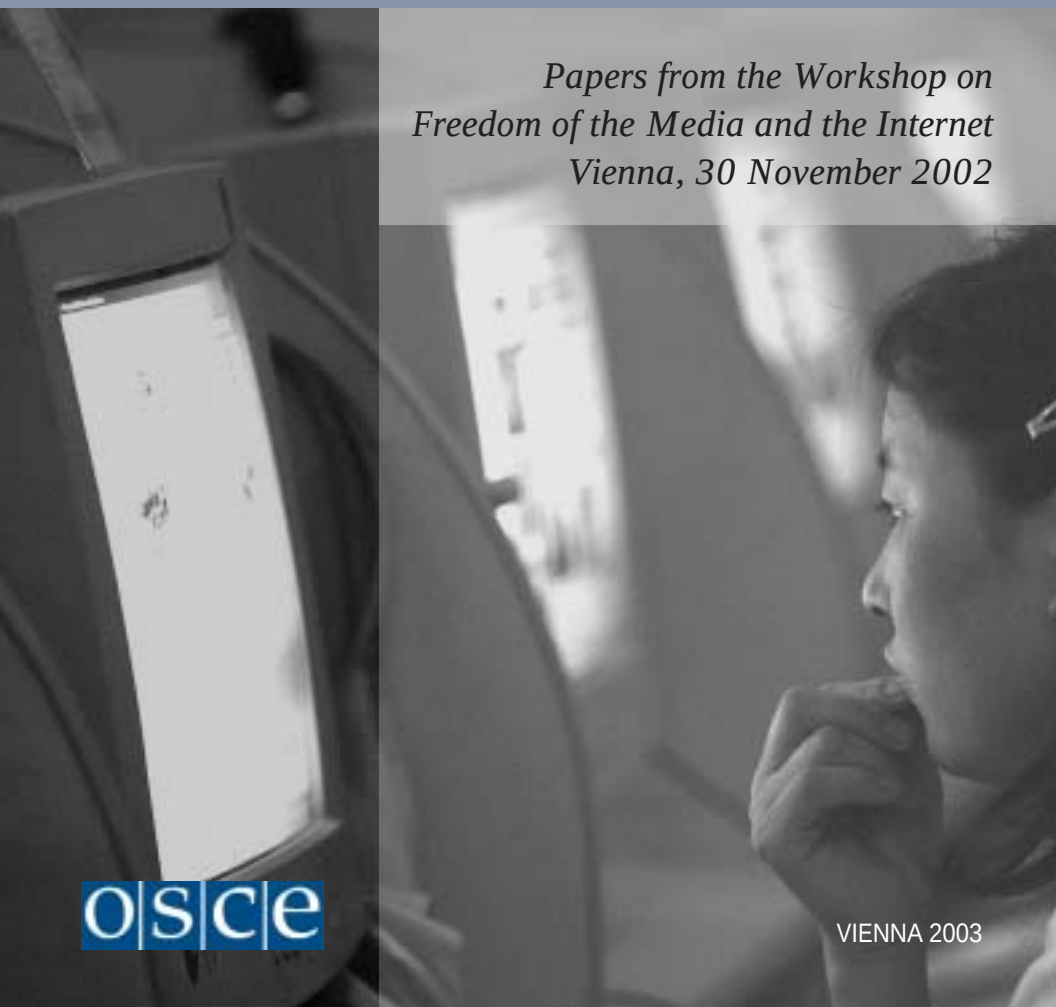
From Quill to Cursor

The Representative on Freedom of the Media

Freedom of the Media in the Digital Era

Papers from the Workshop on Freedom of the Media and the Internet Vienna, 30 November 2002



OSCE

VIENNA 2003

OSCE

REPRESENTATIVE ON FREEDOM OF THE MEDIA

From Quill to Cursor

Freedom of the Media in the Digital Era

Papers from the Workshop on
Freedom of the Media and the Internet
Vienna, 30 November 2002

Vienna 2003

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 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: AP, Ng Han Guan

Design: WerkstattKrystianBieniek, Vienna
Printed by Eugen Ketterl, Vienna

Contents

Freimut Duve
Preface

The Internet offers an unprecedented means for people all over the world to distribute, exchange and access information. Information and ideas on the Internet are typically not bound by state borders, which makes it easier for people to circumvent existing methods of censorship. However, while the Internet is rapidly becoming more widespread and accepted, so are attempts to curtail this new freedom of expression and the development of new technologies also brings along new means of censorship.

Even if criminal contents or hate speech are accessible on the Internet, the advantages for freedom of expression outweigh the dangers of misuse by far. But although there might be a legitimate need for regulation, this process must be closely monitored to prevent forms of censorship from being imposed on the new infrastructure that would be intolerable with the classic media.

In order to guarantee the freedom of the media on the Internet our prime task is to identify the problems and possible dangers that threaten this universal right. The first step in this direction has already been taken with the FOM workshop in November 2002 in Vienna, where experts from a wide range of organizations were brought together. The papers from the workshop are collected in this publication.

The debate will be continued at the Conference on Freedom of the Media and the Internet, organized by my Office, which will take place on 13 and 14 June 2003 in Amsterdam.

Vienna, March 2003

Karin Spaink
Introduction

From Quill to Cursor: Freedom of the Media in the Digital Era

New Technologies Raise New Perspectives – and New Questions. 'Technology is not just a value-neutral set of tools,' as the Electronic Frontier Foundation (EFF) correctly observed.[1] New technologies (especially those concerning communication and the distribution of information) invariably bring about new political and social relations. Precisely in so doing, they actually change the world, and our minds.

Gutenberg. Once knowledge, ideas, thoughts, insights, and theories started being written down and being put into books, they suddenly acquired a less transient and volatile form. For the first time in the history of humankind one could literally hand down a body of knowledge and preserve it in its original form, not only for oneself and for others, but also for future generations. While we now routinely award prizes to books, in the pre-Gutenberg era books themselves were the prize. Yet, in part because of their sheer cost – books had to be manually copied, one by one, at a painstakingly slow rate – in practice, books were monopolized and were only accessible to a very small elite: some scholars, some of the higher clergy, and, of course, the rich.

1 Electronic Frontier Foundation, *Building People In: Architecture Is Policy* <http://www.eff.org/buildin.html>

It was the invention of the printing press that made books more affordable and more generally accessible. When the excruciating process of copying manuscripts by hand was supplanted by the mechanical printing press, wider sections of society could finally gain access to books. A remarkable interaction was initiated: with the appearance of books, the wish to become literate became general and the ability to read spread outside the elites that had previously had access to handwritten books. Increasing literacy in turn promoted the publication of more books, thus creating a spiral of increasing abilities and knowledge for the masses.

The Gutenberg revolution allowed individuals to educate themselves and made them less dependent upon what others – their superiors, the clergy, or even the travelling troubadours – would relay to them or were willing to summarize for them. After the onset of printing, ideas could spread faster and further, whilst retaining their original form, without intervention or mediation (or 'filtering', as one would now say), and one no longer had to rely on experts or the elite to disseminate or interpret these ideas. In short, the printing press had a tremendous liberating effect on people in general. It enabled them to become generally more knowledgeable and informed, generally more independent, and generally more equipped. One could even argue that the invention of the printing press was one of the founding elements of democratic society.

Publishing Explosion. Currently we are in the middle – or perhaps it is only the onset? – of the digital revolution. Both the variety and the total volume of available texts has increased manifold since articles and books began to be published on the Internet. Some statistics may serve to illustrate the gargantuan volume of this digital explosion.

Usenet is the name for the collected newsgroups, which are organized by subject. Usenet was developed in the 1980s for scientists to exchange information and discuss ideas. By now, there are newsgroups about almost everything: from hobbies, lifestyle and sports to culture, science, and politics. In the early stages of Usenet, it was possible to follow more or less all existing newsgroups and read all postings in them. Nowadays, that is utterly impossible. By 18 December 2002, Newszilla – one of the biggest news servers in the world, run by the Dutch ISP XS4ALL – carried no less than 46,181 different newsgroups.

The total volume of Usenet postings is called the 'newsfeed'. In March 2001, the global newsfeed was measured to be 2 Gb of text[2] and 220 Gb of binaries (pictures, sound files, executables, etc.) per day. Less than 1.5 years later, in October 2002, the global newsfeed had doubled to a daily 400 - 450 Gb.[3]

The number of websites has increased even more spectacularly. The World Wide Web was created in May 1993, when the first application was invented that could present structured, hyperlinked text. That application was Mosaic, the first browser ever. Already that same year, images could be integrated into the text. Much later, around 1996, sound and moving images (film) could be added to web pages.

2 Gb means 'gigabyte'. One gigabyte equals 1024 megabytes (Mb), a megabyte contains 1024 kilobytes (Kb), and a kilobyte consists of 1024 bytes. Thus, a gigabyte is 1,073,741,824 bytes. For comparison's sake: this document is 152,064 bytes long, so it would take 7061 times this text to get one gigabyte of data.

3 Erik Hensema, *FAQ/VVV: De XS4ALL newsservers* (14 December 2002) <http://groups.google.com/groups?safe=off&ie=UTF-8&oe=UTF-8&as_umsgid=newsservers-1039935300-3268%40hensema.net&lr=&hl=en>

The following table presents the increase of websites in the first three years of the WWW, at half-year intervals.[4]

Year - Month	No. of websites
1993 - June	130
1993 - December	623
1994 - June	2,738
1994 - December	10,022
1995 - June	23,500
1995 - December	90,000

By the end of October 2002, the number of individual pages indexed by Google, currently the prime search engine, had reached almost 2.5 billion. Three months later, in January 2003 – just under ten years after the birth of the Web – that number had reached almost 3.1 billion.[5] And although Google indexes a great deal, it doesn't even index everything.

Distributed and Shared Information Makes the Net Robust. The Internet is not only a publishing tool, it is also a distributing technology. Servers all over the world keep polling one another. News servers for instance exchange articles with one another: 'I have this bunch of new newsgroup articles, here ya go.' 'Thanks. Oh, I already have some of them. I'll reject those and take the rest.'

In a similar way, routers (which forward traffic between networks and keep track of which website is located where) assist one another in finding out the shortest route to a website and in figuring a way to get there when a part of the network is down. 'I can't reach www.osce.org. Can't reach their hosting provider, a shackle in the chain from me to them is missing. Do you know how to get there?' To which another router might reply: 'Sure, I know another way. I'll point you.

Go to that machine, then take that one, and then...' Or: 'I can't get there either. But I can get a few steps closer than you can. What if I ask somebody in that neighbourhood?' Or they'd say: 'It takes me 42 hops to reach X. How many hops does it take you? 180? Well, here's how I do it.'

All this filling in of the gaps, finding shortcuts, balancing traffic, sharing information and circumventing fall-out is built into the system. It is an integral part of the underlying structure of the Internet – which is designed to work in such a way that if a connection between two distribution points breaks down, both servers will find new routes to reach one another.[6]

This basic structure is the backdrop of the famous adage that 'The Internet perceives censorship as damage [to the system] and routes around it.' It means that a disruption in the system – no matter whether it is caused by accident, error or malice – will never bring down the system as a whole.

Adopting Routing Relations. A fascinating phenomenon, especially from the point of view of censorship and its prevention, is that Internet users have adopted this principle of routing around damage as a model to base their own behaviour

4 Information taken from Net Genesis (now defunct), quoted in *A Profile of the Internet* <http://www.cwrl.utexas.edu/~tonya/309m/class/internet.html> (sec-tion 2). I proudly testify that my website was one of the 23,500 counted in June 1995.

5 On its front page Google states the exact number of indexed pages; the count is updated automatically.

6 This is true only for the *structure* of the Net, not for its content. When the server hosting my website is down, nobody can reach my website. However, as far as routers are concerned – the machines that point the way on the Internet by making data packets hop from one place to another – its tasks will readily be taken up by other routers. Thus, the damage is minimized.

7 'Censorship' in this respect should be taken broadly. It does not only refer to pages being yanked by governments or by other authorities, but also to pages being closed as a result of libel or copyright law.

upon. When a web page – or worse, a whole site – is under threat of censorship,[7] website owners often utilize their human networks to route around the impending damage. They ask their contacts to take copies of the besieged pages and to publish them elsewhere, in less dangerous places. This phenomenon is known as mirroring.

And just as routers assist one another in finding the easiest way to reach a certain machine, Internet users help one another – dutifully assisted by the courts, one might add tongue in cheek – to find the locus of least resistance, places where certain material will be the least challenged and the most secure. Because neo-Nazi sites will generally be prosecuted in most West European countries, such groups have wisened up and have taken their information out of that continent. Since the USA provides a much broader level of protection for speech, that country has become the international host for sites like this. They have found political asylum there so to speak. Conversely, Singaporean pages about sexuality and religion and US sites about drugs are often hosted in Europe, where such pages meet with less resistance than in their country of origin.

Especially for those whose ideas and perspectives do not match the dominant point of view, or who live in a repressive society, the Internet provides a welcome tool. A newspaper doesn't need to be published in your own country for you to be able to access it. Additionally, the act of accessing certain information becomes less public: when you ask for a magazine in a shop, you have to do so openly, but on the Net, you can retrieve that information without the shop owner – or your neighbours, or the police – knowing anything about it. Suddenly, information can be smuggled out. Or in. Suddenly, the classical censoring of the media no longer works, nor do the standard means of social control.

Internationalized Information. While governments and authorities may on the one hand dislike this internationalization of information and routing around censorship, on the other hand they sometimes hope to reap a benefit by adopting the same practice themselves. The Netherlands for instance is not very pleased by 'its' neo-Nazi's seeking digital refuge in the United States, yet it gladly hosts sites aimed at a US audience craving more objective information about recreational drugs. Simultaneously, CNN hopes to reach and inform the citizens of Middle Eastern countries and to circumvent the media restrictions imposed upon citizens of this region by their own governments. Indeed, the CIA has funded software that circumvents certain types of national censorship and that re-enables foreign citizens to tune in to the Web version of *The Voice of America*.[8]

Various authorities try to limit the impact of this phenomenon by attempting to curtail the Net in a variety of manners. Until now, most of these censorship efforts have generally failed.[9] This is partly because computer experts are technically

8 In December 2001, Safeweb received seven million dollars from IN-Q-Tel, the CIA's venture capital fund and a second investor for the development of this software, which was dubbed Triangle Boy. The product seems to have been discontinued. Safeweb is however still in the business of thwarting those trying to police the Net. Recently, they released SEA Tsunami for secure remote access: once you log in to Safeweb's SEA, your activities on the Net can no longer be logged (see <http://www.safeweb.com/sea_tsunami_features.html>). Western states are more and more interested in such logs and the EU is currently discussing laws that make retention of user logs by their ISPs mandatory. The UK already has such a law, called the RIP Act. For more information about Safeweb and SEA, see Thomas C. Greene, 'US company defeats Brit RIP Act', *The Register*, 17 January 2003 <http://www.theregister.co.uk/content/8/18017.html>

9 For an extensive overview of these censorship efforts, their downsides and their workarounds, see Felipe Rodriquez, 'Burning the Village to Roast the Pig', in this publication, 85-109. Bennett Haselton, however, points out that circumvention software is prone to fail in the long run; see Bennett Haselton, 'List of possible weaknesses in systems to circumvent Internet censorship' <http://www.peacefire.org/circumventor/list-of-possible-weaknesses.html>

more proficient than their policy-making opponents and can, with some effort, figure a way around restrictions and prohibitions and develop new protocols to share and access information, and partly because censorship is by definition reactive, a response to a newly created technical reality, and will thus always be lagging behind.[10] Yet, over the years attempts at curtailing the Net have been getting increasingly knowledgeable and more difficult to circumvent. And while computer experts often do find loopholes in censoring software or policies, and can write software or protocols that circumvent such measures, this in turn usually means that programs are becoming increasingly complicated and thus difficult to use for the uninitiated.[11]

This shifting around of information – either politically and geographically, by finding the locus of least resistance, or technically, by distributing information via rapidly evolving new protocols – is part and parcel of the Net, just as integral and fundamental to it as it is on the structural level of the Internet. Indeed censorship is perceived as damage, and not only does the Net itself try to route around it, but Net users and developers attempt to route around it as well.

