint, the Appellate Court of The Hague quashed the previous ruling and ruled against Scientology on all points in a surprisingly strong-worded opinion. In this case, the court said, freedom of opinion should prevail over the enforcement of copyright. 'The (...) texts show that, in their doctrine and their organisation, Scientology et al. do not hesitate to overthrow democratic values. From the texts it also follows that one of the objects of the non-disclosure of the contents of OT II and OT III ... is to thwart discussion of the doctrine and practices of the Scientology organisation.'

The Appellate Court doesn't offer any further help with the liability regime, leaving it up to providers once more to decide about the freedom of expression online.

Another landmark case that shapes the debate in Europe about liability and freedom of expression online is the *Radikal* case. Last year, XS4ALL was sued by the German national railway company over *Radikal*, a German magazine containing a manual about how to sabotage railways. The manual had been online since 1996. XS4ALL refused to voluntarily comply with both demands: neither to take down the material nor to hand over the personal data of the customer. In preliminary proceedings instituted by Deutsche Bahn, XS4ALL was nevertheless ordered to do so. XS4ALL appealed but lost. The district court only confirmed the judgement that in this specific case, the illegality was painstakingly clear and the provider should have immediately recognized that. According to this ruling, a provider can only ask for more detailed information (for example with the questionnaire) '(...) in the case of information which is allegedly offensive or allegedly breaches copyright (...).'

This assumption of obviousness doesn't help providers in distinguishing between legal and illegal content. Nor does the E-Commerce Directive provide any clear guidelines. In Article 14, the provider is exempted from liability in case of hosting if the ISP has no actual knowledge of 'apparent' illegal content, or if it does, acts expeditiously to remove the content.

What expeditious is, or how 'apparent' can be construed in a universally understandable and predictable way, is left open to the market. Left to this self-regulation, providers don't see much space to refuse requests to take down offensive, damaging or illegal content.

Based on my personal experience, not just with Scientology and *Radikal*, but with many other difficult complaints, I am convinced that the only way to protect freedom of expression online is to refer these decisions to courts. In case of doubt, let a judge decide. As burdensome for the legal system as that might sound, I'm convinced that in practice it would only lead to a very limited number of cases. In 90 per cent of the cases, the complaint stems from a major right holder, and can easily be verified by the provider. In those cases, more than 95 per cent of the customers voluntarily remove or retract the material once they are 'caught in the act'. The remaining complaints from the major right holders are sometimes just wrong, based on a typo or other bad research by the right holders, or unverifiable, for example about peer-to-peer exchanges. It is the 10 per cent of 'other' complaints that deserve close attention. Again, in 90 per cent of those cases customers remove the material voluntarily. What's left, is crucial for the freedom of expression. In my opinion, providers should be protected against any liability for keeping those materials online while courts decide.

The European Commission recognized the difficulties in dealing with the liability regime and organized a two-year research programme called Rightswatch. Rightswatch was an attempt to work out a European self-regulatory framework for copyright infringement on the Internet, with representatives from the copyright industry, from providers and from Internet users. Europe was divided into Southern Europe, the UK and Ireland, and Northern Europe. I participated in the Northern European discussions, and the conclusion of our group was that it was a good idea to create a permanent intermediary between providers and right holders, a body that could transfer complaints to the right address, provide statistics about the type and number of complaints, and decide whether a complaint was difficult enough to be dealt with by a judge.

The Southern European working-group came up with completely different conclusions, very much resembling the procedure in the US of notice and immediate take-down. This procedure can easily be abused to stifle freedom of speech. During one of the general Rightswatch meetings, Yahoo legal representative Greg Wren referred to it as ‘shoot first, ask questions later’. In the English/Irish working-group, no agreement could be reached. Users and providers insisted on a legal underpinning for any notice and take-down regime, after having had bad experiences with a self-regulatory hotline. Right holders were not keen on the hotline either, because according to them, it caused unnecessary delay in removing infringing materials.

In the Netherlands the call from both users and providers for a national body received a warm welcome. Earlier this year, the Ministry of Justice set up a committee with representatives from all parties involved. Currently, we are working on the construction of a central body for complaints about illegal content, similar to the existing hotlines for child pornography and discrimination. This Central Body should be able to discern straightforward complaints that deserve immediate action from the ISP and more complex complaints that deserve a correspondence with the ISP customer, and in case of a serious reply, deserve a court ruling.

The biggest issue to be solved remains the handing over of the customer identity. Even after the disappointing ruling in the *Radikal* case, Dutch providers do not voluntarily hand over customer details to plaintiffs, in accordance with privacy legislation. Right holders, however, are insisting on both take-down and handing over of customer details. Again, it is my personal conviction that only a judge can weigh between the customers right to privacy and the right holders wish to know

the identity of a person infringing on their copyrights.
In practice, the E-Commerce Directive has not brought much clarity in the responsibility of Internet providers. Many civil rights activists and providers have argued for a more formal approach, where only an order from a judge would constitute actual knowledge of infringing material.

Attempts to develop a standardized notice and take-down (NTD) procedure have failed miserably so far. The parties involved – citizens, service providers and copyright holders – have been unable to achieve agreement about the exact meaning of terms like ‘expeditiously’ and ‘apparently illegal’. Providers are not equipped with special moral values that make them a good replacement for the judiciary. Quite the opposite, in fact. Guided by marketeers and stock-value, most providers will avoid risk and rapidly take down any material that might offend anybody; without any right of reply or access to appeal for the customer, without any obligation to the public to justify their acts or publish yearly statistics.

‘Any self-regulatory regime within the context of NTD procedures cannot be truly effective without some form of legislative underpinning’, was the official conclusion of Rightswatch. However, the European Commission has made it clear that the E-Commerce Directive will not receive a review of its text until, at the earliest, 2006. This leaves it up to national governments to choose the level of protection for the freedom of expression. Hopefully, the Dutch can set a good example.

Ian Hosein

On International Policy Dynamics: Challenges for Civil Society

Our conventional understandings of policy and our abilities to affect change in national discourses tend to rely on a single-state deliberative process. Increasingly, however, the dynamics of policy-making are changing alongside other phenomena such as transnational communications networks, globalization of social and economic activities, and international and sub-state threats of crime and terrorism.

We need to study the dynamics of modern policy development, particularly focusing on *policy laundering*, *modelling*, and *forum shifting*, while attempting to engage these policies and their proponents. Policy laundering is a practice where policy-makers make use of other jurisdictions to further their goals, and in so doing they circumvent national deliberative processes. Modelling occurs when governments, overtly through calls of harmonization or subtly through quiet influence and translating of concepts, shape their laws based on laws developed in other jurisdictions. Forum shifting occurs when actors pursue rules in intergovernmental organizations (IGOs) that suit their purposes and interests, and when opposition and challenges arise, shift to other IGOs or agreement-structures.

There are two implications of these new policy dynamics. First, national consultative processes disappear or are weakened, as important policy decisions take place outside of democratic institutions. For example, frequent calls for ‘harmonization’ through treaty ratification and perceived international obligations inhibit the likelihood and effectiveness of traditional national deliberation, while these treaties are negotiated in closed environments. And second, policies are shaped by foreign interests and foreign processes. As an example, the European Union privacy practices are under review because of the influence of recent US laws on travel documentation and procedures.

Bring in the IGOs

The activity of intergovernmental organizations appears, in many cases, to lead the way in developing policy in the 'age of globalization'. If our policy challenges are international in nature, and the infrastructure of trade and communications is also global, then, as the logic goes, we need global solutions developed by international fora. And these international fora are eager to be active and relevant.

This is best illustrated by the response to the terrorist events of September 2001. The United Nations responded with Resolution 1368 calling on increased co-operation between countries to prevent and suppress terrorism. The North Atlantic Treaty Organization (NATO) invoked Article 5, claiming an attack on any NATO member country is an attack on all of NATO. The Council of Europe (CoE) condemned the attacks, called for solidarity, and also called for increased co-operation in criminal matters. Later the CoE Parliament called on countries to ratify conventions combating terrorism, lift any reservations in these agreements, and extend the mandate of police working groups to include 'terrorist messages and the decoding thereof'. The European Union responded similarly, pushing for a European arrest warrant, common legislative frameworks for terrorism, increasing intelligence and police co-operation, freezing assets and ensuring passage of the Money Laundering Directive. The Organization for Economic Co-operation and Development

(OECD) furthered its support for the Financial Action Task Force on Money Laundering and, along with the Group of Eight Industrialized Nations (G8) and the European Commission (EC), called for the extension of its mandate to combat international terrorist financing. Without a pause, these fora were trying to be relevant whilst extending their mandates.

Co-operation between countries is a complex legal affair; when this co-operation is enshrined within multilateral agreements, the complexity only increases. When these multilateral agreements are created within closed fora of discussion within these IGOs, matters are only more difficult. With this difficulty and complexity come risks to existing legal systems and practices. As countries prepare to ratify the Council of Europe Convention on Cybercrime and continue to create, sign and ratify other such agreements, the public debate must be informed of the obligations that these conventions and agreements entail, and the risks that may arise.

An alarming, yet key, component of the recent activities of IGOs and their treaties and conventions is the creation of broad mutual legal assistance agreements. If law enforcement agencies from ratifying states are to co-operate, the implications need to be appreciated. Understanding how mutual legal assistance regimes are established, how the treaties function traditionally, and their implications is key to informing decision-makers, policy-experts, civil society, and the general public.

Co-operation is particularly problematic as ‘modern’ agreements conventions try to do away with traditional concerns for dual criminality; in fact, these conventions tend to dissuade and sometimes prevent countries from refusing assistance to another country on these grounds. The few grounds for refusal to co-operate are ambiguous and uncertain, e.g.

what constitutes a ‘political offence’ and the notion of ‘national sovereignty’ is interpretively flexible. These agreements may create situations where a country will be required to collect evidence on an individual without any contravention of domestic law.

The IGOs are rushing to the lowest barrier, however. The Council of Europe was once circumvented in the 1980s because it insisted on dual criminality; so state actors went elsewhere. In the late 1990s as the CoE developed its Convention on Cybercrime, it had learned from this earlier failure to appease its more interested members and clients: this broad convention does not require dual criminality, and in some cases, argues against the notion.

International solutions to national problems

For a number of years, two international bodies were developing agreements for international co-operation for ‘high-tech’ or ‘cybercrime’. The Group of Eight Industrialized Nations (G8) has been meeting regularly to discuss harmonizing methods, creating new investigative powers, and means of co-operation. Similarly, the Council of Europe, the 43 member state international treaty-making body has laboured to create the Convention on Cybercrime.

Both bodies are aiming to ensure harmonization to enable investigative agencies to investigate and surveil communications and other data without constraint of either time or space. The constraints of space are regulated through international co-operation for these investigative powers: states must respond to requests of assistance from other states. The constraint of time is regulated through expeditious co-operation: in some cases, states may not be told what the co-operation is for, while service providers may be forced to disclose personal information immediately, to foreign police.

Individuals can be monitored and prosecuted with little regard to borders. Once one country requests co-operation from another, the requested government must respond. An American may be investigated by French authorities if the French have reason to do so; and may request the assistance of the US Government and/or the US communications service provider. It matters very little if the conduct being investigated is legal or illegal in the US; once the French make a request, the US is expected to respond.

Refusing to comply

There are three rights of refusal to international co-operation, generally. The first is that for particularly sensitive surveillance, i.e. interception of communications, this should only be done for 'serious' crimes. That every country has a different understanding of what is 'serious' is disregarded.

Second, countries may refuse to assist if the suspected crime is 'political'; that each country has a differing interpretation of 'political' is also disregarded. Finally, refusal may occur if it prejudices the sovereignty or essential interests of the state.

Again, the CoE has 43 member states, and even within the G8 countries each has different laws and regards for these legal terms. Although there may be some consideration of proportionality and adequate protection of human rights, since the 'war on terrorism', what is 'proportional' and 'adequate' is open to interpretation.

New risks of regulatory arbitrage

In August 2001, the FBI apprehended Zacarias Moussaoui and his computer. A request for a warrant to search his computer was rejected by the Department of Justice as the evidence was weak. Being a French national, the FBI planned an extradition to France where his computer could be searched under weaker French protections. On 11 September, this plan was abandoned as the evidence grew.

Another example involves a declaration by Germany in late August 2002, as reported by the BBC, that German authorities would withhold evidence against Moussaoui from the United States unless they can be assured that it will not be used to secure a death penalty. Around this time, it emerged that the US and the EU were negotiating in secret a co-operation scheme that would deal with such situations.

On 16 October 2001, President Bush sent a letter to the President of the European Commission requesting assistance in the international effort against terrorism. The list of proposed actions included ‘overcoming dual criminality obstacles’, proposals to ‘revise draft privacy directives to permit data retention for a reasonable period’, and ‘establish adequate capabilities for investigating terrorism cases that involve use of the internet’. This was a call for increased surveillance capabilities to an extent that does not even exist within the US, and a reduction of any rights of refusal to international co-operation.

This creates a situation of regulatory arbitrage for governments. That is, if they are constrained by their own laws, judges, and constitutions, they may seek assistance from other countries, using the intricacies of international legal co-operation to their advantage. France had a lower threshold for accessing computer data, so the idea of sending Moussaoui there was considered. The United Kingdom does not require judicial authorization of interception warrants; the Europeans generally feel that hate speech is criminal; even national security and terrorism is defined differently; recently the Spanish considered redefining terrorism to encompass ‘violent urban youthful radicalism’.

We are seeing a situation where investigations are increasing, but the grounds for the investigation are decreasingly being divulged, and the legal obligation to do so across borders is disappearing. Once an act can be defined as criminal or terrorist, even the strongest constitutional protections appear to be weakened by regulatory arbitrage. The myth was that our technology and communications are global. The reality is that the world is filled with overlapping jurisdictions; the new myth is that our rights are protected within this new environment. The regulatory burden about to be placed on ISPs as they are forced to respond to a multitude of requests from abroad with little required justification or reason may be inescapable. Regulatory arbitrage is a power being reserved to governments.

The Current Landscape: Four Trends

Cybercrime, terrorism, and transnational organized crime are now, together or separate, a part of our policy landscape. In turn, policies arising from this landscape appear to follow a number of trends.

Trend I: Increased international co-operation in criminal and terrorism matters. The issues surrounding jurisdiction and globalization are confusing and sometimes quite constrictive to governments and other actors. A solution is to foster and generate co-operative regimes and structures. Sometimes this co-operation occurs under Mutual Legal Assistance Treaties; other times it occurs under quasi-rules; either way problems may arise.

The current landscape for international co-operation involves, generally, bilateral treaties amongst countries. In recent years we have seen the emergence of some multilateral instruments negotiated at intergovernmental organizations and other international fora, which since 2001 have seen increasing adoption. However, all countries have different legal systems; how co-operation is to occur within these varying legal systems remains to be investigated in sufficient detail.

Trend II: Increased momentum behind older policies. National policy discourses before September 2001 at best involved a very rich set of discussions, and a number of problematic policies were laid to rest. The Council of Europe Convention on Cybercrime had been criticized heavily by both industry and civil society; industry and government negotiations at the G8 had suffered from a lack of agreement; and a number of privacy invasive technologies had been set aside as their risks were exposed.

In our current policy environment, a number of these policies have re-emerged. The G8 and the Council of Europe policies and instruments are now moving forward with greater momentum; the former released new policy instruments at the 2002 G8 summit in Canada, and the latter's instrument was signed in November 2001 by over 30 countries. ID cards are proposed in countries despite previous resistance; biometrics and face recognition technologies are implemented regardless of reports of their risks and faults; and profiling is re-introduced as a solution to preventing and pursuing criminal and terrorist activity despite known legal problems.

Trend III: Increased powers, reduced protections. A common trend to the new legislation emerging from September 2001 onwards is the reduction of authorization and oversight requirements prior to the use surveillance. A number of countries allowed for ministerial warrants for the interception of communications, or reduced the conditions to the use of invasive investigative methods. Some countries are finding that international instruments are useful for this purpose; one such method will be seen in the fourth trend.

Trend IV: Technology-neutral policy and 'updating' older laws. A common articulation for governments that are making changes to their surveillance regimes is that new technology has forced the 'updating' of older laws. For example, the interception of communications laws in a number of countries speak of postal and telephone systems; *updates* are presumably required to include mobile and Internet communications.

One policy strategy used in this *updating* is technology-neutral policy. Rather than having to create new laws for each new technology that comes about, technology-neutral laws attempt to deal with all technologies equivalently under law. The problem arises, however, that all technologies are eventually treated like the telephone system or some other older infrastructure, despite large differences.

In the US, laws previously protected the privacy of an individual's cable television viewing habits because their viewing habits were considered sensitive information. Telephone traffic data, however, is often treated differently: records of who you call and for how long you spoke for are considered less invasive, and thus protected minimally under law. In the USA PATRIOT Act, passed into law in October 2001, the US Government reduced the protection of Internet traffic data to the level of telephone traffic data, arguing that technology-neutral law was ideal; despite obvious differences in the sensitivity of this data. Traffic data involving Internet devices can include location data, domain names and Universal Resource Locators (i.e.. www.computer.tld/file.html), search parameters, telephone numbers, etc.

Meanwhile, the United Kingdom in its Regulation of Investigatory Powers Act 2000 acknowledged the differences in traffic data, and recognized after a rich discourse that some data may in fact be sensitive. Canada is currently considering updating its own laws on lawful access to data, while proposing to ratify the Council of Europe Convention on Cybercrime. In its current proposals, the Canadian Government is arguing that all traffic data should be treated in a similar way, as regulated in the existing law on telephone traffic. Canada is also considering treating all communications service providers the same, whether they are Internet service providers, mobile phone service providers, or telephone service providers. It may be said that technology-neutral law, therefore, reflects the interests of the policy-makers.

The Implications: Four Paradoxes

Implication I: Specific policy is not about specific problems.

As countries move to ratify the Council of Europe Convention on Cybercrime and implement the G8 policies on high-tech crime, it is important to note that the majority of the substance within the convention and the policy instruments do not deal with cybercrime. Generally they deal with procuring surveillance capabilities and other procedural powers, and ensuring for international application of these powers. The cybercrime content of these instruments is actually quite low.

One may hazard to say that anti-terrorism laws are not necessarily about terrorism either. The substance of many proposed laws around the world has included the creation of new powers that are not limited to terrorist matters. In the United States, for example, an oversight court filed a complaint in May 2002 against the Department of Justice finding that the DoJ previously used anti-terrorism powers to investigate criminal activity, benefitting unjustly from greater powers and reduced oversight requirements.

Implication II: Pleas of harmonization do not provide harmonization. Just as every legal system has differences, as countries adopt international instruments to *harmonize* their national laws and legal procedures, they will all interpret these instruments differently. Canada's interpretation of the CoE convention is quite different to the content of the convention itself; and surely different to the powers already established within the UK, and even within the US. From differing definitions of the technologies, to differences in penalties, oversight and authorization requirements, these differences create an uncertain landscape for the safeguarding of civil liberties.