This phenomenon drastically changes the effect of national law and politics. Information that is not legally available in a country can readily be served to a citizen of that country from a website located at the other side of the globe. And interestingly, the person requesting that information will not even notice that it is coming from elsewhere. This means that the Internet has made national borders and political boundaries more diffuse than they were and has lessened their importance, or at least has undermined their strictness. National laws curtailing information are simply not as effective as they used to be. The internationalization of information

allows citizens to partake of (or distribute) facts, knowledge, relays and experiences that they would otherwise not have been able to access or share. The analogy with the effect of the Gutenberg press is apt.

New Technologies Create Novel Needs and Responses. With the assistance of a cheap computer and a modem, or with an Internet café in the vicinity, anybody anywhere[12] can access foreign newspapers, start publishing their own magazine, make their ideas and knowledge available to the world, read or publish stories which otherwise would never cross the border, exchange and discuss ideas with people at the other end of the globe.

A newly arisen wish is to block some of these pages. This is not only practised by governments – and both China and Saudi Arabia are rather effective in this respect – but also by companies, libraries and schools, the latter two usually at the government's behest. People at home do it too.

---

10 Historically, censorship is always either circumvented through high tech (which is too difficult for censors), or by reverting to low tech (which is too common for it to be censored). When the USSR made printing difficult, dissidents fell back upon the manual carbon-copying of books and articles (samizdat); B92, the censored Serbian news broadcaster, used both high and low tech and eventually depended upon a combination of Internet cable connections for uploading broadcasts and foreign radio stations broadcasting them via medium wave.

11 PGP – encryption – is a good example. While PGP provides an almost foolproof method of rendering e-mail communications illegible for all outsiders (and thus for snooping governments), many people find it very difficult to use. Although PGP nowadays comes with a broad variety of good and easy-to-use interfaces, somehow PGP still has a too technical 'feel' for most people, which in itself works as a rather effective deterrent against using it, no matter how useful or necessary PGP might be.

12 In principle, at least. Some countries are badly connected, and the increasing habit of Western websites to use lots of Flash and other heavy applications makes it very difficult to view these web pages: it takes ages for them to load, so viewing them becomes very expensive. However, web space – i.e. publishing – is getting cheaper by the day, and there are a number of places where one can get free web space (Lycos, Geocities, Tripod etc.). Postings on Usenet (newsgroups) are archived automatically; one doesn't even need to have a website to store them.

There are two basic strategies for blocking pages: imposed blocking and requested blocking. With imposed blocking, a government orders that certain pages should be blocked nationwide. This can be done via a national proxy (a machine that handles all requests for web pages; it acts as an intermediary between a personal web browser and web servers on the Net). The proxy is in such cases configured to refuse requests for any page that matches certain (blacklisted) criteria. Saudi Arabia for instance routinely blocks all foreign pages relating to sex and politics.[13] China, on the other hand, blocks pages based on their IP number (crudely, their Internet address).[14] Australia has implemented a system blocking specific national pages, but does not block international ones.[15] In Germany, the state of North Rhine-Westphalia has ordered ISPs and universities to block access to certain sites (mostly, but not exclusively, neo-Nazi sites).[16] In the US, publicly funded schools and libraries are obliged to block pages deemed to be unfit for children and teenagers.[17]

A nasty characteristic of this type of blocking is that almost invariably, it censors more than it purports to do. Especially blocking based on IP has dire consequences: it affects entire sites or sometimes even a series of web servers sharing the same IP, while actually only a few pages on those sites or servers fall within the scope of the prohibition. Blockages of this type are very difficult to overcome. Additionally, a shared characteristic of imposed blocking is that the citizen has no choice whatsoever in the matter.

Requested blocking on the other hand is voluntary. It takes place at the user's instigation and on the user's computer only. It is usually done to protect children and to present them with a customized, sanitized version of the Net. This type of blocking is done via commercial so-called censorware. (It is

this kind of software that US public libraries and schools use, but in their case it is mandatory.)

An interesting hybrid variant was used by Scientology. The cult developed its own version of a censorware package which, at the user's end, blocks all pages critical of Scientology. Critics of the cult dubbed this censorware Scienositter, after the package of which it was a derivate: Cybersitter. Scienositter had one unexpected characteristic: it was imposed upon unwitting cult members. Scientology sold them a package to create instant 'individualized' proselytizing web pages; the program installed the Scienositter on the sly, thus preventing these members – without their consent – from seeing pages that Scientology deems inappropriate because they oppose the organization's own view.[18]

While voluntarily blocking pages on one's own computer is an unalienable right, blocking pages at school or libraries is an altogether different matter. Civil liberties organizations have made a pretty good case that censorware programs actually filter out more than they profess to do and have – in the USA – started lawsuits asserting that such blocking of information is

13 See Harvard researchers Jonathan Zittrain and Benjamin Edelman, *Documentation of Internet Filtering in Saudi Arabia* <http://cyber.law.harvard.edu/filtering/saudiarabia/>

14 Felipe Rodriquez describes the principle in his essay, 'Burning the Village to Roast the Pig', in this publication, 85-109.

15 See Electronic Frontiers Australia, *Internet Censorship in Australia* (20 December 2002) <http://www.efa.org.au/Issues/Censor/cens1.html>, and Felipe Rodriquez, 'Burning the Village to Roast the Pig', in this publication, 85-109.

16 Alexander J. Kleinjung, 'Vom Daten-Highway auf die Straße', in the German edition of *C'T*, September 2002. The law is heavily criticized by, amongst others, Initiative für ein freies Internet; Plattform zur Veranstaltung von Online-Demonstrationen (ODEM) <http://odem.org/>, and the Chaos Computer Club (CCC) at <http://www.ccc.de/censorship/>

17 The US Congress passed the Children's Internet Protection Act (CIPA) on 15 December 2000. The full text of the act is at <http://www.ifea.net/cipa.html>

18 See *Scientology Censors WWW for Members* <http://scn.martinobrien.com/ABUSE/KRASEL/COS/FILTER/FILTER1.HTM>

in fact unconstitutional. Indeed, on 31 May 2002, a federal court agreed with that criticism. The US state has appealed the ruling, and the case is currently being reviewed by the US Supreme Court.[19]

Fashionable Self-Regulation. Not only is information shifting from place to place to find the locus of least resistance; measures to contain information are doing exactly the same. Slowly, the governments of industrialized countries have arrived at the general agreement that discussions about, and measures against, disputable websites should not be carried out by themselves, but by others. In just a few years, so-called self-regulation of the Net has become one of the policy makers' new buzzwords.

Self-regulation means that the industry is assigned a major role in policing content that is not clearly illegal, and therefore not directly punishable, and/or should reach agreement upon how to act when complaints are received about web pages. The industry is asked to develop, possibly in co-operation with users' interests groups (such as civil liberties and privacy organizations), rules for acceptable use, codes of conduct and procedures for the removal or suspension of disputed pages. The standard categories that are mentioned as areas where self-regulation should be promoted are child pornography, pornography, violence, racism, and 'hate speech'[20].

Almost all European national and supranational governmental and official advisory bodies nowadays promote such self-regulation. The Council of Europe for instance states: 'International co-ordination should also involve the industry, which should be encouraged to develop codes of conduct and self-regulatory schemes. This co-ordination is also essential to guarantee the protection of minors against content which is not strictly illegal, but may be harmful and detrimental to

their personal development, in an environment where traditional ways of controlling access (for example watershed rules) do not work.'[21] This proposal is a rephrasal of the Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content.[22]

Self-regulation will of course never be able to solve the fundamental problem of information travelling to the locus of least resistance. After all, when such information has found a safe haven, that new abode is by definition a country where that information is fully legal. Policing legal material is of course redundant and blatant nonsense. Taking this into account, the only area where general agreement is at all possible is child pornography: it is forbidden in practically all countries. Then again, precisely because the trafficking in or displaying of child pornography is illegal everywhere, self-regulation is not necessary. There are solid laws against it. And policing illegal acts should not be relegated to private parties. All other contested material – from racism to depiction of sex – is legal in one country or another, and can thus never be banned from the Net.

---

19 The US Children's Internet Protection Act is being fought by the ACLU, the American Civil Liberties Union. The case is being reported on as it develops at <http://archive.aclu.org/features/f032001a.html>

20 'Hate speech' is a loosely defined lump term used to denote the propagation of hatred against ethnic minorities. Sometimes they border on or are neo-Nazi types of pages. The amount of attention they get from both other media and policy makers is, however, somewhat disproportional. In 2000, Hatewatch.org counted between 450 and 500 'hard core' hate sites and circa 1750 sites that it deemed 'problematic'. (Source: *QuickFacts: Hate and Hate Crimes* <http://www.media-awareness.ca/eng/issues/stats/isshate.htm>). Let's be very pessimistic and set the number at 50,000 pages all in all. Let's then set the amount of all existing pages in 2000 at 1 billion, a rather high number. Basic maths tells us that even with these exaggerated figures 'hate pages' make up a mere 0.05 per cent of the total amount of pages. One would wish that there was as little racism and hatred in the analogue world.

21 Páll Thórhallsson, 'Freedom of the Media and the Internet', in this publication, 51.

22 Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content, adopted by the Committee of Ministers on 5 September 2001. For the full text, see <http://cm.coe.int/ta/rec/2001/2001r8.htm>

Moving Censorship Out of the Public Realm. Apart from that, there are quite a number of drawbacks to and loopholes in self-regulatory systems.[23] First of all, and it is really begging the question, why should 'content which is not strictly illegal' (to quote the Council of Europe) be subjected to any kind of regulatory measure or process? Parents are after all free – and encouraged – to install censorware if they want to protect their children, while any kind of industry self-regulatory practice affects the rights of mature Internet users to access material that is 'not strictly illegal', which is a rather obscure way of saying that it might be in bad taste but it *is* actually legal, in which case the industry has no right to prevent access to it.

Conversely, where it concerns material which is illegal in country A, but fully legal in country B where it is hosted, the industry of country A has no right to prevent anyone from accessing it. The government of country A can indeed decide to outlaw such material, but then they should take that responsibility upon themselves and not dump it on the industry.

Secondly, some material might indeed be on the borderline, but countries have a fully qualified system to make decisions about the acceptability and legality of specific material: the courts. By moving the assessment of the legality of such material out of the court room, not only do the processes and criteria by which material are judged become opaque, they additionally run a high risk of becoming arbitrary. Indeed, existing self-regulatory bodies – such as the censoring authority in Australia and the child pornography hotline in the UK – have already gained a reputation for being remarkably furtive about their own proceedings. Needless to add that, unlike in court, the accused lack lawyers and the possibility to appeal decisions.

Thirdly, the term 'self-regulation' is highly deceptive. As the above shows, it is not about the industry regulating itself,

but about the industry regulating its customers. In other words, self-regulation primarily concerns itself with regulating others.

Fourthly, the industry is supposed to regulate something in which it itself has a stake – that of having a blooming business without too many hassles. ISPs weren't started to defend users' rights, nor are they generally willing to stand up for free speech when the effects of that speech might damage their reputation or their revenues. In that sense, ISPs and their clients become opponents whenever an ISP receives a complaint about one of its customers. Legally, the customer might be in his full right to publish the disputed material, but the ISP – facing a complaint – is not likely to assist him to find arguments in favour of publication. In other words, one of the parties involved in the conflict has been assigned complete responsibility to decide upon the fine line between legality and illegality. The protection of the constitutional right to express one's opinion is being put in the hands of the industry.[24]

Finally, what is fundamentally wrong with self-regulation is that it allows governments to refuse to set rules and limits, and lets them delegate the matter to a private body, hoping to solve the issue in this way. In doing so, governments are privatizing censorship, without assuming responsibility and accountability for it themselves, and without offering legal redress for either those censored or for those robbed of access to the censored content.

---

23 Sandy Starr elaborates on the theme in 'The Diminishing Importance of Constitutional Rights in the Internet Age', in this publication, 57-72.

24 A Swedish case (Flashback facing MCI/Worldcom over one of its users) and a Dutch/US case (Xtended Internet facing Scientology over one of its users) are described in detail in Christiane Hardy and Karin Spaink, 'Freedom of the Internet: Our New Challenge', *OSCE Representative on Freedom of the Media Yearbook 2001/2002* (Vienna, 2002), 129-43. In both cases, the providers stood up for their clients; in both cases, their upstream providers simply cut the ISP's connection without redress being possible.

Susceptible Search Engine. The gargantuan number of web pages resulting from the new digital publishing-and-distributing technique has created a demand for new meta-technologies: that of indexing and retrieving web pages and newsgroup postings. Indexing web pages and Usenet postings has become a matter of prime importance. After all, what would be the use of publishing something in a newsgroup or on a web page, if nobody could find it in this vast sea of exponentially increasing information? Without retrieval technologies, the only way to be informed about the existence of specific pages would be by word of mouth, which of course defeats the purpose. It would make the sharing and distribution of information a local matter once again.

Search engines provide precisely this service. When you key in a few search terms, search engines will point you to pages or newsgroup postings that contain these terms. Some search engines additionally rate pages by assumed relevance, some search engines organize them in coherent groups, some do nothing but present long lists of so-called 'hits'. What all search engines have in common is that they guide you through the Web and Usenet, and assist you in finding what you were looking for. Search engines have become pivotal to the Net, to the degree that without them, there is no way to find your way around.

Their particular strength makes them susceptible to censorship attacks, all the more so because the possibility to access pages or to censor them, are at heart two sides of the same coin. Indeed, without the facility to sift through indices using search terms, censors wouldn't even be able to decide what pages to block in the first place... While finding a page is the result of filtering massive amounts of data in order to select a set based on specific criteria, blocking is filtering that information in order to suppress that same set.

In the past few years, search engine censorship has been on the rise. Through a number of French court cases, the US based Yahoo auction site was forced to prevent French users from perusing Nazi memorabilia. While the relevant court decisions have finally been overturned in the US,[25] by now a number of search engines have voluntarily adapted their local, nationalized versions so that people consulting the German, French and Swiss version of Google will not be able to find neo-Nazi or white supremacy content, even though these pages are quite legal in the countries where they are hosted and indexed.[26] (However, the mother of all Googles, the international Google, <http://www.google.com>, still lists them and is readily accessible to German, French and Swiss users.) Also, the precise criteria for dropping pages from the nationalized search indices are completely unclear. Who decides what page is labelled as Nazi-like or neo-Nazi? On what grounds?[27] And what are the chances that these pages, after due process, would be deemed on the verge but acceptable anyway in either Germany, Switzerland or France?