Implication III: Technology-neutral law is not neutral. Technology is not separate from society: the Internet is not something that is separate from us; it is, at least to some extent, part of our daily lives. Treating it as a unique space that must be regulated may be problematic; but at the same time ignoring its constitution and its interaction with law may be hazardous. In fact, doing so may meet the interests of the policy-makers.

Technology-neutral policies on lawful access to traffic data, for example, increase the powers of law enforcement by expanding the breadth of application of this power, while access to this data will increase the intrusion into the private life of the individual with only minimal protections and safeguards. As a result, technology policy must be specific in the forms of data that are collected and accessed, and how it is used.

Implication IV: International problems and international solutions are not built equally. Just because a problem is international, such as the regulation of global data flows or the pursuing of criminal activity across borders, does not mean that every international solution that appears is ideal. The G8 and the

Council of Europe policies have serious problems including their general lack of regard to the interests of other actors including civil society and industry; as a result I caution against the blind implementation of these instruments into national policy. These also suffered from insufficient discourse with non-state actors such as industry, law societies, technological experts, and so forth; we must now foster appropriate dialogue with these actors at this very late stage, even if little change can be effected.

The Challenges: Three Questions for Civil Society

The challenges presented here all surround the nature and quality of the policy discourse, as we must question whether it is sincere, informed, and wonder about its richness.

Challenge I: National NGOs and international fora: How sincere is the national discourse? As countries move to ratify and implement policies agreed at international governmental organizations like the OSCE, CoE, and G8, the role of national NGOs comes into question. NGOs are for the most part focused on national policy developments, and are busy enough at that level. Now they have to monitor the processes and outputs of IGOs that do not always operate openly. The Council of Europe, during the formulation of the Cybercrime Convention, argued that consultation is ideally a national process, and not the duty of the CoE itself. While this may be true with respect to its current mandate, the national policy discourses at times of ratification may not be the ideal time to discuss serious problems with the convention once there is already a felt-need to adjust national law accordingly. IGOs must change their mandates to include consultation, perhaps through requiring national consultation prior to the negotiation of charters, agreements and treaties; otherwise the sincerity of the political discourse is highly questionable.

Challenge II: How to make non-technology aware NGOs understand these issues? How informed is the discourse? Even though the CoE convention is not really about cybercrime, many within civil society have been ignoring the convention because of its apparent focus on technology and high-tech crime. Governments need to reach out to civil society to interact with and educate them on the implications of the policy changes, as the policy discourse is conducted in a technology-specific way; or otherwise governments may need to reach out to more technology-aware NGOs that may have a more specific mandate but a smaller constituency.

Challenge III: How rich is the discourse? In previous policy discourses, industry representatives and other actors played large roles. They seem to be disappearing from the discussions, however, as they may not be as willing to raise their concerns. Governments and IGOs need to reach out to other actors such as epistemic communities (law societies, engineering associations and task forces, scientists and researchers) as well as industry organizations.

The current discourses are framed as balances between civil liberties and public security; the very notion of a *balance* is a myth, a false dichotomy. The more actors that are included within the discourse the more the notion of balance will disappear as a fuller set of ideas and ideologies are presented, and more interests arise, and more possible alternative solutions may emerge. Otherwise, the policy discourse will suffer, and the policy outcome will be surely problematic.

On these dynamics

The policy landscape is thus transformed, and not in a favourable shape for national action by national NGOs who have little regard for technology and international legal issues, and little infrastructure for co-operation with other NGOs, industry, and other actors.

Unless capacities are developed, these dynamics will diminish our ability to act. Policy laundering occurred with data retention in the EU based on pressure from the US. Of course that was surely not unwelcome by some within the EU. The modelling of laws involves the adoption of international agreements and calls for harmonization to allow national laws to change with decreased accountability and national discourse. Finally, forum shifting forced the CoE to abandon dual criminality, and when the CoE did not include data retention in the Convention on Cybercrime, governments went to the G8 and then to the EU.

Keeping track of all these activities is work left for the reader. The goal keeps on shifting, the policies keep on being transplanted, and the calls for harmonization and international co-operation increase; and yet we don't appear to be interrogating these claims and following the match too well. We need to pay attention to these dynamics to understand where the game is being played. Then we can create new structures of accountability for the players.

Ian Brown

The Dangers to Journalists from New Security Technologies

Much has been written about access to information *by* journalists – using freedom of information legislation, company reports, disclosures to regulators and so on.

From the perspective of investigative journalists, the Internet has certainly increased the amount and availability of such valuable information, and the ease with which it can be accessed from across the globe. New communications technologies also have benefits for many aspects of investigative work.

But there has been little comment on the growing amount of information available *about* journalists and their sources, and the increasing number of those who have access to that information. A number of governments have passed legislation that requires phone and Internet companies to store information on the activities of their customers, and to make that information available to a wide range of officials. This type of legislation has been driven in particular by recent concerns over terrorism. Comprehensive records of calls made and received, e-mail contacts and mobile phone locations can reveal in detail a journalist's activities, and those of their sources.

Copyright holders have also been developing and lobbying for the protection of new file locking and tracing technologies to protect digital products such as music and movies. While this may reduce piracy to some extent, it may also make it far harder in future for documents to be provided to journalists, particularly in a form that hides their origin.

This chapter will describe some of these technologies in more detail, along with means by which journalists can reduce – although not eliminate – the threats that they present to investigative reporting.

Communications data. 'Communications data' is simply information *about* a communication (rather than its contents). It started becoming prevalent during the 1980s when new digital telephone systems began recording call details and hence enabled itemized billing. This kind of billing data has often been provided to the police with little oversight. British Telecom, for example, has for many years allowed the UK police direct access to its billing databases.

During the late 1990s the volume of communications data grew quickly in parallel with the increasing popularity of the Internet. Internet service providers tend to store, for a short time, large amounts of such information to enable them to diagnose and fix any problems with their services. The systems they run are able to record detailed information on every transaction that takes place – the time, date, source and destination of every web page accessed and e-mail sent or received.

The use of mobile devices, particularly telephones, has provided another dimension to communications data. A mobile phone network needs to be able to forward calls to a customer. This is normally done through a nearby base station (which communicates by radio with phones in the local area or 'cell'). Phones therefore periodically tell their network where they are by sending a 'location update' message. The network can also send a message to a group of cells asking a 'lost' phone to reveal its location. The network knows the location of a phone during a call, as it needs to transmit the call between the phone, a nearby base station, and the other party to the call. The location of a device is therefore available to a network, and is also classed as communications data.

The accuracy of location data varies by location area as well as the technology used by networks. Location update messages in cities, where there are relatively small cells, could be accurate to within 100 m or so, although typically accuracy is between 500 m – 2 km. In sparse areas of the countryside it may only be accurate to 15 km.

Networks can request a more detailed ‘measurement report’ from phones which includes timing information allowing location to about 270 m.

Even more detail can be obtained by triangulating data on other base stations in range of a phone. This capability is required in the US by Enhanced-911 government rules on emergency calls, and is included in Phase 2 of the GSM specification (which is the basis for mobile networks in most countries around the world outside the US).

Third-generation (3G) networks, which are already being rolled out in several European countries, can be much more accurate – down to 10 m. Several countries (such as the US) have mandated that phone networks achieve this level of accuracy during the next few years so that callers to emergency services can be located if their location is unknown, or if the call is lost halfway through.

Access. Given the revealing nature of communications data – disclosing reading habits, contacts and even the location of individuals – it is surprising how little protection is provided in the laws of many countries. Communications data is often treated in the same way as simple itemized telephone bills, which some governments have judged to require less protection than the contents of the calls that they describe.

In the UK, for example, the Government has proposed that under the Regulation of Investigatory Powers Act 2000 all of the following organizations should have self-authorized access to communications data on phone and Internet users:

> The Department for Environment, Food and Rural Affairs
> The Department of Health
> The Home Office
> The Department of Trade and Industry
> The Department for Transport, Local Government and the Regions
> The Department for Work and Pensions
> The Department of Enterprise, Trade and Investment
> for Northern Ireland
> Any local authority within the meaning
> of section 1 of the Local Government Act 1999
> Any fire authority as defined in the Local Government (Best Value)
> Performance Indicators Order 2000
> The Scottish Drug Enforcement Agency
> The Scottish Environment Protection Agency
> The United Kingdom Atomic Energy Authority Constabulary
> A Universal Service Provider within the meaning
> of the Postal Services Act 2000
> A council constituted under section 2 of the
> Local Government etc. (Scotland) Act 1994
> A district council within the meaning of the
> Local Government Act (Northern Ireland) 1972
> The Common Services Agency of the Scottish Health Service
> The Northern Ireland Central Services Agency
> for the Health and Social Services
> The Environment Agency
> The Financial Services Authority
> The Food Standards Agency
> The Health and Safety Executive
> The Information Commissioner
> The Office of Fair Trading
> The Postal Services Commission

Just one of these categories (‘Any local authority within the meaning of section 1 of the Local Government Act 1999’) would have included 467 local councils.

Companies around the world also have access to communications data concerning their staff, logged by their own networks and systems. This may be even more extensive and long-lasting than the data stored by telephone companies and Internet service providers. It provides a very detailed picture of who employees have been communicating with and when.

No special protection is given to journalists in many of the laws regulating access to communications data. It would be relatively easy, given access to records of such data, to identify with whom a particular journalist had been communicating and what they had been reading about on the Internet. Whether they had been in the same location as a suspected source with their mobile phone could be determined at higher cost.

Such access could be obtained using these legal powers or by order of a court, or retrieved by companies from their own records. Alternatively, they could be illegally accessed by hackers or corrupt employees of communications companies.

This obviously presents a great threat to the confidentiality of sources, especially if those sources are within governments (who may use their legal powers to gain access to relevant communications data) or companies (who may check their own records, obtain a court order to check other records, or pay private investigators to use more dubious means to do the same).

Journalists should therefore advise sources to avoid calling, sending or accessing potentially incriminating e-mail from work or home, or their mobile phones. They should instead use public payphones and Internet cafes. Sources should also avoid using long-term e-mail accounts; they should instead set up a temporary account with a free service such as Yahoo! that they use only to communicate with a specific writer. Journalists themselves may like to take similar precautions.

Data retention. New legislation in many countries allows governments to compel telephone companies and Internet service providers to retain communications data for long periods of time – a year or more. These laws have been passed in Belgium, France and Spain, and have also been proposed at the EU level. Interestingly, despite being requested by President George W. Bush in a letter on anti-terrorism measures to Romano Prodi, the President of the European Commission, the Bush administration has not proposed any data retention legislation for the US.

The willingness of sources to communicate with journalists would undoubtedly be reduced once it became known that such large quantities of communications data are being stored. For this and many other reasons, journalists may wish to join human rights activists in lobbying against such laws nationally and internationally.

Trustworthy computing. The music and movie industries have been terrified by the potential impact of the Internet and file-sharing networks upon their businesses. They have persuaded computer software and hardware manufacturers to increase the security of personal computers to reduce this threat. Microsoft's initiative in this area is called 'trustworthy computing'; other computing giants such as IBM and Intel are working on similar projects.

From the large-scale copyright owners' point of view, the most important feature of such a 'trustworthy' system is the ability to digitally lock down a file – whether it is an MP3 music track, a movie or an e-book. Users will only be able to make use of a work in the way that the copyright owner permits. They may only be able to read a book or watch a movie once, or be prevented from transferring a file to another device.

Forthcoming versions of Pentium processors and Windows software will allow files to be encrypted in such a way that it will be very difficult for a user to make an unauthorized copy. Nor will users be able to copy protected text or images from one document to another. Eventually, even the data passing over cables to monitors and speakers will be encrypted to prevent it being copied as it is transmitted between devices.

This may cause difficulties for journalists. Any type of file can be protected using these mechanisms, including incriminating government or corporate internal documents that a potential source may want to leak. It will be increasingly difficult to do so safely. While these types of security systems have been easily broken in the past, they are rapidly improving. It may be beyond the ability of all but the most advanced university or industrial labs to break them in future.

Even the tools needed to attempt to break such security mechanisms are being criminalized by new copyright law. The 2001 European Union Copyright Directive Article 6(2) requires member states to criminalize the ‘manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes’ of tools that break security mechanisms applied to copyright works. Section 1201 of the 1998 US Digital Millennium Copyright Act contains similar provisions.

Sources may be limited in future to using old-fashioned espionage methods such as photographing documents screen-by-screen. Digital cameras will continue to become smaller and easier to conceal, and automatic character recognition may allow the resulting pictures to be automatically converted back to text – although often with an annoyingly high error rate. Miniature digital audio and video recorders may also become necessary to obtain copies of sound or video files.

Journalists may wish to have these types of devices available for loan to potential sources, although leaking protected documents will obviously require a much higher level of commitment from the latter than simply e-mailing a digital file.

Digital fingerprinting. Another technology being developed by copyright owners is digital fingerprinting. This allows information on the original recipient of a digital file to be hidden inside the file, often in a way that is very difficult to remove. This is done using techniques such as subtly changing parts of an image that are less perceptible to the human eye, but which can be recognized by software. An example of such a marked image can be seen below; others can be viewed at <http://www.petitcolas.net/fabien/watermarking/>.

Image invisibly marked with the text: 'Jasc Watermark Demo, 1995-2003, Do not copy'. By kind permission of Fabien A.P. Petitcolas

Many other fingerprinting techniques exist for different media. Even with text, typographical details (such as tiny variations in the space between letters, words and lines) and textual alterations (e.g. replacing certain words with one of their synonyms) can be used to embed information.

The intention behind fingerprinting is that if a copyright work (such as a music file) is illegally made available on a file-sharing network, the copyright owner can track down the person identified in the file and prosecute them. But this technique can obviously also be used by organizations attempting to trace the provenance of a leaked document. Courts rarely hesitate to order journalists to hand over leaked source documents when they infringe copyright, trade or official secrets; an organization could then determine which of its staff originally possessed that copy of the document.

Again, this type of copyright technology is protected by the EU Copyright Directive and the US Digital Millennium Copyright Act. EU member states must provide ‘adequate legal protection’ against ‘the removal or alteration of any electronic rights-management information’ (which is the legal term used).

It may be that in future it will become too risky to sources for journalists to keep original copies of leaked documents. Printing, photographing or even transcribing a document may still leave some information on its source intact.

Conclusions. Journalists face a triple bind from new security technologies. Potential sources will find it increasingly difficult to copy digital documents in an unauthorized way. If they succeed, increasing communications surveillance will make it easier to trace the source of that leak. And even if they manage to extract and confidentially provide a document to a journalist, that document – if obtained by the organization where it originated – may contain the identity of the source in a way that is very difficult to remove.

This presents serious obstacles to the freedom of the press to investigate controversial issues that could in future be much better protected against leaks. Recent US history might have unfolded very differently if the Pentagon Papers could only have been read on a small number of computers in the Pentagon, and could not be printed or otherwise copied. Journalists may need to become more expert on these technological mechanisms than they perhaps would like.

Governments should also consider the impact on the media of laws requiring the retention of communications data, and that mandate access for large numbers of government officials. Instead, they might consider extending the requirements of the EU Telecoms Privacy Directive – which forces communications companies to delete or anonymize communications data once it is no longer necessary for business or law enforcement purposes – to corporations, so that employee privacy can be better protected.

Acknowledgements:
Thanks to Duncan Campbell and Simon Davies for their useful comments on an earlier draft of this chapter.

Seán Ó Siochrú

ICT Networking and the Influence of Governance

Not all the requisites and obstacles to ICT networking can claim a direct link to governance. But perhaps a surprising number of them are at least indirectly influenced. This article sketches their relationship, often covering some distance. Although the impact is sometimes direct and accounts for most or all of the issue in question, for others, governance is just one among a wider set of factors that together constitute an obstacle to engaging in networking using ICTs.

Three layers of conditions that affect ICT networking were identified, each with a number of components. Here, layer by layer, the components are examined in terms of their relationship or otherwise to governance.

Layer 1: Physical access and enabling tools and resources

Network infrastructure and affordable access. The Internet today can be accessed directly from anywhere in the world, as testified to by the media's use of mobile satellite equipment. In practice, however, virtually all TCSOs (transnational civil society organizations) are restricted to Internet access via publicly available networks, mainly for reasons of cost and regulation. The availability and affordability of an adequate network infrastructure is a prerequisite to TCSO networking in that, in general, the Internet is carried over a phone or data line for which a connection fee and regular rental must be paid.

And their absence is probably the single greatest obstacle facing TCSOs in networking in the South. Many rural areas have virtually no access at all, or are limited to expensive poor quality long-distance phone connections. But in urban areas, the cost of connection and monthly rental of a phone line can put network access beyond the reach of many civil society organizations beyond mere sporadic use. The scale of this challenge in the South is enormous, and is especially acute in rural areas and among poorer communities. The ITU (International Telecommunication Union) reports that the 'growth rate in the number of new telephone subscribers plunged in 2001'.[1] Although rural versus urban figures are unavailable and are in general inadequate, it seems likely that the lower-return rural lines were hardest hit.

Governance is deeply implicated in whether an Internet connection is available and offered at affordable prices. Although private, market-driven provision of infrastructure has more and more become the norm, the demand for governance and regulation is in many respects greater as compared to that for state-owned monopoly provision. The nature of the intervention has shifted from government policy directing a national supplier, to government regulation creating the environment for competition between multiple suppliers. Major concerns are governance factors that influence the physical coverage of infrastructure; the quality of infrastructure in terms of the networking services it can offer, and the tariffs charged for them. These determine availability and affordability.

The early phase of privatizations and foreign investment in the 1990s saw relatively rapid network expansion. Hugely profitable markets in urban areas in the South were quickly tapped, and mobile phones, even beyond major urban centres, became a quick and profitable means to supply the wealthy and middle classes with a basic service. The accompanying move towards cost-based tariffs in effect reduced tariffs for international and long-distance calls but increased tariffs for local calls and the monthly line-rental charge.

Yet it was difficult for developing countries to formulate, implement and enforce effective universal service policies, lacking the specialist expertise and facing powerful corporations and sometimes diplomatic pressures from their corporate homes. Furthermore, in many poorer countries, especially in Africa, demand even among the business and middle class sectors was so low that national telecommunication operators were sold at knock-down prices with virtually no licence obligations attached. At the height of the telecommunications boom during the 1990s the focus of some investors was simply on securing markets and licences as the global telecommunication sector was carved up among a handful of corporations. Overall, such universal service strategies have been implemented at a national level with only limited success.

From this quick sketch, a number of governance issues can be identified as having played, and as continuing to play, a significant role in the availability and cost of telecommunication access.

At the highest level, the effective narrowing of sources of investment and control to the private sector, and the continuing emphasis of major governance institutions such as the IMF (International Monetary Fund), World Bank and WTO (World Trade Organization) on liberalization and privatization policies at the very least limit the options available to governments and other actors in confronting an uncomfortable future investment and network development scenario. Given what we believe to be the limitations and likely redundancy of this recipe, an urgent exploration of other options would seem to be justified.

[1] ITU, *World Telecommunication Development Report 2002: Reinventing Telecoms* (Geneva, 2002), p. 1.