The reason why search engines engage in such censorship is obvious: to prevent lawsuits. The big question for the future is: how far will this local censoring go? Will the universal

25 A summary of the ruling is given in *U.S. Court Releases Yahoo! Inc. From Compliance With French Court Order* <http://www.ffhsj.com/bancmail/pdf/011120.pdf>. For a more elaborate description, see Christiane Hardy and Karin Spaink, op. cit.

26 Jonathan Zittrain and Benjamin Edelman from Harvard Law School have investigated Google at large and discovered that Google has dropped 113 sites, in whole or in part, from its localized version for French, German and Swiss users (<http://www.google.fr>, <http://www.google.de> and <http://www.google.ch> respectively). See Jonathan Zittrain and Benjamin Edelman, *Localized Google Search Result Exclusions. Statement of Issues and Call for Data* <http://cyber.law.harvard.edu/filtering/google/>. The paper gives a brief overview of other attempts to censor search engines.

27 Zittrain and Edelman stress (op. cit.) that while 'many such sites seem to offer Neo-Nazi, white supremacy, or other content objectionable or illegal in France and Germany, [..] other affected sites are more difficult to cleanly categorize.'

index – in this case, the one at google.com, remain generally accessible? And if not, will other – by then more daring – search engines supplant them?

New Monopolies: Connectivity/Bandwidth. So far, we have looked at new ways of distributing and new methods of censorship. Another important issue is ownership.

Many media watchdogs are worried about concentration of ownership leading to media monopolies; the Italian case (Berlusconi) springs to mind. However, there is no similar worry over monopolies on the Internet.

In some countries, access to the Net is completely controlled by the government. In China for instance, one needs to register before one can buy a modem; in some countries, the only body providing Internet access is the government-owned telco. In countries where such a monopoly exists, it is comparatively easy to censor users: since the government controls access, it can restrict users or impose a national proxy blocking specific pages (Saudi Arabia, Dubai, and Singapore all do this).

In industrialized Western countries, monopolies are on the rise. While a country may have many ISPs providing Internet access, the ISPs themselves need to buy bandwidth and connectivity from so-called upstream providers. These upstream providers in turn have their own upstream providers where they buy bandwidth and connectivity. Worldwide, that specific market is owned by four or five companies.

If you follow the line upwards in Sweden, you will discover that all ISPs depend for their bandwidth and connectivity upon one single US-based multinational: MCI/Worldcom. In an infamous case where a user's page repeatedly garnered complaints and the user's provider, Flashback, refused to block the page – the prosecutor had investigated the page

earlier and found it legal – a complainant went to Flashback's upstream provider, who then decided to block the whole of Flashback. When Flashback tried to buy connectivity and bandwidth elsewhere they discovered that MCI/Worldcom was the final upstream provider in the whole country – and MCI/Worldcom had told all their clients to refuse Flashback. All this happened over one single user's page that the prosecutor had deemed legal.[28]

Currently, wireless Internet is on the rise.[29] Wireless Internet operates in an unregulated and unlicensed band of spectrum, that is shared and available for use by anyone. Until now it was most commonly used for personal appliances, such as for a microwave oven, or a cordless home phone, and even for the radar 'gun' used by law enforcement to read the speed of a moving vehicle.

Unlike today's wired network, a wireless network requires little more than an access point (abbreviated as AP). Access to a wireless-based service doesn't require an expensive connection to each user – there is no need for running wires to each building, or for the installation of a satellite dish. Wireless technology is also far less expensive to deploy than the limited wireless technologies of existing cellular service providers. And, because in most countries it operates in an unregulated spectrum, anyone can deploy a wireless access point. Basically, a wireless access point is nothing less than a broadband network.

---

28 Flashback <http://www.flashback.se> is currently up again, but now only as a news agency; it has abolished its user pages. A list of news articles about the shutdown is available through Flashback's mirror at <http://fb.provocation.net/www.flashback.se/>. The case is described in detail in Christiane Hardy and Karin Spaink, op. cit.

29 The following description is taken from Alan Levy, *Matching new wifi technology with virtual private networks to create affordable universal internet access* <http://www.developmentgateway.org/ict/dg-contribute/item-detail?item_id=272929>

Wireless connectivity might in the near future become one of the prime means of offering connectivity to countries lacking a telephone or cable infrastructure. There are great concerns that the big 'players' in the connectivity market will attempt to block this development, fearing that wireless connectivity will lose them part of the market (a part which they themselves have not yet deemed interesting enough to explore).

.

What is Journalism and Who Qualifies as a Journalist?
One last question to ponder is what, in this post-Gutenberg era, qualifies as journalism and who as a journalist. This question is of special importance for the OSCE Office of the Representative on Freedom of the Media (FOM), since some of its tasks are to provide early warning on censorship and other violations of freedom of expression, to respond to obstruction of media activities and to act against unfavourable working conditions for journalists.

It used to be rather straightforward: journalism was what the media engaged in, and a journalist was anybody who would work for such a medium. With the rise of the Net, that definition has become too strict. After all, one need no longer be employed by a radio or television station, magazine or newspaper. Any individual with Internet access can start a news magazine of his own – he is suddenly equipped with a Gutenberg press and a distribution centre.

While people making a website about their private hobby – collecting stamps, or gossiping about pop idols – are not likely to be put through any political hassle, there is nothing to say that others, who engage in more political content, will not suffer the same repression that 'classic' journalists experience. And if they do, there is no reason whatsoever to withhold from them the kind of support that their colleagues

working for traditional media hope to get from the OSCE/FOM. In fact, they might need it all the more, because there are not many organizations standing up for them.

Apart from that, Internet journalists increasingly face a new problem. Several governments – Italy, Spain, Turkey; and Finland is proposing to do the same – have imposed existing media laws upon Internet publications, demanding that each and every website owner registers himself and informs a designated authority of any updates or changes, a demand which is clearly impossible to live up to on the Net.[30] Until now, laws like this have only been called upon to penalize websites and Internet journalists that do not concur with official policies.

Conclusions and Recommendations. The rise of the Internet creates all new kinds of questions pertaining to freedom of the media and the freedom to access media. A number of questions have been discussed in this article, yet there are still questions that haven't even been touched upon here. How are texts distributed and accessed nowadays? Will ownership of texts (copyright) remain the same?[31] What is the position and meaning of Internet journalism, as opposed to broadcasted or

30 For Italy, see Manlio Cammarata, 'Qui succede un "quarantotto"', *Interlex* , 4 April 2001 <http://www.interlex.it/stampa/48.htm> and Snafu, *Re: <nettime> Indymedia Italy under Attack* <http://amsterdam.nettime.org/Lists-Archives/nettime-l-0202/msg00109.html>. For Spain, see Julia Scheeres, 'Fears of a Website Inquisition', *Wired*, 29 May 2001 <http://www.wired.com/news/business/0,1367,44110,00.html> and Steve Kettmann, 'Spanish Web Law Sparks Debate', *Wired*, 1 May 2002 <http://www.wired.com/news/print/0,1294,52201,00.html>. For Turkey, see Kemal Altintas, Tolga Aydin, and Varol Akman, 'Censoring the Internet: The Situation in Turkey', published in *First Monday* <http://www.firstmonday.org/issues/issue7_6/altinta/index.html>. For Finland, see Electronic Frontier Finland, *Freedom of Expression: The Law on Liabilities in Public Communications* <http://www.effi.org/sananvapaus/index.en.html>

31 For that question, see Jennifer Jenkins's contribution to the 30 November 2002 OSCE Vienna Workshop, 'The Importance of Public Domain for Creativity, Innovation and Culture in the Digital Age', in this publication, 73-83.

written journalism? How are media laws applied to the Net? What exactly is censorship in a post-Gutenberg epoch, and what do media monopolies look like?

In answering these questions we should at least take the following points into account:

1. Censorship on the Net does not merely copy censorship of the classic or traditional media: it is more diffuse, less centralized, more widespread, and far less tangible than older forms of censorship, and it is becoming more and more common in industrialized countries, e.g. regarding content filtering and limiting or denying bandwidth.
2. The implementation of censorship is slowly being delegated from governments to the Internet industry, whereby the latter is given quite a power to wield over citizens' (constitutional) rights.
3. The face of journalism is changing. People who are persecuted over their web pages need our support just as much as people who are prosecuted over their work in the traditional media. After all, one type of journalism merits as much protection as the other.
4. The political risks of Internet monopolies need to be taken into account, and varied means of access need to be promoted and supported.
5. Finally, we need to take into account the vulnerability of certain pivotal services on the Net, above all that of search engines, and support them when they are under siege.

Verena Metze-Mangold

Universal Access to Cyberspace: Strategies of the Intergovernmental Council of the Information for All Programme (IFAP/UNESCO)

The Internet has become a key instrument for the exercise of the right to freedom of expression and freedom of the media. This is reason enough to raise the following questions: Who has access to the Internet? What kind of access – universal? conditional? What are the limitations and exceptions for having access? Who is ruling the developments of our virtual environment? There is no Cyberspace Convention. What we have on an international scale are some international standards for technology exercised by the International Telecommunication Union (ITU), copyright treaties of the World Intellectual Property Organization (WIPO) and an economic regime of the World Trade Organization (WTO). What is at stake at the level of the UN system and especially the UNESCO?

The Internet is:

- the one digital platform in the twenty-first century for all traditional media, which in communication theory has been called 'point to multipoint communication' or more simply 'one to many';
- the medium of personal or group communication, so-called 'point to point communication' or 'peer-to-peer' exchange.

With this potential it serves a multitude of functions: the functions of personal research and information; the function of publishing; the function of communication – be it for private

purposes or for the exchange of scientific knowledge; the function of political communication; and the business functions Business to Business (B2B) and Business to Consumer (B2C).

The Right to Freedom of Expression. Freedom of the media is enshrined in the Universal Declaration of Human Rights (1948) in Article 19 and Article 27: the freedom of information and the freedom of culture. This has recently been underpinned by The Universal Declaration of Cultural Diversity which was acclaimed unanimously at the General Conference of UNESCO in November 2001.

Article 19

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

Article 27

> (1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.
>
> (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary and artistic production of which he is the author.

As with all human rights these rights underlie freedom from discrimination: everyone is entitled to all rights and freedoms – without distinction of any kind. We speak today of the human right to read, the right to write information and the right to communicate on a global scale. However, the reality is different.

Who has Access to the Internet? Any aim lies in walking distance, given that we have enough energy and enough time. But we lack time in our rapidly developing world, and the

uneven pace of development is a key characteristic of our era. Today it is estimated that up to 90 per cent of the world population does not have access to the Net.

The report of the Enquete Commission of the German Parliament on Globalization of the World Economy (2002)[1] states the same as the United Nations Conference on Trade and Development (UNCTAD) report of 2001[2]. While the social and economic importance of access to information is growing, the discrepancy between the 'Information Haves' and the 'Information Have-Nots' has enlarged on a global scale. The digital divide of today could possibly be the social divide of tomorrow (which would create an enormous problem for migration).

This is not a question of technical access alone, for example telephone and Internet connections. It is a question of energy supply and of tariffs – the use of the Internet is correlated to the costs of access.[3] Whilst the telecommunication markets in the Third World are mostly in the hands of state monopolies, the infrastructure of connectivity and the knots of the Web lie in the hands of the West. Cable and satellite lines are directed to and often via the Western world. This adds up to an enormous loss of telecommunication income in developing countries. The average cost of access is 75 dollars per month in Africa, compared with 10 dollars a month in the USA. Naturally the difference is much bigger if we correlate these figures with average income.

---

1 Deutscher Bundestag (ed.), *Globalisierung der Weltwirtschaft. Schlussbericht der Enquete-Kommission* (Opladen, 2002).

2 UNCTAD, *Trade and Development Report 2002* (New York, Geneva: UNCTAD, 2002).

3 ILO (2001 b), *World Employment Report 2001. Life at Work in the Information Economy* (Geneva: ILO, 2001), 17. See also ILO (2001 a), *Report of the Working Party on the Social Dimension of Globalisation* (Geneva: ILO, 2001).

Seventy per cent of websites are American, 80 per cent of Net content is in English; between 5 to 10 per cent of content comes from non-Western countries – although the developing world makes up 80 per cent of the world population. Last but not least there is the question of human capacity. Of course education standards in the regions of the world are – to put it mildly – different. This applies also to media education and the standard of programmes and services used in education that are geared towards people's needs and circumstances. For example, where do people learn the meaning of information autonomy?

These figures may be decisive factors behind the possible pace of access growth in the world. However, they are arguably not the most important reasons for limitations on access.

There are Further Limitations on Access to the Net: There are constraints in the dynamics of the interrelated world which are more complicated to understand. Information and communication (I&C) are considered to be necessary factors of democratic societies. In the twenty-first century, however, they are more than that. They are key elements of the knowledge society and make up the future wealth of a society. I&C are still the source of public opinion. But at the same time they have undergone a rapid change in function and are regarded more and more as commercial products – goods and services – as well as being the subject of attention so as to be taken out in patents or included in proprietary systems. Therefore the aforementioned report of the Enquete Commission does not just speak of the need to define rules and regulations for the new 'social room', cyberspace, by following the old principle of what is right in the offline world must be right in the online world. Instead, it states that a change of paradigm is needed. The report votes that information, knowledge, and technology should themselves become the subject of law considerations,

in order to regulate the development of an inclusive and equitable knowledge society.

At least three sectors are included in this debate. In all of these sectors, the task could be defined as a new balance between private and public concerns:

1) **Access to information and the constraints built into technologies**
   This applies to hardware, software and the architecture of the Net[4]. Who decides upon these codes and this architecture? Do we even think about it?

2) **Access to information and privacy**
   The notion of the banalization of time and geography might be banal itself. However, as the regulating power of the national state diminishes whilst warlord and terrorist power grows, we notice not only constraints on privacy from the state but also a change in public opinion. People seem to be prepared to exchange freedom for security. And not only that. The Net has an 'open' architecture and allows the reconstruction and representation of our behaviour and habits – the reconstruction of our digital shadow as we call it in Germany. Having such an infrastructure in our so-called 'economy of the attention span' means that the misuse of freedom is programmed; and all of us know that it is the misuse of freedom that always endangers freedom.

3) **Access to information and developments in the field of international copyright and Digital Rights Management**
   The developments endanger, or at least change, the principle of fair use. It can be explained perhaps as a result of

4 Lawrence Lessig, 'Cyberspace's Architectural Constitution', lecture given at Amsterdam, the Netherlands, manuscript dated 12 June 2000; Lawrence Lessig, 'Architecting for Control', keynote given at the Internet Political Economy Forum, Cambridge Review of International Affairs, manuscript, 11 May 2000.

'Napsterization' – the file sharing culture in peer-to-peer communication – which has led to access to information becoming more and more constrained by enlarged proprietary systems. Copyright and patent law have been enforced, prolonged, enlarged and applied on new subjects such as designs, composition of smells or colours and especially on collections of information in databanks. The amount of trademark patents is one of the criteria of benchmarking an economic region and is therefore given a great deal of attention in the process of global competition. Ninety-seven per cent of all patents are held by industrial countries (TRIPS GATS[5]/ Universal Declaration of Cultural Diversity[6]). The knowledge economy is growing strongly and on the international scale is distinctly imbalanced. This results in massive concentration of media and information ownership (which even touches on the freedom of scientists) and new forms of inequality of access to knowledge.

Who is Regulating the Internet? To understand the Internet we have to see it not just as another transport or communication instrument. Instead we have to see it as our 'electronic environment' in which we probably spend more time than in the fields and woods. We should think about principles and criteria which could be applied to this virtual environment in the process of creating our future world – comparable perhaps to the question of biodiversity. If we do think about it, we would perhaps rather see the need for an 'Agenda 21' for our virtual information environment than an Article 19 alone.