On the positive side, the pursuit of universal service or universal access policy is among the most important, aiming to provide affordable access to all. Although in practice this goal remains a distant aspiration for most countries of the South, universal service policy strives to exert ongoing pressure to extend telecommunication access beyond what would be accepted as commercially viable from the narrow perspective of return on investment. This aspiration remains the same, whether under monopoly government networks or private competing operators, though the modalities for achieving it are very different.

The locus of universal service policy and implementation is first and foremost at national level – there exist no global mechanisms for universal service or cross-subsidization.[2] But it is the global level that now drives the trend through the GATS (General Agreement on Trade in Services) agreement under the WTO. Since 1998 GATS signatories are obliged in their national policy to:

- Open markets to foreign investment in all areas of telecommunications, including voice telephony, leased lines, mobile and satellite;
- Ensure that discrimination by dominant players is prohibited, to ease market entry;
- Ensure fair, transparent and non-discriminatory interconnection with dominant suppliers;
- Require a regulator independent of any telecommunications supplier;
- Allocate frequencies, numbers and other resources in a transparent and non-discriminatory manner.

The precise interpretation has yet to be tested by WTO adjudication mechanisms. But as noted, universal service policies have seldom been successfully implemented in the South. The emerging GATS-compliant norm is that an independent sector regulator develops universal service policy and implements this through imposing conditions on the issuance of licences to existing and new operators. These licence conditions can vary enormously, and may refer not only to extending the basic network and reducing tariffs but also to the provision of advanced services and tailored packages such as community telecentres in rural areas. Telecentres[3], providing collective access to ICTs usually in rural areas, have become a popular policy tool favoured by many donors. Results so far regarding benefits and sustainability suggest that there exists no single formula for success and that much depends on local circumstances and the strategy adopted.[4] But there are successful examples, some of which are used extensively by civil society organizations for networking.

Internet access. Factors influencing the accessibility and affordability of Internet use, the next stratum up on the enabling infrastructure, include the presence of an Internet service provider (ISP) offering services at affordable rates, and the availability of appropriate Internet domain names. Current trends suggest the following. Dial-up ISP access at local call rate (or less) is growing in most Southern countries, sometimes beyond the main urban areas. In some major cities, cable or high speed access is even available. However, in most rural areas, access is still unavailable or of very poor quality. In wealthier countries, high speed access is spreading in urban areas and in rural, though still at a relatively high cost.

[2] Some international cross-subsidization (albeit unintended, unsystematic and incoherent) had been effected under the ITU administered accounting rate system, but this is now largely abolished.

[3] Known variously as community multimedia centres, community cybercafés, etc. They range in services from a usual basic set of telephony, Internet access, fax, copying and printing; but can also include community radio and other media and information activities.

[4] Florence Etta, *The Experience with Telecentres*, ACACIA Programme, 2003 <http://www.acacia.org.za/telecentres_etta.htm>.

Policy can and has been used to lower the cost of using the Internet. Many countries in the North and South have introduced special low tariffs for the dial-up use of the phone line, thus reducing the cost of use – though the network is often unable to sustain a good long-distance connection.

A proposed new Internet Protocol IPV6 may also have an impact on services in the long term. Apart from potential risks to privacy and of increased surveillance, dealt with further on, the migration to the new protocol may lead to an additional suite of services available to users at additional cost. While this is to be welcomed in one way, the danger is that more basic and affordable services will be gradually phased out. A similar situation can be seen with regard to UUCP (Unix to Unix Copy Protocol), a protocol that was a forerunner to the current IPV4. This offered cheap e-mail and spread rapidly in poor countries.

As Internet use becomes more intensive and varied, registration of an Internet domain name can become useful and even essential for TCSOs. Some domain names can be bought and registered online with relative ease, such as those in the high level domains of .org and .com, but the selection of names available on these can often be limited since so many have already been registered. Registering a country domain name (such as .in for India) generally offers a wider choice of names, a useful tool for NGOs in terms of projecting an identity and being easily contactable. Yet such registration can still be problematic.

A high profile instance of a success for an NGO was ‘eToy vs. etoys’, otherwise known as the Toy War. A company that sold children’s toys via its website attempted to sue a small electronic arts collective for the use of a similar domain name, despite the fact that the artists had been using their site for several years. As the case progressed through the courts, the artists mobilized a network of supporters including tech savvy hacktivists and experienced public relations experts to create a blitz of negative publicity for the toy company. Tactics included posting messages about the campaign in chat rooms linked to online stock exchanges. Eventually, the toy company pulled back but continued to suffer from brand erosion; ultimately it collapsed into bankruptcy.[5]

Hardware and software. The cost of hardware is clearly identified as a major obstacle to participation in ICT networking. There are some efforts to address this head on, through the production of low-cost computers tailored to low-income users. One of the better known examples is the Simputer, developed in India by a trust with the specific goal of bringing ICT technologies to poorer communities. (http://www.simputer.org/simputer/) Built on Open Source software, it also incorporates user interfaces to facilitate use by illiterate people.

Governance issues also have a significant say in the cost of software. For instance, Microsoft would be unable to charge what they do for their products were it not for the fact that software is now probably the most heavily protected of all knowledge-based products.[6] Under TRIPS (trade-related aspects of intellectual property rights), software qualifies not only for copyright protection but in some countries for patent protection too. Yet copyright is intended to cover creative activity rather than industrial or economic tools, and so was not the most obvious choice of protection for software producers. They differ significantly from most other copyrighted material in being primarily a business tool. The explanation for the anomaly lies largely in the fact that while patents expire

[5] Steve Kettman, 'Etoy Balks at Olive Branch', *Wired.com*, 29 December 1999 <http://www.wired.com/news/politics/0,1283,33351,00.html>.

[6] UK Commission on Intellectual Property Rights, *Integrating Intellectual Property Rights and Development Policy* (London, 2002), p. 116 fn 6.

twenty years after they are filed, copyright is enforced for fifty years after the death of the author, and for a total of fifty years in the case of a corporate owner.[7] While not being the obvious candidate, copyright offers the most enduring and strongest of all protection mechanisms to owners, and is instrumental in keeping prices high.

With TRIPS in place, enforcement of copyright is also gaining strength, with corporate and bilateral pressure being put on countries with perceived high levels of 'piracy'.

Layer 2: Generating, retrieving and using content

The second layer of requirements for effective ICT networking is the content layer or the substance of networking: the wherewithal to access and use a variety of relevant information sources, to generate content, to interact in a variety of ways with many different actors. Several potentially inhibiting factors are identified.

Public domain and intellectual property. The public domain is that reservoir of information and data that can be freely drawn on by all, for a multitude of purposes, free of charge and without legal constraints. Information in the public domain is common property, a part of our shared heritage or commons.

While 'information overload' is one factor identified as discouraging ICT networking, restricting access to information is clearly not a solution. Unnecessary restrictions on the public domain limit information readily available and thus the raw material for networking. TCSOs draw on the public domain for research, for publications and for advocacy, a key feature being that it costs nothing. Alternative news organizations make extensive use of public domain information, in producing programmes and compiling news; and research and information dissemination activities often rely heavily on public domain material.

Information can find its way into the public domain following several possible routes though some restrictions are legitimate, for instance to protect privacy. Sometimes a balance must be struck between competing interests at the point of entry, one such case being intellectual property rights and especially copyright.

Copyright is a monopoly granted by the state for a given period over the reproduction of the output of creative work. It is especially relevant in this context since it can cover everything from academic research to music, to media output and even software. Copyright, in its origins and based on legal judgements, is intended to strike a balance between the right of the creator to receive a reward for the effort put in and the right of society to enjoy the fruits of such creativity. By adequately rewarding creativity, the goal is to encourage further creativity into the future.[8]

The Internet has posed new challenges to copyright. Although attempts by the US and Europe in the mid-1990s to introduce copyright even for browsing the Web (on the basis that a temporary copy is made) into the TRIPS agreement were thwarted by a coalition of telecommunication and Internet companies and libraries[9], related issues remain around ‘linking’ in websites. In the US and elsewhere, even simple links to another website (which are ‘publicly’ on the Web anyhow) have been found guilty of copyright infringement if they facilitate unauthorized access to copyrighted material.[10] But what

[7] The Commission on IPRs, ibid., set up by the UK Government, noted that there is no clear economic rationale for copyright protection being so much longer than for patents.

[8] Seán Ó Siochrú and Bruce Girard, *Information Wants to be Free;* an ITU *Visions* Paper, (Geneva, 2003) <www.itu.int/visions>.

[9] Seán Ó Siochrú, Bruce Girard and Amy Mahan, *Global Media Governance: A Beginner's Guide* (Oxford and Boston: Rowman & Littlefield, 2002), p. 94.

[10] WIPO, *Intellectual Property Rights on the Internet: A Survey of Issues* (Geneva, 2002) <http://ecommerce.wipo.int/survey/index.html>, p. 51.

is described as ‘deep-linking’ or ‘embedded linking’ is even more problematic in that it bypasses the home pages, and links to secondary material. When systematically used to gather information on a sustained basis, such linking is probably contravening the database law in the EU, and in the US cases have been taken relying on copyright, trespass, breach of contract, and common law misappropriation. Similar cases are taken against ‘framing’ of content from another website. In this case copyright protected material that may legitimately be accessed from one website is ‘framed’ by a different website possibly with different logos and advertising (though only in the RAM of the computer). In Germany this has been found to transgress the national Copyright Law.

These trends in copyright mean that the fruits of intellectual endeavour are more expensive than they need be, including scientific and research information of direct relevance to TCSOs. A further effect of the electronics revolution has been to exacerbate the tension between copyright owners and reproduction for ‘fair dealing’ and ‘fair use’, such as education, an issue carefully circumscribed under the Berne Treaty and balanced as an integral part of copyright. Under fair use small scale, partial copying is permitted for non-commercial, research, educational and archival use. These by no means fulfil the needs of poorer countries, being far too restrictive[11], but what is there hangs under a future threat in the digital era.