This puts forward the question of who is regulating? How is it done? By mastering information through knowledge and reflection? If we reflect we recall that there are interrelations. There is an interrelation between the biodiversity of a

society and its cultural diversity. In other words: we know that liberalization of markets can release inventions and innovative forces and thus foster developing processes. On the other hand, we know that the liberalization of the telecommunications market brought an enormous wave of mergers and concentration of market power – the opposite of diversity. 'Globalization and uniformity,' wrote a media magazine, 'is generated in a market, which is not concerned with questions of sense.' Economists know the notion of 'meritorious goods and services', and they apply this notion to goods whose social value is more important than their market value.

Who or what is regulating them? The answers of political scientists are the law, the market, codes (e.g. technology) and the norms of civil society.[7] This multi-level system of steering must be seen in the national and international context. In this multi-level system, the state has quite a difficult role, or, to be more precise, different roles. The state is guarantor of basic rights, and legislator; thus it structures the legal framework for development. The state is the supervisor of regulative frameworks with self-regulative elements. It decides on technological infrastructure, insofar as the state is a 'global player' itself and in the role of a competitor on the global market. Nevertheless, in the process of globalization and the debate about the norms of our global system, the nation-state has seemingly gone through a renaissance and has come back to a central position. It has to sign international conventions and treaties,

5 'Members Outline Plans for Accelerating Service Talks', *WTO Reporter*, 30 May 2000.

6 <www.unesco.org> and <http://webworld.unesco.org>

7 Beth Simone Noveck, 'Information Society', keynote speech at Information Cultures and Information Interests (ICII): European Perspectives for the Information Society, UNESCO Regional Pre-Conference for the World Summit on the Information Society (WSIS), 2003; Claus Leggewie and Christa Maar (ed.), *Internet Politik: Von der Zuschauer zur Beteiligungsdemokratie* (Cologne, 1998).

devises international law, and the state together with interested parties and civil society is even developing a so-called 'soft law': 'Resolutions and Declarations'. It is interesting to see how the state is handling its contradictory situation regarding universal access. Before we come to that we have to clarify what universal access means.

The Basic Texts and Social Meaning. Universal access to cyberspace can be understood as the possible solution to the buzzword of the new millennium: the digital divide. Providing access to information (for all) has been a major concern for many international organizations in the last 50 years, expressed directly or indirectly in numerous declarations, recommendations, resolutions, statements, and national and international programmes. This is true of the Universal Declaration of Human Rights (1948), renewed in the United Nations Millennium Declaration of 2000; the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe (1950), renewed and updated in 1998; for the Okinawa Charter on the Global Information Society of the G8 countries (2000); and the Action Plan of the G8 DOT Force 2002; the Task Force of ECOSOC; not to mention the European Union Charter of Fundamental Rights in 2000, among many others.

The term 'universal access' has diverse meanings:

Access to information is a freedom

The 'freedoms' can be classified as follows[8]:

- freedom for individuals to access information held on them
- freedom to access general information in the public sector
- freedom to access general information in the private sector

The contrary notions of general freedom of access consist of:

- safeguarding the privacy of information held on individuals from access by others

- confidentiality of information held by institutions including commercial confidentiality
- protection of intellectual property rights
- the blocking of access to 'undesirable' material on the Net.

This covers denial of access to personal data by unauthorized third parties, restricted general access for good reason in the public sector and from the Web, and the need for commercial and industrial or political secrecy.

Despite significant differences in interpretation of the basic texts due to cultural diversity and heterogeneous political interests, they are considered the programmatic ethical foundations of modern societies. Among the commonly agreed-on values is the free access to information (which does not necessarily mean free of charge, but free of restrictions) – because benefits arise from publicly produced and distributed knowledge. It is considered the major means to compensate otherwise existing deficiencies, to further equality both on a micro (individual) and on a macro level (between nations or regions), and to promote the establishment and development of democratic societal structures.

Support measures for the production of knowledge and for its distribution, for access to knowledge and information which are in addition financed by the public, are generally considered society's investment in the future. Therefore, to achieve the central goal of equal chances in democratic societies, public support for the production of knowledge and for the dissemination of information, by access to information, has for a long time never been questioned in principle, even

8 Les Neal, The British Computer Society Ethics Committee 'Freedom of Access to Information' <http://www.bcs.org. uk/ethics/freedom.htm>

in market-dominated societies where privatization and commercialization of knowledge and information have led to the current dominance of commercial information markets. There has been no doubt that there is still a need for a second 'market', which should perhaps instead be called a 'forum' for the public and not a commercial exchange of knowledge. This idea can be found in our schools, in public libraries, in public broadcasting systems.[9] Today this idea is being questioned by the rules and modes of the GATS Regime, the General Agreement on Trade in Services of the World Trade Organization (WTO). The GATS Doha Round (2000-2005) focuses on trades and services in education, culture, and audiovision.

What is at Stake in the UN system? The UN must consider themselves as 'catalysts of change', said Kofi Annan when he presented the UN Millennium Declaration, and he continued: 'As catalysts of change whose effects do not result from the exercise of power but from the exercise of values and global norms.'

UNESCO, the UN's special organization for education, science, culture and communication, is more than other intergovernmental institutions open to civil society, to NGOs and special stakeholders – as in our case journalists and the media industry. With regard to the information and communication programme of UNESCO, the year of paradigm change was 1996. Until then, the leading idea had been that the social and economic inclusion of developing countries would be a result of the market – a belief which was expressed in a similar way in the former Washington Consensus. However, in 1996 the Executive Council of UNESCO stated that the new technologies of connectivity bear enormous potential for development in all fields of UNESCO's mandate – education, science, culture, and communication. 'But the only effect until now,' stated the Executive Council in 1996, 'has been a widening gap.'

The Draft Recommendation on Multilingualism and Universal Access to Cyberspace. In 1997 the 29th session of the General Conference debated on a 'Preliminary report by the Director General on the feasibility of an international instrument for the establishment of a legal framework relating to cyberspace and of a recommendation on the preservation of a balanced use of languages in cyberspace.' Almost every country will experience the need for an international legal environment, the report said. This means that a tighter fabric of international norms needs to be woven, expanding the rule of law worldwide and enabling citizens to exert their democratic influence on global processes. The report noted that the field was marked by numerous divergences of interest. 'The rights of users and universal access to information are fundamental to this process. Essential values such as freedom of expression, respect for the "public good" and protection of privacy should also be strengthened so as to promote democracy.' 'Where the opening-up of new frontiers has created new legal requirements there is no lack of precedents for the framing of a *ius novum*. Recent examples are the Outer Space Law and the Law of the Sea.'

'Such an international instrument in the form of a convention might be legally binding. It could also have the form of a declaration, proclaiming moral commitments with no binding legal effect. In this respect, international law and practice demonstrate that a resolution or a declaration preceded almost every international convention prepared by the United Nations. The progressive development of international law moreover recognizes the binding legal nature of *soft law* under particular

9 Rainer Kuhlen, 'UNESCO Activities in Communication and Information – Programmes and Recommendations, Chancen und Risiken globaler Vernetzung', keynote speech at the international seminar at 'Amerikahaus Berlin', Berlin, 21 and 22 February 2002.

circumstances, e.g. the Universal Declaration of Human Rights, to cite but one instance. In order to avoid administrative and procedural constraints, it might be feasible to begin by preparing a draft declaration on a basis of a set of commonly agreed guidelines and principles to be discussed by UNESCO governing bodies and subsequently submitted to the United Nations General Assembly. Following approval of the draft declaration by the UNESCO governing bodies, steps could be taken to examine the feasibility of preparing a specifically binding international instrument with its own supervisory mechanism in order to strengthen existing international instruments.'

The Info-Ethics Expert Conferences. In 2001, after a series of expert conferences on Info-Ethics (1998-2000), the General Conference had to decide on a Draft Recommendation for the Promotion and Use of Multilingualism and Universal Access to Cyberspace.

UN World Summit on Information Society. The 'Recommendation Concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace' was originally intended to become the conceptual basis for UNESCO participation in the UN World Summit on the Information Society, which will take place in 2003 under the leadership of ITU. 'Universal access' in this context is defined 'as equitable and affordable access by all citizens to information infrastructure and to information and knowledge essential to collective and individual human development.' The preamble of this recommendation also claims, 'that one of the ultimate goals of any society is empowerment of all its citizens through access and use of knowledge.' 'Universal access to information and communication technologies and particularly to global information

networks is essential for achieving goals of social cohesion and economic inclusion.' Well said. Nevertheless, the recommendation ultimately failed to be adopted by the 2001 UNESCO General Conference.

According to the report of the German delegation there are several reasons for the failure of the recommendation: The demand for 'a new fair balance between the interests of authors and publishers and those of the public concerning free access to information' was not accepted by the majority of members. And the request that 'member states and UNESCO should defend the principle of universal access against attempts to strengthen intellectual property rights through technological means such as digital rights management' was obviously against current worldwide trends in legislation as expressed in the WIPO 1996 treaties, the US Digital Millennium Copyright Act, and, in particular, the Directive of the European Commission on the Harmonization of Copyright from 5/2001 (Article 6), where technical means are clearly favoured to protect copyrights on intellectual property which is controlled by private interests.

'Information for All' Council and Programme. The year 2002 saw the publication of the completed action plan of the Okinawa DOT Force – without any further consequences. In addition, that year saw the establishment of the first intergovernmental body dealing with 'Information for All' (IFA/IFAP) – a council and a programme with the very same name. Whereas statements of and reports on conferences are an easier way to reach consensus, it is more difficult to achieve the necessary majority for UNESCO official decisions such as those on new programmes or on official recommendations or even conventions. Therefore it is all the more remarkable that

UNESCO has agreed, after a long period of intensive discussion, on the new IFA intergovernmental programme which, by nature of its title, was provocative for some members, in particular for lobbying groups from the information economy. IFA, by name, is a programme for access to information for all. It is based on the UNESCO constitution. Therefore 'UNESCO's mandate "to promote the free flow of ideas by word and image" (Article 1) clearly indicates the part that the Organization is called upon to play in making information and knowledge freely accessible to all, with the ultimate objective of bridging the gap between the information rich and the information poor' (preamble). IFA thematicizes the challenge of the modern information society where 'new methods for accessing, processing and preserving information raise problems of an ethical nature, which in turn create moral responsibilities, to which the international community must respond. Among the issues here are the quality, reliability and diversity of information, the balance between free access to information, fair use and protection of intellectual property rights, the privatization of information, the preservation of the world's information heritage and the privacy and security of personal data.'[10]

The Intergovernmental Council Information for All (IFA) is well aware that the objectives to 'promote and widen access (to knowledge) through the organization, digitization and preservation of information' can only be achieved by new forms of partnership. 'Collaboration with stakeholder NGOs and the private sector shall be established in order to create a multiplier effect from improved communication and collaboration to contribute to achieving the objectives of the Programme.' As concrete means for supporting free access, the IFA recommends 'strengthening institutions as gateways for information access', in particular establishing a 'UNESCO portal to

information institutions worldwide' and also 'national public gateways to information in several countries of all regions' (from area 3 of the programme).

The IFA recommends the following strategies:

- Move towards a redefinition of the role of information institutions
- Extend the role of established professional and institutional infrastructures such as libraries, archives, community centres etc.
- Promote the creation of new information institutions, particularly local gateways to information
- Create awareness of the importance of the complementarities between institutions providing access to non-digital and digital information
- Promote the creation of digital content by information institutions
- Promote international co-operation through networking among professional communities/associations
- Promote co-operation between public information institutions and the private sector (in particular content providers)
- Greater use of technology by information institutions for information preservation.

And as concrete action it recommends:

- Analyse and report on the changing role of information institutions in the information society
- Support the implementation of technology and professional standards for the management and preservation of physical collections of information
- Support the creation of public gateways to information, particularly in developing countries

10 Rainer Kuhlen, op. cit.

- Support the networking of institutions to provide access to information resources
- Support the digitization of information, particularly indigenous knowledge useful to local communities
- Foster co-operation with the information industry to develop formulas for providing equitable access for economically disadvantaged users
- Support resource-sharing of digital and non-digital resources
- Encourage and support the use of ICT to manage and preserve information resources.

Information Cultures and Information Interests (ICII Resolution). In 2002 the UNESCO European Pre-conference to the World Summit on the Information Society in 2003 in Geneva, whose host was the German Commission for UNESCO, adopted a resolution[11] which underpins the urgency of these issues, being convinced that the summit should not fall victim to the mere technical problems of the digital divide. At the second preparatory conference, the so-called PrepCom in Geneva in March 2003, the summit agenda will be decided upon. Moreover, the 32nd UNESCO General Conference will also take place this year in October 2003.

The revised draft of the Cyberspace Recommendation and the Executive Board's comments thereon will be presented to the General Conference at its 32nd session. The procedure of drafting the new version of the recommendation was somewhat surprising. At least two different groups of experts had been invited by the General Director to work on the recommendation and that changed the result. The articles relating to copyright have been turned upside down. There was pressure from the information economy, especially the copyright industry. Since the draft has passed the Executive

Council this October it will not change again. Notwithstanding, during the last General Conference in November 2001 another declaration had been adopted.

The Universal Declaration on Cultural Diversity. While the filing of the Cyberspace Recommendation was going on for six years, parallel to this a declaration has been in the process of drafting since the World Culture Conference in Stockholm five years ago. It was adopted just one year ago. In the action plan, the member states are asked to pursue national policies of cultural and media diversity. Moreover the declaration asks member states, after having agreed on this 'normative instrument', to decide whether it is necessary to work on a legal instrument.

Meanwhile we see several lines of activity on a multilateral level in Europe. The Assembly of the European Council recommends that the Committee of Ministers:

1) Joins forces with other international bodies that are currently considering access to digital material on the Internet in order to develop norms for the fair use of such material for educational and other socially relevant purposes and
2) Ensures that such norms are applied in member states (June 2002).

The European Regional Ministers for Culture and Education unanimously adopted the Brixen Declaration on Cultural Diversity and GATS during the Assembly of European Regions on 18 October 2002. The declaration reads: 'We fully concur with the recognition as expressed in the Universal Declaration on Cultural Diversity ... that cultural diversity is as necessary for humankind as biodiversity is for nature and that policies to promote and protect cultural diversity thus are

11 <www.unesco.de>

an integral part of sustainable development; that cultural goods and services which, as vectors of identity, values and meaning must not be treated as mere commodities or consumer goods and that cultural and audiovisual policies, which promote and respect cultural diversity, are a necessary complement to trade policies.' (Article 16)

'We have to acknowledge with regret,' the ministers state in Article 6, 'that the decision to include educational, cultural and media services as a constituent and integral part of the General Agreement on Trade in Services (GATS) has been taken without in-depth information or full consultation of the wider public. It has been without real parliamentary deliberations in national parliaments and, to a large extent, without reference to regional governments although constitutionally demanded where there are exclusive or mixed legislative competences, for culture, education and media.'[12]

The Canadian Minister for Culture proposed a protocol to the GATS treaty referring to the Declaration on Cultural Diversity, thus importing universal norms and values to the economic regime of the WTO.

Social scientists agreed on a working platform to set up a 'Charter for Cyberspace'.[13] The catalyst function seems to work. But the development of the widening gap has – to this day – not been halted. The World Summit on the Information Society is *ante portas*: 2003 in Geneva and 2005 in Tunis.

12 <secretariat@a-e-r.org>

13 Initiative 'Charter on Sustainable Knowledge Societies' <http:\\www.worldsummit2003.org>

Páll Thórhallsson

Freedom of the Media and the Internet

The new information and communication technologies offer unprecedented possibilities for individual and group expression and for an increased participation of individuals in public affairs. The Council of Europe is convinced that an active policy co-ordinated at the international level is needed to maximize the benefits of the new information and communication technologies and ensure that freedom of expression and information as well as other human rights and fundamental values are fully respected. In this paper, I will try and highlight some issues in this field where the Council of Europe thinks that there may be a need for internationally co-ordinated work.

The Council of Europe is in favour of developing a vision of the information society which gives priority to human rights, in particular freedom of expression and information, and the opportunities of empowering citizens to take a more active part in democratic society. At the same time, other human rights and fundamental values such as human dignity and privacy must be fully guaranteed. Public policy objectives, such as the efficiency of government services and network security, should be seen as serving this higher goal.[1]

Means should be sought to guarantee the fullest respect for freedom of expression and information in the future information society. Individual participation and the use of new

1 See Council of Europe contribution to the World Summit on the Information Society <http://www.humanrights.coe.int>

information and communication technologies should be encouraged through public policy and protected by legal means with independent courts being the ultimate guarantor of individual rights. Public authorities should develop innovative strategies to increase transparency and make public information available with the help of the new technologies in a neutral, comprehensive and easily accessible manner, allowing enhanced public control over and active participation in public affairs. The Council of Europe has launched a work on defining common standards for e-governance which will focus on giving citizens increased possibilities of interaction with public authorities and allowing more active participation between elections. A recent Council of Europe Recommendation on access to official documents pursues also the same aim of ensuring more transparency of government.[2]

Freedom of expression and information has to co-exist with other fundamental rights and values. Legal frameworks, necessary as they are, must be designed in such a manner that any restrictions on this freedom serve legitimate purposes and do not go beyond what is necessary in a democratic society. In particular, they should not go further than what has been generally accepted at the international level regarding traditional offline communications. On the European continent, this refers first and foremost to Article 10 of the European Convention on Human Rights and the relevant case law of the European Court of Human Rights.

Enhanced international co-operation is necessary, *inter alia*, to define common standards on content matters and on liability of both primary actors and intermediaries, and to find responses to questions of jurisdiction and applicable law. Illegal content should be marginalized and any safe havens for illegal activity closed through international pressure. The recently

adopted Council of Europe Cybercrime Convention[3] responds to this need. The parties to the Convention and its additional protocol agree that certain content should be considered criminal, namely breaking into computer systems, child pornography, racist speech, and piracy of content protected by copyright. The Convention, furthermore, provides for international co-operation in combating criminal activity in cyberspace.

International co-operation should also involve the industry, which should be encouraged to develop codes of conduct and self-regulatory schemes. This co-operation is also essential to guarantee the protection of minors against content which is not strictly illegal, but may be harmful and detrimental to their personal development, in an environment where traditional ways of controlling access (for example watershed rules) do not work.[4]

Coming back to the main topic of this paper, it is obvious that the new information and communication technologies are not an end in themselves, but a means of supplying, accessing and preserving information and content. The danger exists that genuine information will be more and more difficult to find in the plethora of communications. It may also become increasingly difficult to distinguish between credible and valuable information and pseudo-knowledge or other communications which serve propaganda or advertising purposes. The Council of Europe has started working on defining the role of the media in promoting democracy in the information age. In a draft position paper, made public in December

2 Recommendation (2002) 2 on access to official documents <http://www.humanrights.coe.int/media>

3 See <http://conventions.coe.int/>

4 See Council of Europe Recommendation (2002) 8 on self-regulation concerning cyber content <http://www.humanrights.coe.int/media>. The site also contains information about self-regulatory initiatives in several European countries.

2002[5], it is stated that one of the roles of the media has traditionally been to provide the general public with information about the activities of public authorities. Increasingly, however, such information is made directly available to the general public on official websites. This is at first sight a positive development serving the right of the public to access information. The question arises, however, of what role remains for the media? Once, they used to be a unique link between public authorities and the citizen, while now they may become marginalized.

It seems obvious that the media should continue to extract information from the public sector, since there is no guarantee that the information provided by public authorities on their own initiative is objective and exhaustive. Furthermore, it may be argued that the amount of available information makes 'filtering' and interpretation even more necessary than before. No one seems to be better placed than independent media to correct misleading official information. The media should therefore, it may be argued, act as an independent observer of public authorities and their information policy, highlighting what is really newsworthy and criticizing what could be done better.

It is commonplace to say that the media reflect public opinion. New technical possibilities allow the media to collect the views of the public in a much more direct way than before. Conducting an online vote with the help of the Internet is technically fairly easy and many online media invite the public to voice their opinion on certain topics, for example by simply clicking a 'yes' or 'no' button in answer to particular questions. The question arises, however, whether the media should develop guidelines on how to conduct and present the results of such online votes. For the sake of fairness and transparency,

the media might, for example, provide information on the composition of the sample which would allow the audience to judge to what extent it is representative.[6] Furthermore, it might be interesting to know if the media present the results of such votes to decision-makers, requesting a reaction.

There is nothing new about the fact that the media offer the public the possibility of engaging in a discussion about public affairs. This has been done in the past in the form of letters to the editor, talkshows on radio and television, etc. New technologies open up new possibilities in this respect. Many online media invite readers to comment on stories or to provide input in chat-sessions or discussion fora on topical issues. Several questions can be raised in this respect. Firstly, whether the media should issue any guidelines to participants in online debates regarding respect for the law and ethical principles. Secondly, whether the debates should be moderated and, in the affirmative, whether they should be premoderated or postmoderated.[7] Premoderation may, in particular, be necessary when sensitive topics are being discussed[8] or where children are encouraged to take part. Thirdly, whether participants should be allowed to hide their identity.

---

5 See <http://www.humanrights.coe.int/media>: 'Outline position paper on the role of the media in promoting democracy and participation in the information society.'

6 The BBC Online Editorial Guidelines <http://www.bbc.co.uk/info/online/> state that care has to be taken that online expressions of opinion are not translated into anything that could be construed as an accurate representation of public opinion as a whole.

7 'Premoderation is where material cannot be accessed by visitors to the site until the moderator has seen it and decided it is suitable for placing on the Internet. Postmoderation is where the moderator sees the material, and decides whether it is suitable to remain on the site, after it has been posted.' (quoted from the BBC Online Editorial Guidelines).

8 The French newspaper *Le Monde* announces, for example, on its website that the online debate on the Middle East is premoderated, see <http://forums.lemonde.fr/>

In addition to these questions, which the media will first and foremost decide for themselves, there is the issue of legal responsibility for the content of online debates.[9]

Over and above these issues, which are immediately linked to the organization of online debates, there is the question of what is done with the results. Is there an attempt by the media to draw conclusions from such debates and present them to decision-makers? This might add a new sense and increased importance to participation in the debate.

The media may also have an important role to play in promoting democratic practices. This can be done, for example, by encouraging participation in elections and referenda and devoting special attention to such democratic processes. This could also involve providing information to voters about the democratic system that they belong to. In the context of the information society, this would mean that the media follow closely new developments aimed at increasing democratic participation in decision-making about public affairs. Where no such developments are taking place, the media could inquire why this is the case.

The media may also pay special attention to the phenomenon of diminished interest in public affairs and suggest ways for public authorities and politicians to involve the general public to a greater extent than before. More public interest and involvement will also ultimately be beneficial to the media themselves, at least as regards the sustainability of serious reporting about politics, the economy, etc.

Arguably, the media should pay special attention to the views, concerns and situation of marginalized or excluded parts of society. Such a moral obligation is to be found in many ethical codes and is respected in practice by a large number of media professionals. This may be particularly urgent in the context of the information society, where new forms of social

exclusion may arise. People without access to the Internet or lacking skills in using the Internet may effectively be worse off than before from a democratic point of view.

The bottom line is that independent, professional journalism, adhering to ethical standards, will not be less important in the information society than before. The provision of relevant, timely and well-researched information by media professionals will continue to be essential in laying the foundations of an informed public debate about current affairs and public policy. The necessary conditions for journalists to be able to pursue their scrutiny of the state and other powerful forces in society, providing an indispensable counterbalance, must be maintained. This includes not only legal protection against harassment of a physical or other nature, but also that media organizations create the conditions for journalists to carry out their work properly, despite increased pressure from the market with respect to instant and low-cost provision of information.

Genuine independent public service broadcasting should be recognized as an essential component of the information society, guaranteeing quality information. There is a need for trusted sources of information as a point of reference in a world where the flow of unmediated raw data increases steadily. The multitude of information sources with any particular mass media reaching a lesser part of the population than before, carries furthermore the risk of diminishing social cohesion. Here again, public service broadcasting can play a vital role in creating common frameworks of reference.[10]

---

9 In Finland, a draft law which would clarify questions of liability for content of online bulletin boards is being discussed in Parliament, see <http://www.helsinki-hs.net/news.asp?id=20021216IE5>

10 See Council of Europe Recommendation (1996) 10 on the guarantee of the independence of public service broadcasting <http://www.humanrights.coe.int/media>

Since the means of transmission may be of less relevance than before, consideration should also be given to extending the concept of public service broadcasting to the new communication and information technologies, with a view to developing a new policy of public service communication.

Sandy Starr

The Diminishing Importance of Constitutional Rights in the Internet Age

In this paper, I address two factors which I believe have fundamentally eroded the constitutional rights of Internet users in recent years: the framework of self-regulation, and the framework of human rights. To illustrate the impact that these two factors have had, I conclude with a case study of copyright regulation in Europe.

I. The Framework of Self-Regulation. By self-regulation, I mean any situation where regulation of speech is carried out by a private commercial body, rather than a public statutory body.

At first, this definition seems hopelessly broad – don't all commercial publishers, online and offline, practice benevolent self-regulation simply by deciding not to publish certain things? But self-regulation becomes opposed to constitutional rights, as soon as it is used in the service of state regulatory interests. Constitutional rights can only be defended against the powers of the state, if the state exercises those powers accountably and in the open.

By making everyone with a computer and a connection into a potential publisher, by transcending national boundaries, and by making it difficult to identify the publisher of specific content, the Internet posed an enormous challenge to state regulation when it became widely used in the 1990s.

Self-regulatory regimes, where Internet regulation devolves from accountable arms of the state to unaccountable para-state,

international and industry bodies, are best understood as a defence mechanism in reaction to new technology. With self-regulation, regulation mimics the decentralization that frustrates it.[1]

Organizations such as the Internet Hotline Against Child Pornography in the Netherlands; the Internet Watch Foundation in the UK; the CyberTipline in the USA; and the Australian Broadcasting Authority in Australia differ in their methods and their stated intentions, but they all recommend removal of content either to Internet service providers (ISPs) or directly to content providers, bypassing due process in a court of law.[2]

Perhaps the type of Internet content most subject to self-regulation is child pornography, for the simple reason that whatever country people live in, they tend to find it so appalling that there is little or no objection to whatever method is used to regulate it.

But just because self-regulation is politically and morally expedient, this does not make it constitutionally legitimate. Unfortunately, the impact and consequences of self-regulation are difficult to measure, because self-regulation takes place out of public view. When the regulatory apparatus is exported into the marketplace, it becomes impossible to determine accurately what content is being removed from the Internet, and why.[3]

Therefore, rather than attempting to gauge the statistical impact of Internet self-regulation, I thought it more useful, for the purposes of this paper, to assess the most common justifications for Internet self-regulation. There follow five such justifications, each of which I believe is in fact a fallacy.

Fallacy 1: Self-regulation is constitutionally legitimate

The argument goes that if an independent commercial body voluntarily elects to regulate content that it is responsible for publishing, then that body is not transgressing any constitutional rights. There are two faults in this argument.

First, commercial bodies are not necessarily politically independent. The distinction between an industry consortium pursuing its own interests on the one hand, and a quango pursuing the interests of government at a distance on the other hand, is by no means always clear. Statutory bodies can put pressure on an industry to enforce a particular self-regulatory regime. The Internet Watch Foundation, for instance, was officially established and is funded by industry, but is endorsed by the UK police and by the UK Government's Department of Trade and Industry.

Second, it is not at all evident who should be considered responsible for publishing content on the Internet. Legislation has tended to characterize ISPs as publishers, but this is more a matter of regulatory convenience than of constitutional principle. The category 'publisher' is in many ways completely inappropriate for ISPs, whose relationship to content and to content providers differs significantly from the relationship of a print publisher to content and to content providers.

---

1 This is true not only of self-regulation in relation to the Internet, but of self-regulation as a response to new publishing technology throughout history. See Christopher Hunter, 'A Brief History of Censorship', *Filters and Freedoms 2.0: Free Speech Perspectives on Internet Content Controls*, Electronic Privacy Information Centre (Washington: Electronic Privacy Information Centre, 2001).

2 See the Internet Hotline Against Child Pornography <http://www.meldpunt.org>, Internet Watch Foundation <http://www.iwf.org.uk>, CyberTipline <http://www.missingkids.com/cybertip>, and Australian Broadcasting Authority <http://www.aba.gov.au> websites.

3 Although there have been laudable attempts to gauge the impact of Internet self-regulation. For example, Chris Ellison's paper 'Oppression Net' (in *Economic Affairs*, vol. 20 no. 1, March 2000) reports that in the UK in 1998, 400 times more content was removed from the Internet on the instruction of the Internet Watch Foundation than was removed from the Internet on the instruction of a court of law. There are also ongoing projects to catalogue specific examples of content removal through self-regulation, for example on the websites of the Electronic Frontier Foundation <http://www.eff.org> and the Chilling Effects Clearinghouse <http://www.chillingeffects.org>. And the Electronic Privacy Information Centre documents numerous instances of wrongly filtered content, in its book *Filters and Freedoms 2.0: Free Speech Perspectives on Internet Content Controls*, Electronic Privacy Information Centre (Washington: Electronic Privacy Information Centre, 2001).

Fallacy 2: Self-regulation restricts liberty less than state regulation

The argument goes that self-regulation which is opted for by individual users, such as filtering, is preferable to criminal penalties directly restricting certain kinds of speech.

This argument was most famously endorsed by the American Civil Liberties Union, in its 1997 pamphlet 'Fahrenheit 451.2: Is Cyberspace Burning?', which argued that 'user-based blocking programs...are far preferable to any statute that imposes criminal penalties on online speech'.[4]

But there is a central flaw in this argument, as is pointed out by the US legal theorist Lawrence Lessig. Lessig argues that only when regulatory requirements are 'imposed by the state' can 'these requirements...be tested against the Constitution'. He goes on to explain the dangers of 'non-transparent' regulation: 'If there is speech the government has interest in controlling, then let that control be obvious to the users. Only when regulation is transparent is a political response possible.'[5]

Fallacy 3: Internet users are adequately represented under self-regulation

The argument goes that because an ISP has to abide by the terms and conditions in the contract it signs with its customers, and because there are numerous organizations and campaigns that represent consumer rights, therefore Internet users have adequate representation under self-regulation. There are three faults in this argument.

First, consumer rights are not constitutional rights. Consumer rights merely entitle you to expect good business practice. Constitutional rights, on the other hand, embody universal principles such as free expression.