Layer 3: The control environment

Up to now, we have been dealing with the requirements of ICT networks, the enablers of networking. Now we turn to factors that by their presence actively inhibit the capacity for TCSOs to network using ICTs. By ‘control environment’ we mean external political, legal, corporate, and military constraints imposed on the TCSO environment that hinder TCSO networking in a number of ways, sometimes causing severe problems. Overt forms are Internet censorship and direct suppression of networking activities. Less obvious but in some respects more insidious are surveillance and various disruptive techniques utilized by security forces, governments and transnational corporations.

Freedom to access, use and exchange information without censorship, filters or limits. Censorship affects the transmission, sharing and reception of information. While it is true that there are many cases in which the Internet has been used by TCSOs to bypass censorship, early claims that the Net is somehow 'by nature' uncensorable have been shown to be largely inaccurate.[12]

The technical capacity to censor the Internet is usually based on filters placed in proxy computers.[13] The proxy server is used by ISPs to download the web content requested by users, acting as an intermediary between the user and the final source of the information.[14] Although not designed for this purpose (for instance, they store locally frequently requested pages thus saving on costs and speeding up interactions), a filter can be installed to monitor traffic to nominated addresses, prevent access to them, and/or inform specified parties of the request.

[11] UK Commission on Intellectual Property Rights, op. cit., p. 111; S. Ricketson, *The Berne Convention for the Protection of Literary and Artistic Works: 1886 * 1986* (London: Kluwer, 1987), p. 591.

[12] Most famously, by Lawrence Lessig in the seminal *Code and Other Laws of Cyberspace* (Basic Books, 1999).

[13] For a technical account, if dated, see Philip McCrea, Bob Smart and Mark Andrews, *Blocking Content on the Internet: A Technical Perspective*, National Office for the Information Economy, Australia, June 1998 <www.cmis.csiro.au/projects+sectors/blocking.pdf>, accessed 21/05/2003.

[14] Christiane Hardy and Karen Spaink, 'Freedom of the Internet – Our New Challenge', *OSCE Yearbook 2001/2002. Report on Freedom of the Media* (Vienna: OSCE, 2002).

Some proxies are more easily circumvented than others, but in general directly dialling an ISP in another jurisdiction will get around them though this is not always an available option. In Germany the Government attempted and failed to block all access to a major Dutch ISP, XS4ALL, that carried a left-wing autonomist publication.[15] Indeed this illustrates the 'blunderbuss' approach of proxy filters – they often block out huge amounts of information that they claim not to target.

While some argue that state censorship of Internet content is technologically untenable, pointing to users' multiple strategies for circumventing control, others indicate that government censorship technologies and strategies are becoming increasingly sophisticated. For example, in China, TCSOs use counter-filter software, mirror sites, anonymous UseNet BBS (Bulletin Board System), anonymous remailers, encryption, and other tools.[16] However, major firms including Cisco and Sun have been working with the Chinese Government to develop and strengthen sophisticated content filtering and user monitoring systems.[17] Initial 'clumsy' filters that once blocked the entire Google search engine have been replaced by fine-tuned software that targets a specific subset of political pages.[18] While there may always be backdoors and ways around censorship, increased technological blocking tools and severe penalties for infractions limit free access to information to those technologically sophisticated and/or daring enough to cross the lines of state control.

Some groups turn to other means to censor Internet content and in particular to pressuring commercial companies into taking action. In combination with a virtual global monopoly on wholesale bandwidth (from which ISPs buy their bandwidth and connectivity), the impact could be significant. The idea of industry self-regulation has also become somewhat fashionable in areas such as child pornography, pornography, violent content, racism and so forth. The Council of Europe, for instance, proposed that the industry should develop codes of conduct and self-regulatory measures. In absolute terms, such an approach can never be fully effective except in the few areas, such as child pornography, that are deemed illegal everywhere. Policing legal material is, in the end, untenable. But self-regulation can nevertheless have a significant long-term effect on the availability of information, through for instance the obstacles, costs and uncertainty of mounting constitutional legal challenges especially in grey legal areas – of which there remain many in national and international law.

Concern with self-regulation goes deeper than its capacity to uphold censorship. The danger is that it allows governments to refuse to set rules and limits, and to devolve key issues for society to private bodies, bodies often dominated by commercially minded industries.

This article is a portion of a report commissioned by and prepared for the Social Science Research Council programme on Information Technology and International Co-operation in 2003. The full, original version is available at the SSRC website <www.ssrc.org/programs/itic> or by contacting the Social Science Research Council directly in New York.

[15] See <http://www.xs4all.nl/~tank/radikal/>

[16] Jason Lacharite, 'Electronic Decentralisation in China: A Critical Analysis of Internet Filtering Policies in the People's Republic of China', *Australian Journal of Political Science*, 37, no. 2 (2002), pp. 333-46.

[17] Greg Walton, 'China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China', *International Centre for Human Rights and Democratic Development*, 2001 <http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html>.

[18] Jonathan Zittrain and Benjamin Edelman, 'Empirical Analysis of Internet Filtering in China', Berkman Center for Internet and Society, Harvard Law School, 2003 <http://cyber.law.harvard.edu/filtering/china>.

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.

Glossary

(Source Wikipedia, the Free encyclopedia, www.wikipedia.org)

Cache – A cache in computer science is a short-term memory in a computer with quick access. A cache is intended to speed up access to a set of data. The cache will be a piece of memory that is faster (hence more expensive, hence smaller) than the principal data storage area for the data in question. The cache operates by storing a part of the data, allowing that part to be accessed more quickly. A speed-up is achieved if many accesses to the data can access the data in the cache. The reason caches work at all is that many access patterns in typical computer applications have locality of reference. There are several sorts of locality, but we mainly mean that often the same data is accessed frequently or with accesses that are close together in time, or that data near to each other are accessed close together in time.

Censorware – Censorware is a term used to describe content filtering software by its opponents. They point out that content filtering software acts as an effective restraint on speech, and that government-driven mandatory installation of content filtering software is equivalent to censorship. Censorware is often proposed as a solution to the problem of hate speech on the Internet. Opponents of censorware point out that these tools not only block other content in addition to hate speech, either unintentionally, or as part of the political agenda of the manufacturers of the content filtering software, but also fail to block all the hate speech.

Client – A Client is a system that accesses a (remote) service on another computer by some kind of network.

Congestion – In telecommunication, the term congestion has the following meanings:

1. In a communications switch, a state or condition that occurs when more subscribers attempt simultaneously to access the switch than it is able to handle, even if unsaturated.
2. In a saturated communications system, the condition that occurs when an additional demand for service occurs.

Denial of service attack – A denial of service (DoS) attack is a term used to describe certain forms of malicious damage to computer systems. The aim of such an attack is to prevent legitimate users from accessing their services. A DoS attack is generated in a number of ways. There are three basic areas of attack – the consumption of limited resources, such as bandwidth, disk space or CPU time; alterations to configuration information, such as routing information or registry entries; and the physical disruption of networking components. The attack on resources has become increasingly popular, mainly through attempts to 'flood' a network with excess or spurious packet data over the Internet, thereby preventing legitimate traffic. Distributed denial-of-service (DDoS), where many computers work in unison to attack a target system, has also gained notoriety due to the efficient tools which are available to create and launch such an attack.

DNS – the Domain Name System, is a distributed database that handles the mapping between host and 'domain names' which are more convenient for humans, and the numerical Internet addresses. That is, it acts much like a phone book, so you can 'call' www.wikipedia.com instead of 64.78.205.6.

FTP – The File Transfer Protocol, (FTP) is a protocol that is able to transfer files between machines with widely different operating systems.

Gigabyte – A gigabyte is a unit of measurement in computers of approximately one thousand million bytes, (the same as one billion bytes in the American usage) or roughly 1000 megabytes.

Google – Google is an Internet search engine founded in 1998 by Larry Page and Sergey Brin, two Stanford Ph.D. candidates, who developed a technologically advanced method for finding information on the Internet. As of 2002, it was the most popular search engine.

Internet – As a proper noun, the Internet is the publicly available worldwide, interconnected system of computers (plus the information and services they provide and their users) that uses the TCP/IP suite of protocols. Thus, the largest internet in the world is called simply 'the' Internet.

IP address – The Internet protocol (IP) knows each host by a number, the so-called IP address. On any given network, this number must be unique among all the hosts that communicate through this network.

ISP – Internet Service Provider (ISP), provider of Internet services. Most telecommunications operators are ISPs. Provides services like Internet transit, domain name registration and hosting, dial-up access, leased line access and colocation.

Kazaa – KaZaA Media Desktop is a peer-to-peer file sharing application on the Music City network, developed by FastTrack for Consumer Empowerment. It is very similar to Morpheus, which also used the FastTrack protocol. Many consider KaZaA to be superior to other programs because of its file selection and fast transfer speeds. Countering that is KaZaA's use of spyware and adware installed as default with the main product. The Altnet software, also installed by default, is another problem, it allocates users' bandwidth to serve advertisements to others.

Mirror – On the Internet, a mirror is an exact copy of data stored in a different location. Popular sites use mirrors to reduce network traffic on any one server.

Morpheus – Morpheus is also the name of a file sharing client operated by the company Streamcast (formerly called Musiccity) that originally used the OpenNAP peer-to-peer platform. It has a web-based search interface, just like Audiogalaxy, though Morpheus searches all kinds of media, not just mp3. In 2001, Morpheus changed protocol from OpenNAP to FastTrack. On 26 February 2002, all Morpheus clients suddenly stopped working when the FastTrack protocol was updated and Morpheus users no longer were allowed to log into the network. This was apparently because of licensing disputes between StreamCast and the owners of FastTrack. On 2 March, a new Morpheus client using Gnutella as its P2P medium was released.