Second, removal of content from the Internet impacts not only upon the provider of that content, but also upon the

broader culture – upon every other Internet user who might otherwise have read that content, and who probably has no idea it has been removed. Self-regulation has a chilling effect not just upon Internet users in their specific role as content providers and ISP customers, but upon the free speech of Internet users as a whole.

Third, consumer rights activists are by definition self-appointed and unaccountable, presuming to represent the views of a public that never elected them, and often playing to the media. Far from being adequate representatives of users, they tend to be presumptuous opportunists with personal agendas.

Fallacy 4: Self-regulation is morally justified

The argument goes that certain types of content – foremost among them child pornography and hate speech – are so morally repugnant as to justify any form of regulation.

The problem with this argument is that it undermines due process, by assuming that it is incumbent upon all of us to police allegedly illegal content. In truth, only a court of law is qualified to decide the illegality or otherwise of content.

The moral argument is frequently posed in such a way as to erase the distinction between speech and action. It is assumed that speech is directly harmful to its consumers, that speech impels its consumers to perform certain actions, or that speech is equivalent to the abuses it describes and depicts.

Such confusion is, unfortunately, reflected in contemporary law and policy – it is embodied by the very category of 'hate speech', and embodied by laws such as the UK's Criminal Justice and Public Order Act 1994 and the USA's Child

4 American Civil Liberties Union, 'Fahrenheit 451.2: Is Cyberspace Burning?', reproduced in *Filters and Freedoms 2.0: Free Speech Perspectives on Internet Content Controls*, Electronic Privacy Information Centre (Washington: Electronic Privacy Information Centre, 2001), 109.

5 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books), 178-81.

Pornography Prevention Act 1996, both of which equate the creation of artificial images of child abuse with the photographing of genuine acts of child abuse.[6] Nonetheless, the distinction between speech and action remains crucial to the defence of constitutional rights.

Fallacy 5: The legitimacy of self-regulation can be measured by the response to it

The argument goes that if a self-regulatory regime meets with few complaints, then the system must be 'working', and is therefore legitimate.

This argument would have us believe that a system which assumes guilt on the part of content providers, and is ruthlessly efficient at removing content on that basis, without any qualified evaluation of claims, must be legitimate if the content providers never protest their innocence.

But the fact remains that under self-regulation, the presumption of innocence has been reversed. Content providers are forced to operate under permanent threat of content removal, and it is incumbent upon content providers to protest their innocence when content is removed.

Whether content providers actually go to the effort of lodging a complaint, or whether they are simply discouraged from expressing themselves freely thereafter, there is a chilling effect whose full extent cannot be measured. Self-regulation is illegitimate regardless of the response it elicits.

II. The Framework of Human Rights. There's a moral orthodoxy that surrounds the concept of 'human rights' today. European law is predicated on human rights, and human rights are invoked by everyone from government representatives to their most outspoken critics. It is usually assumed that human rights are eternal, morally unimpeachable, and transcend political interests. To criticize human rights is unthinkable.

But in truth, human rights are not eternal or morally unimpeachable. Nor are human rights necessarily coterminous with constitutional rights, or coterminous with any Enlightenment model of universal rights.

The doctrine of 'human rights', as it is understood and applied today, was first conceived by Franklin Roosevelt's administration in the immensely politicized circumstances of the Second World War – before going on to be championed by US representatives at the 1945 United Nations founding conference, and enshrined in the Universal Declaration of Human Rights adopted by the United Nations in 1948.[7]

Since the Second World War, human rights have been put to a multitude of political purposes – ranging from justifying interventionist foreign policy (on the grounds that Western nations have a duty to secure the rights of those in other nations), to consolidating domestic support for political parties ('human rights' is a concept flexible enough to be used to dress up a diverse range of policies as liberal and just).[8]

---

6 The UK's Criminal Justice and Public Order Act 1994 <http://www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm> incorporates revisions to a previous piece of legislation outlawing child pornography, the Protection of Children Act 1978, so that every reference to an 'indecent photograph' in the earlier Act is changed to refer to an 'indecent photograph [or pseudo-photograph]'. The USA's Child Pornography Prevention Act 1996 <http://www.politechbot.com/docs/cppa.text.html> also incorporates revisions to a previous piece of legislation outlawing child pornography, 18 USC 2256(8), so that a depiction of a minor can now be classified as child pornography (and therefore as illegal) where 'such visual depiction has been created, adapted or modified to appear that an "identifiable minor" is engaging in sexually explicit conduct'. ('Identifiable minor' here means identifiable as being a minor, not identifiable as a particular minor.)

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

8 The political (mis)use of human rights is comprehensively documented in Kirsten Sellars, *The Rise and Rise of Human Rights* (Stroud: Sutton Publishing, 2002); and also in David Chandler, *From Kosovo to Kabul: Human Rights and International Intervention* (London: Pluto Press, 2002).

Most problematic, when it comes to the Internet, is the fact that the human rights framework prescribes rights directly, rather than prescribing limits to state power so that rights might be exercised. A prescribed limit to state power can be implemented unambiguously, as it describes a default condition where the state simply does nothing. But a prescribed individual freedom can only be implemented ambiguously, because it describes a default condition in which the state does something, and is restless.

Rights are minutely codified in human rights legislation – not so much in the Universal Declaration, and in the European Convention for the Protection of Human Rights and Fundamental Freedoms, as in subsequent legislation aimed at clarifying the ambiguities that these initial statements of principle throw up. Human rights legislation tends to require perpetual clarification, meaning that it can accommodate compromises that would not be possible if rights were treated more absolutely.

Such accommodation is epitomized by Article 15 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which states that 'in time of war or other public emergency threatening the life of the nation', a government is permitted to 'take measures derogating from its obligations under this Convention'. After the terrorist attacks of 11 September 2001, Article 15 became the pretext for emergency government powers in the UK, whereby suspected terrorists could be detained without trial.

Civil liberties campaigners have challenged these emergency government powers in the UK, but since it's difficult to arrive at a clear definition of a 'threat to the life of a nation', the debate hinges on semantics. By attempting to use human rights as the basis for their challenge, these campaigners have

shot themselves in the foot[9] – it is the minute codification of rights in the human rights framework that allows governments to rewrite their own powers in the first place.

Human rights constantly negotiate freedoms, rather than protecting them. Alongside the framework of self-regulation, the framework of human rights has had a seriously adverse effect on constitutional rights in relation to the Internet. For example, the framework of human rights enabled the UK's Regulation of Investigatory Powers (RIP) Act 2000, which grants security services powers to monitor Internet traffic and grants the authorities the power to demand the keys to encrypted communications, to be passed.[10]

Initially, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which upholds the right to privacy, appeared to pose an obstacle to the RIP Act. But in practice, the deadline for incorporating the European Convention for the Protection of Human Rights and Fundamental Freedoms into UK legislation actually became the pretext for rushing the RIP Act through parliament.

---

9 For example, the UK human rights and civil liberties organization Liberty <http://www.liberty-human-rights.org.uk> invoked Article 5 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which prohibits arbitrary detention and imprisonment, in its campaign against the emergency government powers.

10 The Regulation of Investigatory Powers Act 2000 <http://www.hmso.gov.uk/acts/acts2000/20000023.htm> allows 'the imposition...on persons who...are providing...public telecommunications services...of such obligations as it appears...reasonable to impose for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with' (Part I, Chapter I, Section 12) (in practice, this means requiring ISPs to install 'black boxes' that record Internet traffic data); and grants the authorities, whenever data has been seized and 'a key to...protected information is in the possession of any person', the power to 'impose a disclosure requirement in respect of the protected information' (Part III, Section 49).

Because new communications technology had made the limits of the UK Government's surveillance powers ambiguous,[11] and because compliance with the European Convention for the Protection of Human Rights and Fundamental Freedoms required these surveillance powers to be more clearly defined, the RIP Act was justified as necessary for clarification. Rather than curtailing surveillance powers, the human rights framework strengthened the UK Government's hand.

And when it transpired that the RIP Act appeared to contradict an item of European data protection law (the 1997 Telecoms Data Protection Directive), the UK authorities simply reconciled the two pieces of legislation, in a document entitled 'Lawful Business Practice Legislation'. This kind of triangulation between contradictory laws is made easy by a human rights framework, whereas it would be far more difficult under a framework based more on constitutional rights.

Now, if you want to snoop on others in the UK without falling foul of the law, all you have to do is visit the helpful Office of Surveillance Commissioners website set up by the UK Government, whose homepage (at the time of writing) states: 'this website is primarily designed to be used by those who authorise and conduct covert surveillance operations and covert human intelligence... It shows you how to carry out these activities in compliance with the powers granted by parliament.'[12]

Privacy campaigners attempted to invoke human rights in opposition to the introduction of the RIP Act.[13] But once again, in doing this they were shooting themselves in the foot. The human rights framework gives the state latitude to set the terms on which freedoms are negotiated, rather than giving citizens the means to insist that their freedoms are protected.

III. Case Study: European Copyright Regulation. In recent years, debate has raged internationally about digital piracy of copyrighted works, and what should be done about it. In Europe, there has been heated discussion about the European Copyright Directive of 2001.[14] But in terms of its negative impact upon constitutional rights, the copyright regulation enforced by the earlier Ecommerce Directive of 2000 is even more significant.[15]

The Ecommerce Directive enforces a self-regulatory regime for copyright regulation, by stipulating that ISPs are liable for copyright-infringing content that they host, unless they remove it 'expeditiously' upon notification of infringement.[16] Due process is entirely bypassed under this regime.

---

11 The previous piece of UK legislation which dealt with surveillance – the Interception of Communications Act 1985 – could not be clearly applied to Internet communications. Ironically, just like the RIP Act that followed it, the Interception of Communications Act 1985 was originally introduced to clarify a human rights ambiguity – after the European Commission on Human Rights declared phone tapping a breach of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, in the case of 'Malone v UK' <http://hudoc.echr.coe.int/Hudoc1doc/HEJUD/sift/118.txt>.

12 Homepage of the Office of Surveillance Commissioners <http://www.surveillancecommissioners.gov.uk> website.

13 The RIP Act was campaigned against by organizations including Privacy International <http://www.privacyinternational.org>, Statewatch <http://www.statewatch.org>, Cyber Rights and Cyber Liberties <http://www.cyber-rights.org>, and the Foundation for Information Policy Research (FIPR) <http://www.fipr.org>. To be fair, it should be noted that the FIPR was instrumental in several modifications to the Act that reduced its adverse impact on privacy – see the 'Achievements' section of the FIPR website <http://www.fipr.org/achievements.html>.

14 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.

15 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').

16 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'), Article 14.

This is a good example of self-regulation as a defence mechanism, as was mentioned earlier – copyright regulation is mimicking the decentralized content distribution that frustrates it. This kind of enforced self-regulation also reflects the European Commission's lack of lawmaking legitimacy – by far the most effective way for it to create a new international regime, quickly and efficiently, is by intervening at the level of the marketplace.

The Ecommerce Directive is a remarkably irresponsible piece of legislation, in that it is deliberately ambiguous and incomplete. Not only does it enforce regulation by the marketplace; it also gives the responsibility for coming up with the specifics of the regulatory system it enforces to the marketplace.

The European Commission was unwilling to risk confrontation by grappling with the obvious conflicts of interest that surround copyright. Therefore, the Ecommerce Directive states that governments must 'encourage...the drawing up of codes of conduct...by trade, professional and consumer associations or organizations' for copyright regulation.[17]

Many industry figures still live in hope that the European Commission will, at the very least, clarify the system it has gone halfway towards creating. They'll be waiting for a long time. In November 2002, Margot Froehlinger, head of unit at the Internal Market Directorate General, European Commission – who was partially responsible for drafting the Ecommerce Directive – told an audience of rightsholders, lawyers and user representatives in Brussels that on no account would the European Commission do anything to clarify the Directive in the foreseeable future.

Such wilful and unrepentant ambiguity, on the part of the European authorities, is breathtaking. As well as being a

scandalous abdication of responsibility, this attitude can also be understood as a further self-regulatory defence mechanism.

Froehlinger was speaking to a conference organized by the European Commission funded research project RightsWatch.[18] RightsWatch is run by a consortium consisting of several organizations with a commercial stake in the way that copyright is regulated (plus one university),[19] and was established in an attempt to tidy up the confusing regulatory mess created by the Ecommerce Directive.

In March 2002, RightsWatch approached me to act as a representative of Internet users in one of its working groups. This meant that I had a dilemma. Should I turn RightsWatch down – because I'm in no way qualified to represent Internet users, because no Internet user ever elected me to represent their views on the regulation that affects them, and therefore representing Internet users is a completely illegitimate position? Or should I accept the position – in the hope that I can do something to make the regulatory system more just, and in order that I might write papers such as this one, about how these regulatory decisions are made?

---

17 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'), Article 16.

18 See the RightsWatch <http://www.rightswatch.com> website. The conference, 'Notice and Takedown in Europe (2)', was held at the Renaissance Brussels Hotel on 12 November 2002. Details of the conference can be found in the 'Events/Meetings' section of the RightsWatch website.

19 The consortium that runs RightsWatch consists of the Music Alliance <http://www.mcps-prs-alliance.co.uk> (an operational venture between two UK licensing and collecting societies – the Mechanical Copyright Protection Society <http://www.mcps.co.uk> and the Performing Right Society <http://www.prs.co.uk>), assisted by British Music Rights <http://www.bmr.org>; British Telecom <http://www.bt.com>; Telia <http://www.telia.com>, assisted by consultant Philipson & Associates; Denton Wilde Sapte <http://www.dentonwildesapte.com>; and the University of Florence <http://www.unifi.it>.

In the end, I said yes, and became an illegitimate, unelected representative of Internet users in the development of copyright regulation. It was an interesting experience.

Since there are obvious conflicts of commercial interest between publishers, rightsholders and ISPs, when it comes to copyright regulation, it's fascinating to sit in on a situation where their representatives all have to talk to one another directly and come up with a common solution.

The way it's done is through the very fashionable, therapeutic method of 'consensus-building' – an expression which conjures up an image of a friendly discussion over a cup of tea. But what consensus-building really amounts to is the careful management of compromise, where people negotiate endlessly and circuitously, and you try and steer them and make sense of the product.

The human rights framework is essential to this method of drafting regulation, because it embodies compromise, allowing liberties to be negotiated and constitutional rights 'balanced' with other concerns – as though you're writing a cooking recipe, rather than playing with the rights and freedoms of citizens who never elected you.

Another important factor in this kind of regulation is risk management. When regulation is conducted by the marketplace, legal categories such as liability and indemnity cease to be well-defined absolutes, and instead become exchangeable commodities. There were proposals in the RightsWatch working groups, for example, that rightsholders should undertake to indemnify ISPs to a degree proportional to the speed with which ISPs remove content – in other words, that legal indemnity be used, by those who can afford it, as a bargaining chip for content removal.

The outcomes of the three different RightsWatch working groups are interesting examples of the kind of convoluted gymnastics that regulators (legitimate or otherwise) have to engage in, when trying to rationalize a wilfully ambiguous self-regulatory regime:

- The UK and Ireland working group (the one that I worked for) called for the creation of a statutory legal underpinning for copyright regulation – going against the spirit of the Ecommerce Directive, by trying to restore some statutory coherence to copyright regulation.
- The Northern European working group called for an impartial central body to oversee copyright regulation – but unfortunately, no matter how 'impartial' and 'central' that regulatory body is supposed to be, that doesn't make it an accountable or constitutionally legitimate body.
- The Southern European working group called for a multi-track procedure, where you can trade liabilities and indemnities in order to guarantee faster removal – the risk management model of commodified justice.[20]

All three solutions suffer from the RightsWatch working groups having limited room for manoeuvre. The working groups were left to scrabble around in a tiny space for debate, after the real debate was had long ago, and closed down, by the European Commission.

The European Commission's brief to RightsWatch – to develop fair and coherent regulation in the context of the Ecommerce Directive – was an impossible one. The only possible consequence of struggling to meet this brief was greater or lesser erosion of the constitutional rights of the Internet user, as can be seen in the three working group solutions.

20 The three working group reports are available in full in the 'Reports' section of the RightsWatch <http://www.rightswatch.com> website.

To conclude, European copyright regulation makes for a useful case study of the diminishing importance of constitutional rights in the Internet age. It embodies some of the worst symptoms of this erosion of constitutional rights: irresponsible legislation; commodified justice; unaccountable representatives and regulators; and the use of human rights to negotiate liberties.

Jennifer Jenkins

The Importance of Public Domain for Creativity, Innovation, and Culture in the Digital Age

I. The Public Domain in the Digital Age. What is the public domain? It is often described as the wellspring of material that is freely available for everyone to use and build upon. It includes our heritage of science, art, culture, facts and ideas; it contains the raw materials for (among other things) scientific inquiry, artistic expression, political debate, scholarly research, and education.

The potential functions of the public domain have been expanded and invigorated by the Internet, which allows people to collect, process, and share information with unprecedented speed and ease. Concerned constituents can readily access government information, scientists conducting experiments from around the world can share data, musicians who have never met can create songs together, professors from different universities can share and discuss course materials, and researchers can explore the contents of vast digital archives.

As the Internet offers enhanced opportunities for democratic participation, innovation, creativity and knowledge advancement, the public domain becomes an even more vital resource. The Internet itself owes its rapid development to the fact that its core protocols, such as TCP/IP and HTML, are in the public domain. Yet, just as technology opens new doors, intellectual property laws are blockading them: the public domain is 'under attack' by hastily expanding intellectual property rights. These rights are expanding in length (for example,

the recently upheld twenty-year copyright term extension in the United States), in the subject matter they cover (for example, patent protection for gene sequences and for common business methods), and in the actions that they cover with respect to that subject matter (for example, legitimate personal and non-commercial uses of digital content are being chilled, curtailed, and criminalized). As more rights affect more people in more ways, it is becoming increasingly difficult to engage in routine acts of expression, even consumption, without violating someone else's intellectual property rights.

II. Significant Threats to the Public Domain. Following are a few examples of expanding intellectual property protections that threaten to (or already do) diminish the public domain.

Copyright Term Extension Act (CTEA)

In the United States ('US') the copyright term originally lasted for 14 years, with the option to renew for another 14 years. Over the past 40 years, however, this copyright term has been extended 11 times. The most recent term extension locked up an entire generation of works for an additional 20 years, extending the duration of copyright protection to the life of the author plus 70 years (and for works initially owned by a corporation to 95 years). This extension was retroactively applied to existing works, thus removing works from the public domain with little plausible claim of offering incentives for creation – granting an extension of copyright to dead authors will hardly induce the creation of new works. Now, works created over 100 years ago may no longer be in the public domain. Artists, scholars, archivists, and others who wish to use these works must first track down their copyright holders and clear necessary rights – a process that, even for seasoned copyright attorneys, is complicated, lengthy, expensive, and sometimes impossible.

The recent challenge to the CTEA in the US Supreme Court (*Eldred v. Ashcroft*, 537 US ___ (2003)) was unsuccessful: declining to 'second guess' Congress, the Court held that Congress acted within constitutional limits on its authority in adopting the term extension, and refused to find that the law was a restriction of free speech. In the minds of many, this decision casts serious doubt on whether there are real limits on Congress's power to create intellectual property rights, and whether the public domain is constitutionally protected. (Links to a wealth of additional information on this case are available at Lawrence Lessig's weblog: <http://cyberlaw.stanford.edu/lessig/blog/>.)

Digital Millennium Copyright Act (DMCA)

As Lawrence Lessig has written, although the Internet was initially built as an open information environment, it is evolving into an architecture of perfect control. A major source of this control is the DMCA. The DMCA protects technical measures that directly control access to and uses of digital information. As Professor Pamela Samuelson has observed, these measures may protect digital versions of existing public domain works, and can persist after copyrights expire, keeping new works from entering the public domain. In addition, technical measures do not have to be designed to allow for uses that are otherwise privileged under copyright law, such as fair use. For example, the DVD Content Scrambling System (DVD-CSS) doesn't allow for fair uses, or even for users to skip through commercials.

Under the anticircumvention provisions of the DMCA, it is illegal for anyone to circumvent a technical measure, for example by deciphering the encryption for a software system or building a tool to bypass it. Not only is circumvention itself illegal, but it is illegal even to share information about how to circumvent technical measures.

The DMCA, with these legally-backed 'digital fences', gives copyright holders a powerful and unprecedented tool for restricting access to and uses of digital works. In doing so, the DMCA threatens to thwart the free flow of digital information and rob the public of existing rights under copyright law, most notably rights under the first sale and fair use doctrines. (Under the first sale doctrine, the owner of a copy of a work can lend, sell, or modify that copy; allowing, for example, libraries to freely loan out books, or someone to give a video to a friend. The fair use doctrine allows for well-accepted and important uses such as parody, commentary, criticism, news reporting, education, research, and reverse engineering to achieve software compatibility.)

As many have recognized, these anticircumvention provisions have an obvious adverse effect on computer science, and particularly on encryption research. For example, Edward Felten, a computer science professor, accepted a public challenge from the music industry and broke their new encryption code for digital music distribution. As he was preparing to publish a paper about his findings, he received a threatening letter from the Recording Industry Association of America (RIAA) which warned him that publication of this paper would violate the DMCA. When he sought a declaratory judgement that publishing the paper was not in fact a violation of the DMCA, the RIAA suddenly changed its position. The case nevertheless had chilling effects – in the wake of the case, researchers began to shy away from conferences in the US for fear of being arrested under the DMCA.

Perhaps more alarming is the case of Dmitry Sklyarov, a Russian computer programmer who faced American jailtime because he wrote software making it possible for people to read books encrypted by Adobe for its eBook reader. The DMCA

protected Adobe's eBook encryption, even where it would prevent readers from making otherwise privileged uses of the same books. For example, a reader who owned a hard copy of the book could freely read it, lend it to a friend, or excerpt a quote from it as permitted under copyright law; but these uses of the digital version would be prohibited. These uses would even be prohibited for digital versions of public domain books, which would otherwise be free for unrestricted use.

So far, challenges to the DMCA in US courts have failed. In a recent case, an appellate court enjoined not only posting, but also linking to other sites that post, DeCSS, a computer program that circumvents the copy protection scheme for DVDs. (However, Jon Johanson, the fifteen-year-old Norwegian who wrote the code, was recently acquitted in a Norwegian court of violating data break-in laws and for helping others to illegally copy films.)

Uniform Computer Information Transactions Act ('UCITA')

UCITA essentially turns everyday 'sales' of digital works into a binding licence by legalizing 'shrink-wrap' licences that restrict the uses that purchasers may make of the works, even if these uses are otherwise legal. UCITA presumes that these licences are enforceable, and this presumption can only be overcome after litigation. Therefore, as Professor Samuelson has explained, many will be chilled from engaging in activities that would eventually be found legitimate in court. Fortunately, because of the criticism surrounding it, UCITA has only been enacted in two states.

Database Rights

One of the most basic tenants of the US intellectual property system is that unoriginal compilations of facts, and the data in original compilations, will remain in the public domain, to

be available as the raw material for future creativity and innovation. In recent years, however, the US Congress has considered a number of proposals that would protect the contents of databases similarly to the directive adopted by the European Union in 1996, which allows those who have made a 'substantial investment' in a database fifteen years of exclusive rights to control the extraction and reuse of all or substantial parts of the contents of that database. This directly takes facts and data out of the public domain, creating, as opponents have observed, 'an unprecedented right to control transformative, value-added, downstream uses of the resulting collection or of any useful fraction of that collection.' Indeed, much of education, scientific research, and journalism would be significantly hindered if facts could be owned and their use restricted. In the US, these proposals have not been enacted yet because of strong opposition from scientists and legal scholars, who have emphasized the threat posed to the public domain and to innovation.

III. Are Recent Expansions of Intellectual Property Rights Necessary? As Professor James Boyle has described, the US system of intellectual property is premised on the following economic rationale. Information goods – inventions, artistic works – are both non-rival and non-excludable. 'Non-rival' means that uses do not interfere with each other: while only one person can use a rival good such as a jacket, any number of people can simultaneously enjoy a non-rival good such as a sonnet. 'Non-excludable' means that it is difficult to exclude users from accessing the good – the sonnet could easily be available for anyone to use how, where and when they wish. The problem, then, is that the information good can be copied and used an infinite number of times, but the producer of the

good cannot charge for each individual unit, defeating the economic incentive to produce. The intellectual property system seeks to solve this problem by granting the producer exclusive rights to the information good for a limited period of time.

The 'copyright and patents clause' in the US Constitution empowers Congress to grant such exclusive rights 'To promote the Progress of Science and the useful Arts.' This clause, as interpreted by the US Supreme Court, strikes a cultural bargain that allows Congress to grant exclusive private rights only if these rights also benefit the public – in the words of the Court, if they encourage '[i]nnovation, advancement and things which add to the sum of useful knowledge.' In addition, these exclusive rights must not remove or restrict free access to materials that are already in the public domain.

The recent expansions of intellectual property rights have upset this balance between private property rights and the public interest, and taken inputs directly out of the public domain. Many have raised concerns about the costs of recent intellectual property expansions; but the benefits are less clear. Professor Boyle has posed the critical questions: first, are these expansions of intellectual property rights necessary to respond to new copying technologies? The answer is that we don't really know: as he points out, while the Internet does make copying easier, it may also lower the costs of production, distribution, and advertising, and increase the size of the potential market. Then, are these expansions desirable because they will encourage innovation or creativity? Again, we don't know: these laws were pushed through Congress by a handful of large content owners without convincing empirical evidence that they will stimulate innovation or encourage creativity, and despite good arguments that they will actually impede innovation and stifle creativity.

The challenges posed by digital technologies to our existing intellectual property scheme are numerous and complex. Before reflexively granting expansions of intellectual property protection, we need to better understand what is at stake: are these laws really necessary and beneficial, or are we risking enormous costs to the public and the future of the Internet? As part of this inquiry, we need to engage in careful empirical studies to assess the actual effects of these laws.

We also need to examine how the intellectual property system does and does not work in the digital environment – how incentives and production may operate differently, offering possible alternative solutions. A number of scholars have discussed the emergence of non-proprietary production on the Internet. Professor Yochai Benkler argues that the current intellectual property expansions favour the 'commercial proprietary production' of large media companies: these corporations produce mass-mediated culture, which is sold to enormous numbers of consumers who simply receive finished goods. Consumption is separated from production. But, on the Internet, consumption and production are mixed so that people are not merely producers or consumers, but users. Thus, different modes of non-proprietary production have become increasingly important sources of information and cultural materials. This includes, most notably, peer-to-peer production and professional production from the non-profit sector. The Internet promises to greatly expand these types of production, while current intellectual property laws endanger it.

One of the most well-known alternatives to proprietary production is open-source software, which is released under licences providing that anyone may copy, add to, or modify the source code, and incorporate it into a new program; but if they do so, their new program must also be covered by the same licence, which would make this new work freely available for

others to use and build upon. The open source model thereby ensures that source code is publicly available and encourages follow-on innovation. This model has become exemplary because it is successful: many agree that open-source software exceeds the capabilities of proprietary software.

In the words of Eben Moglen, open source works effectively outside of the incentive system offered by intellectual property because: '[I]ncentives' is merely a metaphor, and as a metaphor to describe human creative activity it's pretty crummy. I have said this before, but the better metaphor arose on the day Michael Faraday first noticed what happened when he wrapped a coil of wire around a magnet and spun the magnet. Current flows in such a wire, but we don't ask what the incentive is for the electrons to leave home. We say that the current results from an emergent property of the system, which we call induction… So if you wrap the Internet around every person on the planet and spin the planet, software flows in the network. It's an emergent property of connected human minds that they create things for one another's pleasure and to conquer their uneasy sense of being too alone.'

The Internet is rich with examples of non-proprietary production – in the absence of property rights, it appears that people will nevertheless produce, whether for gifts, reputation, enjoyment, excitement, or other personal and social rewards. These modes of production need to be analysed and better understood before locking the Internet into a proprietary framework.

IV. A Positive Look at the Public Domain. The public domain has traditionally been thought of as the outside, the opposite, the negative, the 'other' to the intellectual property system; in Professor David Lange's words, the 'dark star in the

constellation of copyright.' But the public domain is a vital, indispensable part of our intellectual property system. The inputs in the public domain are just as important to the function of the intellectual property system as the outputs protected by intellectual property, and ensuring that necessary materials remain in the public domain is equally important to the continued progress of science and culture as the granting of intellectual property rights.

If we are to preserve the public domain, we need to reorient our thinking. As Professor Boyle has said, the public domain needs to be studied and appreciated with the same care and precision that has been afforded intellectual property. Rather than focusing only on the wisdom and drawbacks of intellectual property protections, we need to affirmatively focus on the public domain as a necessary part of the intellectual property system. To respond to the well-travelled rhetoric and arguments in favour of intellectual property protection, the public domain needs its own vocabulary, metaphors, rhetoric, agenda, scholarly research and policy analysis. We must strive to understand and articulate its role and function, appreciate its value, and set the appropriate balance between what is protected by intellectual property and what is in the public domain.

Dramatically expanding intellectual property laws, and notably the *Eldred* decision, have begun to rouse a counter-response by the public. We need to capitalize on this, and mobilize a wide group of constituencies who are all affected by threats to the public domain: writers, musicians, scientists, archivists, librarians, historians, researchers, software developers, journalists, educators, and Internet users. If all of us work together, we may be able to effectively nurture and safeguard the public domain in the digital age.

This overview extracts from the developing body of public domain scholarship a basic framework for thinking about the importance of the public domain. For a more thorough discussion of the public domain and its role in a variety of areas, please visit the website of the Conference on the Public Domain, the first-ever conference to focus squarely on this subject, held at Duke Law School in November, 2001. The webcast is available at <http://www.law.duke.edu/pd/realcast.htm>. Papers from this conference will be published in an upcoming volume entitled 'The Public Domain', 66 Law & Contemp. Probs. (Winter/Spring 2003), which will be available online at <http://www.law.duke.edu/journals/lcp/>. Several of the papers in the volume are referred to in this overview: these include Yochai Benkler, 'Through the Looking Glass: Alice and the Constitutional Foundations of the Public Domain'; James Boyle, 'The Second Enclosure Movement and the Construction of the Public Domain'; and Pamela Samuelson, 'Mapping the Digital Public Domain: Threats and Opportunities'.

Felipe Rodriquez

Burning the Village to Roast the Pig:[1] Censorship of Online Media

> ***Censorship.*** In the strict sense, censorship is an act of government in which it becomes criminal to obtain or disseminate certain types of information. The term is also used to describe restrictions on the way ideas are expressed, such as using profanity.
>
> The purpose of censorship is to control people by influencing the way they think and act. It is understood that people's thoughts and actions are shaped by the information they have available. To the extent one can control what information people have, one is able to control the people themselves. For this reason, censorship is very common among, perhaps even essential to, totalitarian governments.
>
> *Source: Wikipedia, the Free encyclopedia*

Introduction. Since the arrival of the Internet as a popular medium to exchange information, concerns have been expressed about access to online content deemed to be offensive or dangerous.