Napster – Created by Shawn Fanning, Napster was a music and file sharing service that made a major impact on the Internet scene during the year 2000. Its technology allowed music fans to easily share MP3 format song files with each other, thus leading to massive copyright violations.

Newsgroup – A newsgroup is a repository within the Usenet system for messages posted from many users at different locations. Newsgroups are arranged into hierarchies, theoretically making it simpler to find related groups.

NGO – A Non-Governmental Organization (NGO) is an organization which is privately funded (mostly by donations from the general public) and is independent from the government and its policies. Most often it is a non-profit organization.

NNTP – Network News Transport Protocol. A TCP-IP protocol based upon text strings sent over 7 bit ASCII TCP channels. It is used to transfer articles between servers as well as to read and post articles. Defined in RFC 977. The format of messages is specified by RFC 1036.

Operation Clambake – Operation Clambake is the title of a World Wide Web page that has become known as the single most important site with information about Scientology. It is run by Andreas Heldal-Lund, a critic of Scientology who views the organization as a cult. The website provides considerable insight into the workings of Scientology, and it includes links to Scientology's 'secret' documents as well as other information that the organization has tried to suppress. The website is one of the focus points of the war between Scientology and the Internet. Scientology had made numerous legal threats to various Internet service providers that have hosted the site, demanding that it be removed from the Internet. In various incidents that have been documented in such publications as the *New York Times, Slashdot* and *Wired Online*, Scientology has also used copyright law to force notable websites (including the Google search engine) to remove all references to the Operation Clambake site.

Peer-to-peer – As opposed to non-peer or client-server. Peer-to-peer describes a symmetric protocol, application, or network where every node has equivalent capabilities and privileges. Any node is able to initiate or complete any supported transaction. Peer nodes may differ in local configuration, processing speed, network bandwidth, and storage quantity. A protocol can be categorized as peer (symmetric), non-peer (asymmetric, usually client-server), or both. Consider the Usenet news service. Usenet news servers are NNTP peers among themselves, but NNTP servers to Usenet newsreaders. Usenet newsreaders are NNTP clients to the Usenet servers but do not communicate with other Usenet clients directly. Usenet clients and servers implement only the portions of NNTP that are needed for their purpose.

PICS – Platform for Internet Content Selection; The PICS specification enables labels (metadata) to be associated with Internet content. It was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing and privacy.

Scientology – Scientology is a controversial system of beliefs and teachings, begun in 1952 by author L. Ron Hubbard, and presented as a religion. It was first incorporated in the US as a non-profit organization in 1954, and is considered to be a religious non-profit organization under the tax code administered by the Internal Revenue Service. It is not a recognized religion in many countries, and in some countries, notably Germany, it is officially seen as a dangerous practice.

Search Engine – A search engine is a program designed to help the user access files stored on a computer, for example on the World Wide Web, by allowing the user to ask for documents meeting certain criteria (typically those containing a given word or phrase) and retrieving files that match those criteria. Unlike an index document that organizes files in a predetermined way, a search engine looks for files only after the user has entered search criteria. In the context of the Internet, search engines usually refer to the World Wide Web and not other protocols or areas. Because the data collection is automated, they are distinguished from Web directories, which are maintained by people.

Software cracking – Software cracking is software hacking in order to remove encoded copyright protection. Distribution of cracked software (warez) is generally an illegal (or more recently, criminal) act of copyright infringement.

SMS – Short Message Service (SMS) is a service made available on most digital mobile phones that permits the sending of short messages (also known as text messages) between mobile phones. SMS was originally designed as part of the GSM digital mobile phone standard, but is now available on a wide range of networks, including forthcoming 3G networks.

Software-patch – A software release is to create a new version of the system or program and release it to the user community. Each time a software system or program is changed, the programmers and company doing the work decide how to distribute the changes or the changed system or program to those people using it. A software patch is a method of distributing the changes. It is either a program that modifies the original unchanged system or a program to create the new one or a list of instructions for a person who follows them to create a new one.

Software-piracy – The term software piracy refers to copyright violation for profit, i.e. the unauthorized selling of counterfeit computer software, music, movies etc. The copying of software, music and films where no money changes hands, sometimes known as warez, is legal in some jurisdictions. In Russia, it is legal to copy any software as long as it is not in the Russian language.

Spamming – Spamming is the process of sending unwanted electronic messages. The most common form of spam is Unsolicited Commercial Email (UCE) or Unsolicited Bulk Email (UBE), the electronic form of junk mail. A spammer will send identical or nearly identical messages to a large number of e-mail addresses, often harvested from Usenet postings or web pages, or obtained from databases, without the permission of the recipients.

Steganography – Steganography is the science of writing hidden messages, where ‘hidden’ means not only that the message cannot be read by anyone other than the intended recipient, but also that no one else even knows that a message has been sent. Generally a steganographic message will appear to be something else, like a shopping list, an article, a picture, or some other ‘cover’ message.

Streaming media – Streaming media is a term that describes ‘just in time’ delivery of multimedia information. It’s typically applied to compressed multimedia formats delivered over the Internet.

The Web – The World Wide Web (‘the Web’ or ‘WWW’ for short) is a hypertext system that operates over the Internet. To view the information, one uses a piece of software called a web browser to retrieve pieces of information (called ‘documents’ or ‘web pages’) from web servers (or ‘sites’) and display them on the user’s screen. The user can then follow hyperlinks on the page to other documents or even send information back to the server to interact with it. The act of following hyperlinks is often called ‘surfing’ the Web.

Traffic – The information moved over a communication channel.

URL – A Uniform Resource Locator, or URL, is a standardized address for some resource (such as a document or image) on the Internet. First created by Tim Berners-Lee for use on the World Wide Web, the currently used forms are detailed by IETF standard RFC 2396 (1998).

Usenet – Usenet (also known as Netnews) is a set of protocols for generating, storing and retrieving news ‘articles’ (which resemble mail messages) and for exchanging them amongst a readership which is potentially widely distributed. It is organized around newsgroups, with each newsgroup carrying articles about a specific topic. Readers see all the articles posted to each newsgroup in which they participate. These protocols most commonly use a flooding algorithm which propagates copies throughout a network of participating servers. Typically, only one copy is stored per server, and each server makes it available on demand to readers able to access that server. Usenet was thus one of the first peer-to-peer applications.

UUCP – (Unix to Unix Copy Protocol) This Project started in the early 1980s as a means to facilitate the exchange of electronic mail among sites using the UUCP store-and-forward transport mechanism. This UUCP software, originally part of the UNIX operating system became available on a variety of operating systems and platforms, from large mainframe to small home PCs.

Webcam – A webcam is a small digital camera attached to any computer that is connected to the Internet. It is mainly used to take pictures and make short films of the surrounding area or the camera’s owner and post them in (almost) real time to the World Wide Web. Other uses might include chatting, security, and video conferences over the Internet.

Web Log – A web log (also known as a *blog*) is a website that tracks headlines and articles from other websites. They are frequently maintained by volunteers and are typically devoted to a specific audience or topic.

The Authors

Christian Ahlert is a visiting fellow at Oxford University's Programme in Comparative Media Law and Policy, located at the Centre for Socio-Legal Studies. His research interests include Internet regulation, media law and policy, technological change and globalization. Most recently he convened the conference 'Politics of Code' at Oxford, funded by the Thyssen Stiftung, see <www.codepolitics.info>. Currently he serves on the Nominating Committee of the Internet Corporation for Assigned Names and Numbers, which is charged with the selection of directors for the global Internet regulator. He is also an expert consultant on a number of European Commission funded projects. Under the Safer Internet Action Plan, he is examining the effectiveness of self-regulatory structures and he consults on Internet policy reform in Vietnam and Indonesia. He publishes articles on the Internet and politics in newspapers and online editions such as *spiegel-online*, *politik-digital*, *telepolis*, *Die Woche*, FAZ and FR.

Yaman Akdeniz is a lecturer at the Faculty of Law, University of Leeds where he teaches and writes mainly about Internet-related legal and policy issues. He is also the founder and director of Cyber-Rights & Cyber-Liberties (UK) <http://www.cyber-rights.org>, a non-profit civil liberties organization. Dr. Akdeniz is an international policy fellow of the Open Society Institute and is working on a project entitled *Civil society participation in the policy-making process of the Turkish Government in relation to the development of an Information Society in Turkey* (March 2003 – March 2004). His publications include *Sex on the Net? The Dilemma of Policing Cyberspace*; *The Internet, Law and Society* and he was involved in drawing up the Regulation of Investigatory Powers Act 2000.

Ian Brown is director of the Foundation for Information Policy Research. He has spoken and written extensively on communications and healthcare privacy, copyright and e-voting. Dr. Brown is an honorary research fellow at London University, from where he received a PhD in communications security. He is advising the US Government on the security of their next-generation emergency communications systems, and is the co-author of a forthcoming Kluwer book on this subject. Brown has consulted for other large organizations such as the BBC, JP Morgan and Credit Suisse. He is also a trustee of Privacy International.

Freimut Duve, a German politician, human rights activist, writer and journalist, was elected the OSCE Representative on Freedom of the Media by the OSCE Ministerial Council in December 1997. Duve was born in Würzburg and received his education in Modern History, Sociology, Political Science and English Literature at the University of Hamburg. He worked as an editor at the Rowohlt publishing house and was a Social Democratic member of the Bundestag (German Parliament) from 1980 to 1998, representing his city, Hamburg.

Benjamin Edelman is a student fellow at the Berkman Center for Internet & Society. He has written extensively about Internet filtering in countries worldwide, and he served as an expert witness in the American Civil Liberties Union's lawsuit challenging the constitutionality of requiring Internet filtering in American public libraries. Mr. Edelman's research brings a quantitative focus to Internet policy – writing software to collect data as to the behaviours of interest. Beyond Internet filtering, Mr. Edelman studies and writes about domain names and ICANN; Internet advertising, pop-ups, and 'spyware'; junk email; and P2P filesharing.
Publications can be found at <http://cyber.law.harvard.edu/edelman>.

Alberto Escudero-Pascual is assistant professor at the Royal Institute of Technology (KTH) in Stockholm. In 2002 he obtained his PhD on the subject of privacy in the next generation Internet. Since his arrival to Sweden, Escudero has been involved in design and deployment of different wireless initiatives including the IT University wireless infrastructure (2000), a broadband wireless access in the city of Nora (2001), the neutral access network StockholmOpen (2002) and lately in two projects in Laos and Vietnam (2003) with the support of the Swedish International Development Agency (SIDA). <http://www.it.kth.se/ aep> <aer@kth.se>

Ian Hosein is a visiting fellow in the Department of Information Systems at the London School of Economics and Political Science. He is an advisor to a number of non-governmental organizations, including Privacy International and the American Civil Liberties Union. As a researcher and lecturer, he focuses on topics including international anti-terrorism policies, the dynamics of international co-operation and policy-making, privacy and data protection, and technology policy and regulation. <http://is.lse.ac.uk/staff/hosein>

Mindaugas Kiškis is a researcher at the Department of Legal Informatics at the Law University of Lithuania. He received an LL.M. degree from the Faculty of Law, Vilnius University in 1998 and continued legal studies and research at the University of Amsterdam, the Netherlands (1998); Stockholm University, Sweden (1999); LaTrobe University, Australia (2000); European University Institute, Italy (2001) and Oxford University, United Kingdom (2002). In June 2002 Mr Kiskis was awarded a PhD from the Law University of Lithuania for his doctoral dissertation on the topic of software law. He has published in foreign and Lithuanian periodicals on intellectual property law, Internet law, citizen's rights and other legal issues of the knowledge society. <mkiskis@lpvp.lt>

Hans J. Kleinsteuber has been a professor of Political Science/Comparative Government and Journalism at Hamburg University since 1982. He teaches media policy (technology, economy) in Germany, Europe and North America from a comparative perspective, Internet and electronic democracy, public spheres, and comparative research schemes etc. 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 and curator of the association <politik-digital.de/europa-digital.de>. His recent publications include *Information Superhighway in the US* (1996); *Information Highway in Hamburg* (1997); and *Recent Trends in US Media* (2001).

Tarlach McGonagle is a project researcher at the Institute for Information Law (IViR) at the University of Amsterdam. He studied Law and French at the National University of Ireland, Galway (including one year at l'Universite de Poitiers, France) and International Human Rights Law at the University of Essex, England. He has worked as a journalist and as a language teacher (teaching both English and Irish at l'Universite Charles-de-Gaulle-Lille-3, France). He has worked as an intern for the Irish Council for Civil Liberties, the Council of Europe, and as an intern and consultant for ARTICLE 19, Global Campaign for Free Expression. His research interests are primarily freedom of expression issues, minority rights and human rights law, especially in a European context

.

Christian Möller is project assistant at the Office of the OSCE Representative on Freedom of the Media. Before that he had worked from 1999 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 in Kiel and is currently working on his doctoral thesis about the effects of technical innovation on freedom of expression on the Internet.

Sjoera Nas works for Bits of Freedom, a not-for-profit privacy and civil rights organization in the Netherlands. She is the editor of EDRI-gram, a biweekly newsletter about digital rights in Europe. From 1998 until 2002 she worked for the Internet provider XS4ALL. As public affairs officer, she was responsible for the policy regarding principal issues, like freedom of speech and privacy. She initiated a court case against a spammer, decided to defend freedom of speech in a court case instigated by Deutsche Bahn about the magazine *Radikal* and played a very active role in the association of Internet providers to promote privacy protection. Responsible for the sponsor policy, she was one of the organizers of HelpB92 in 1999. She is still a member of XS4ALL's advisory board.

Peter Noorlander is a legal officer with ARTICLE 19, Global Campaign for Free Expression. Having joined the ARTICLE 19 Law Programme in 2001, he specializes in issues of freedom of expression and privacy, freedom of information, broadcasting and new technologies, and has contributed to many ARTICLE 19 publications. Before joining ARTICLE 19, he worked with JUSTICE, the UK section of the International Commission of Jurists, where he was part of the privacy and EU criminal policy team.

Seán Ó Siochrú is a writer, consultant and activist. He has written several books, most recently *Global Media Governance: A Beginners Guide* (with B.

Girard and A Mahan: Rowman & Littlefield, 2002). He is a spokesperson for the CRIS Campaign (Communication Rights in the Information Society: <www.crisinfo.org>); and chairperson of Community Media Network and Dublin Community Television in his home country, Ireland. To earn a crust, he works as a consultant on media and ICTs issues for international bodies such as UNDP, IFAD and the EU; and is director of NEXUS Research, a non-profit research organization.

Felipe Rodriquez founded XS4ALL in 1993, and acted as its CEO until 1997. He also founded the Dutch ISP association in 1995, and acted as its chair until 1997. He has been at the centre of the legal debate over censorship and Internet service provider issues in Europe and the world. He currently works as a board member for a number of companies and organizations.

Karin Spaink is a freelance writer who has published eight books and hundreds of articles and columns. Her main subjects are politics, health, information technology and language. She started writing about civil rights and the Internet in 1995. She chaired Contrast.org, an organization providing asylum for sites banned elsewhere, and is currently chairing Bits of Freedom <www.bof.nl>, the main organization for civil rights online in the Netherlands. She is also a juror for the Dutch Big Brother Awards. Internationally, she's best known for her ongoing legal case with Scientology, a battle that has in part to do with copyrights but mostly with freedom of speech. In September 2003, she won the third round of this battle with flying colours. Scientology is now expected to go to the (Dutch) Supreme Court. <http://www.spaink.net>

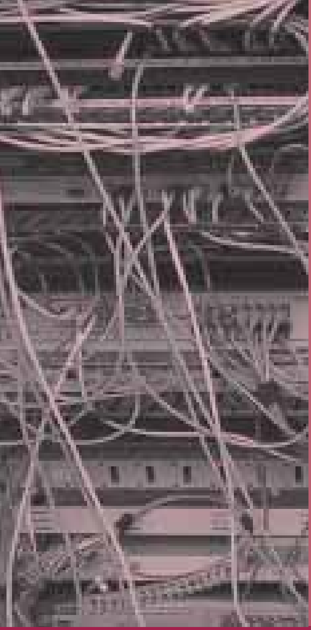
Sandy Starr is public relations officer at the online current affairs publication *spiked* (www.spiked-online.com), and co-ordinates *spiked*'s analysis of information technology issues. He also writes for publications ranging from the *Times Literary Supplement* to *The Sun* newspaper, is a contributor to the recent book *The Internet: Brave New World?*, and has worked with the European Commission research project RightsWatch on copyright regulation issues. He believes in unqualified freedom of expression, and he is concerned that new frameworks of human rights and self-regulation are invisibly eroding free expression on the Internet.

Jelena Surčulija graduated from the Faculty of Law at Belgrade University. She works as a senior media legislation assistant with the Media Department at the OSCE Mission to Serbia and Montenegro, Belgrade. As an OSCE representative she is actively involved in the drafting of new media legislation in expert working groups. She assists the licence and frequency advisor, thus directly contributing to the OSCE monitoring and support programme for the licensing of Serbian electronic media. She also contributes to the drafting of internal bylaws for regulatory agencies and has initiated and helped to set up the Yugoslav Association of Internet Service Providers.

Páll Thórhallsson is a legal officer in the Council of Europe's Directorate General of Human Rights. He is the Secretary to the Group of Specialists on online services and democracy. Before joining the Council of Europe, Mr. Thórhallsson worked as a journalist and lawyer in Iceland. In 1998, he graduated from Strasbourg University, France, with a DEA in Comparative Human Rights Law. He has published several articles on legal matters in Icelandic journals.

Mikko Välimäki is a researcher at the Helsinki Institute for Information Technology, Finland. He has published on the subjects of computer law and law & economics and is currently writing his PhD on software licensing. Mr. Välimäki has also been a visiting scholar at the University of California, Berkeley. He is a co-founder and chairman of Electronic Frontier Finland. Mr. Välimäki graduated with a Masters in Law (major in law & economics) from the University of Helsinki in 1999.

Jonathan Zittrain is the Jack N. and Lillian R. Berkman assistant professor for Entrepreneurial Legal Studies at Harvard Law School, and a director of its Berkman Center for Internet & Society. His research includes the technologies and politics of control of Internet architecture and protocols, and the influence of private intermediaries upon online behaviour. He has a strong interest in creative, useful, and unobtrusive ways to deploy technology in the classroom. Publications can be found at <http://cyber.law.harvard.edu/zittrain>.



www.osce.org/fom

Christian Ahlert
Yaman Akdeniz
Ian Brown
Benjamin Edelman
Alberto Escudero-Pascual
Ian Hosein
Mindaugas Kiškis
Hans J. Kleinsteuber
Tarlach McGonagle
Christian Möller
Sjoera Nas
Peter Noorlander
Seán Ó Siochrú
Felipe Rodriquez
Karin Spaink
Sandy Starr
Jelena Surčulija
Páll Thórhallsson
Mikko Välimäki
Jonathan Zittrain