The absence of national borders on the Internet has an effect on the availability and proliferation of controversial information. Community standards are a local affair, and different communities have different standards. Information that in one country is illegal, such as bestiality in the United States, is legal in another, such as the Netherlands. Vice versa neo-Nazi propaganda is constitutionally protected in the United States, whereas it is illegal in the Netherlands. In the analogue age this was a trivial difference, as it was possible to control

1 'Any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig.' Judge Stewart Dalzell, ACLU -v- Reno, 11 June 1996.

the distribution of the carrier of information, such as paper, audio/video cassettes or electromagnetic waves. There was always a small amount of clandestine distribution but the public majority was mostly unable to access censored information. Digital communications have changed the paradigm, and we now live in a world where information is not restricted by physical boundaries, except for a few exceptions such as China and Saudi Arabia. On the Internet a Dutch person can access any information on the US part of the Internet, even if that information is not legal in the Netherlands. And a US national can access any kind of information in the Netherlands that is illegal in the US.

Censorship laws are sometimes seen by politicians and governments as the solution to these problems, and several countries have implemented comprehensive systems of censorship on the Internet. Parents, schools and other entities have turned to privately manufactured Internet rating and filtering programs, with varying rates of success.

The debate about online content is still very much alive, and none of the available solutions to protect against offensive content are completely satisfactory. At one extreme of the debate are religious leaders and community groups that want some sort of protection against offensive content on the Internet in a desperate attempt to protect the local community standards. At the other extreme are civil liberty groups that see any form of censorship as a threat to freedom of speech. Regardless of the moral position on censorship, the reality is that effective censorship on the Internet is incredibly difficult without harming legal access to information.

This paper aims to provide a bird's eye view of online censorship and the technologies that are used to implement or circumvent censorship; it is not an exhaustive analysis.

Overview of Internet Technologies. The debate about censorship of online media is usually focused on the World Wide Web[2] and Usenet newsgroups[3]. The Internet provides much more than just the Web, e-mail and Usenet. In any discussion about censorship we need to define what technology we are talking about. I am providing here a *limited* overview of available technologies, to aid us in the discussion about censorship of online media.

E-mail. 'E-mail, or email, is short for "electronic mail" and refers to composing, sending, and receiving messages over electronic communication systems. Most e-mail systems today use the Internet, and e-mail is the most popular use of the Internet.'[4] E-mail is not limited to private conversations; there are numerous public e-mail mailing lists on the Internet that anyone can subscribe to.

Many people that have used the Internet for a while receive unwanted e-mail, also called spam[5]. These e-mails are often scams or advertisements for erotic products, such as penis enlargement or live sex shows. Some of the e-mails the author regularly gets in his mailbox have subject lines such as:
'Get Christmas Money – Santa's Best Kept Secret'
'Make your love life better, grow inches now'
'One form, one time, thousands of instant cash prizes!'
'Your health care…'
'Add ? inch in one week'
'Sample viagra'
'Hello it's Teresa, naughty girls who love to smoke'
et cetera

2 The Web, see glossary
3 See glossary
4 Source: <www.wikipedia.org>
5 See glossary under Spamming

In some countries the senders of commercial advertising e-mails need to include an opt-out mechanism, which enables the receiver to unsubscribe from that particular spam list, but in practice these opt-out mechanisms rarely work. The author has dealt with the spam problem by turning on a set of filters provided by his provider, XS4ALL. This strategy identifies 99 per cent of spam, and has enabled the author to receive these messages in a separate folder.

The World Wide Web. The Web is usually the main target of Internet censorship proposals. The Web and e-mail are the most visible components of the Internet. Therefore the Web arouses much of the controversy about online content. A lot of content on the World Wide Web is static, but not all of it is. For example, the many webcams[6] are anything but static, and provide a constantly changing picture of the environment the webcam is pointed at. Webcams are sometimes used by users to engage in amateur pornography, to share their pornographic fantasies with an audience.[7]

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.'[8]

Close to a million messages are published in Usenet discussion groups every day[9], generating slightly more than 130 gigabytes[10] of data. One gigabyte equals over 1,000 books of text.[11] Google provides a searchable archive of the Usenet.[12] A small percentage of the messages on Usenet contain pornographic content[13] or are used to exchange pirated software[14]. Commercial spam messages are prolific on the Usenet, and concerned citizens have taken it upon themselves to censor these messages by erasing them for the rest of the community,

a dubious activity because it takes away the choice of the individual to legally access the information and filter it if deemed necessary. These grass-roots community censors defend themselves with the argument that without their activity the Usenet newsgroups would soon be flooded by endless amounts of commercial advertising.

IRC & Instant Messenger Technology. 'Internet Relay Chat (IRC) is a form of instant communication over the Internet. IRC is a predecessor to the class of applications known as instant messaging.

IRC has a decentralized network of servers that can be accessed by special client programs. The protocol for IRC is open, and there are many client (and server) implementations. Unlike popular instant messaging applications, there is not an inherent login id that one must acquire; it's typically a much more anonymous medium than instant messaging.'[15]

'An instant messenger is a computer application which allows instant text communication through a network such as the Internet. An instant messenger is a client which hooks up to an instant messaging service. Instant messaging differs from e-mail in that conversations over instant messaging mediums happen in real-time. Generally, both parties in the conversation see each line of text right after it is typed (line-by-line), thus making it more like a telephone conversation than exchanging letters.'[16]

---

6 See glossary
7 See <http://www.webcamnow.com>, unmonitored adult area
8 Source: <http://www.wikipedia.org/wiki/Usenet>
9 Usenet Stats: <http://news.gamma.ru/stats-week.html>
10 See glossary
11 Computer Basics, storage devices <http://dragon.ep.usm.edu/~it365/module/Basics/storage.htm>
12 Google groups at <http://groups.google.com>
13 See alt.binaries.erotica.* Usenet groups
14 See alt.binaries.warez.* Usenet groups
15 Wikipedia <http://www.wikipedia.org/wiki/IRC>
16 Wikipedia <http://www.wikipedia.org/wiki/Instant_messaging>

IRC enables private communications and group chats. Group chats can be private and restricted, or open to the public. IRC and some of the instant messenger technology also enable the user to transmit files to other users, and with robot software this file distribution facility is sometimes automated. The content on IRC is highly dynamic, consisting of the private and public chat messages that users exchange. Censoring or filtering IRC is unlikely to be successful because of these dynamics.

Many of the concerns about safeguarding children from predatory behaviour by adults on the Internet concern chat or messenger technology.

Streaming Media. Streaming media are the online alternative to traditional broadcasting. Streaming media client[17] software enables the user to access live or archived audio and video content. Many radio stations provide their broadcast online through streaming media technology, and some television broadcasters do as well. Streaming media technology is not limited to traditional broadcasting organizations; it can be used by end-users as well to participate in video chat groups or to broadcast their own productions. Some providers of pornographic content use streaming media technology for their pay-per-view products.

Peer-to-Peer Technology. 'Put simply, peer-to-peer computing is the sharing of computer resources and services by direct exchange between systems. These resources and services include the exchange of information, processing cycles, cache storage, and disk storage for files.'[18]

Peer-to-peer technology acquired popularity and a certain amount of notoriety with the introduction of the Napster[19] file sharing service, which provided a very popular music swapping platform. The service soon became the object of scrutiny

of the RIAA, the Recording Industry Association of America, because much of the music that people exchanged through the Napster service infringed the copyright of the recording industry. The RIAA litigated against Napster, and was ultimately able to shut it down. Peer-to-peer file exchange technology is still around today, and is more popular than ever.

It is important to keep the dynamic nature of information on the Internet in mind, as this provides important challenges to any attempt to censor online content.

Censorship Today: A Few Examples. Historically the censor worked towards enforcing local community standards, this was possible because analogue information was mostly locally distributed. Enforcement of censorship was relatively easy because information had a physical carrier, and a licence was required when broadcasting through the ether. The use and distribution of these carriers could be controlled, the carrier could be destroyed or confiscated, or a licensed broadcaster could be threatened and closed down. Such controls have become unpractical since the popularization of the Internet.

Digital information can be infinitely replicated without cost inhibition; the absence of significant reproduction costs has caused an explosion of published information. The global information infrastructure has transcended the region, as it is by definition a global grid. The effects of infinite duplication and internationalization of information pose an impossible challenge for the censor. The resources that are required to review and block the more than four billion pages of web content around the world are mind-boggling.

---

17 See glossary

18 'What is Peer-to-Peer' <http://www.peer-to-peerwg.org/whatis/>

19 See glossary

One important thought to keep in mind is which technology we are talking about when discussing online censorship. Are we talking about the World Wide Web, or about e-mail, or about chatboxes, or about peer-to-peer file exchange networks, or about streaming media, or about Usenet newsgroups? Discussions about online censorship are usually limited to the Web, but the Internet offers so much more than just the Web.

Government Censorship. How does one enforce local community standards in a global environment?

China has implemented the most comprehensive censorship system on the Internet. The Internet is somewhat of a paradox to the Chinese authorities, as it provides access to information that will be crucial to the country's industrial and scientific development. Yet at the same time the Internet greatly complicates the pursuit of internal security, and officials have warned that the Internet could be 'harmful to social stability'.[20]

The system of censorship China has implemented involves routers that block access to certain IP addresses,[21] surveillance of users, the use of informers, arrests and seizures.[22] China focuses primarily on websites and e-mail.

Technologically the system is quite crude, because thousands of websites may be grouped under a single IP address. Blocking the IP address blocks all those websites, even if the content on those sites is not controversial. Implementing an IP blocklist also degrades network performance; large blocklists can cause serious performance problems. 'Blocking can be done only intermittently, because the software does not have enough computer power to block every objectionable site all the time.'[23] An IP blocklist can be defeated by changing, or rotating, the IP address of a website. Recently the Ministry for Public Security implemented a system of domain name hijacking, which is a somewhat more sophisticated system of access control. The

technique works by falsifying the records in Domain Name Servers[24] (DNS) throughout China. The domain name system is the connection between a domain name, such as www.xs4all.nl, and the IP address of that site. By interfering with the DNS system the Chinese authorities are able to divert traffic[25] to certain domains to unrelated IP addresses, thereby blocking access to the website and diverting traffic to another (government controlled) website.[26] There are some indications that China has developed the capability to automatically block individual web pages by using content rules, based on individual words, or combinations of words that appear on the page.[27] It is estimated that the Government employs as many as 30,000 people to enforce Internet censorship.[28] '...Chinese filtering is quite effective, not as granular as Saudi Arabia.'[29]

Saudi Arabia has a similar, but less effective, system of censorship, aiming to censor offensive and unislamic content.[30] It is estimated that Saudi Arabia blocks around 400,000 IP addresses.[31] In Saudi Arabia a user that tries to

---

20 Zhao Ying, 'Information and Security Issues', *Jingji Guanli*, 5 (5 May 1998), as printed in Rand Report, 'You've got dissent!', chap. 2, Government Counter Strategies, 48 ff.

21 See glossary

22 Rand Report, 'You've got dissent!', chap. 2, 49 ff.

23 Rand Report, 'You've got dissent!', chap. 2, 64 ff.

24 See glossary

25 See glossary

26 Bill Dong, 'Forbidden Sites Hijacked all over China', Dynamic Internet Technology <http://www.dit-inc.us/report/hj.htm>

27 'The Shrinking Frontiers', *Online Journalism Review* <http://www.ojr.org/ojr/world_reports/1037922526.php>

28 'A glimpse of China's business, technology revolution', *China Online* (20 March 2002) <http://www.chinaonline.com/commentary_analysis/thiswk_comm/020320/C02031231.asp>

29 Quote by Harvard researcher Ben Edelman, 'The Shrinking Frontiers', *Online Journalism Review* <http://www.ojr.org/ojr/world_reports/1037922526.php>

30 Documentation of Internet filtering in Saudi Arabia at <http://cyber.law.harvard.edu/filtering/saudiarabia>

31 Human Rights Watch Report for Saudi Arabia at <http://www.hrw.org/wr2k2/mena7.html>

access a censored website is shown a notice that the site has been blocked; this is not the case in China.[32]

Saudi Arabia and China are two examples where censorship on the Internet has been implemented somewhat successfully. It is noteworthy that both are repressive regimes, which has enabled these states to take control of the distribution of digital content, the use of informers and intimidation. Other countries, for example Singapore, South Korea, Iran, and Syria, have implemented similar censorship systems, with varying rates of success.

Although these censorship frameworks have achieved a degree of success in suppressing information, it must also be noted that a lot of legal and uncontroversial content is filtered as a consequence, because the technological tools that are implemented are crude and usually affect entire websites or even hundreds of web servers that share the same IP address. Important elements of the censorship framework in all these countries are the low-tech solutions, such as the use of informers, arrests, seizures and intimidation.

Implementing online censorship in a democratic nation is infinitely more complicated, and so far there have been very few successful attempts at doing so. Australia has the most comprehensive system of censorship among democratic nations since it implemented the 'Broadcasting Services Amendment (Online Services) Bill 1999'.

> 'The Broadcasting Services Amendment (Online Services) Act 1999 commenced operation on 1 January 2000. To date (November 2002) it has been implemented in a way that does not require ISPs to block access to content on overseas sites. (The government regulator has the power to require ISP blocking if they consider the current implementation of the law to be inadequate).
>
> However, ISPs/content hosts are required by law to delete Australian-hosted content on receipt of a take-down notice from the government regulator, i.e. the Australian Broadcasting Authority ("ABA").
>
> The regime is complaints based. The ABA implemented a Complaints System which enables Australian citizens to lodge complaints about Internet content that is, or is likely to be, classified/rated:

- R18 (information deemed likely to be disturbing or harmful to persons under 18 years),
- X18 (non violent sexually explicit material involving consenting adults) or RC (Refused Classification/banned)

by the Government censorship office, i.e. the Office of Film and Literature Classification ("OFLC"). Internet content (including text, static images and moving images) is classified using criteria set out in the Classification Guidelines for Films and Videotapes (not the Guidelines for Publications) established under the Commonwealth Classification Act.

- Content hosted in Australia: The ABA issues take-down notices to ISPs and other Internet Content Hosts requiring them (under threat of fines) to delete content on their servers (e.g. Web, Usenet and FTP) that is classified X18 or RC, and also R18 if access to R18-rated material is not subject to an ABA approved adult verification system (AVS). The approved AVS for R18 material requires sites, including non-commercial sites and those who charge no fee for access, to collect personal information from visitors to their site, such as credit card details or a copy of a driver's licence or birth certificate, before granting them access to R-rated information. The ABA is required to have Australian-hosted content classified by the OFLC before issuing a final take-down notice (an interim take-down notice is issued in the case of material likely to be classified X18 or RC, but not R18).
- Content hosted outside Australia: The ABA issues notices to approved filtering/blocking software providers informing them to add content the ABA considers likely to be classified X18 or RC (but not R18) to their blacklist. Australians are not required by law to use filtering/blocking software products. The ABA is not required to have content on overseas sites classified by the OFLC, the ABA makes its own determination of whether the content would be likely to be classified X18 or RC.'[33]

The problem with Australian Internet censorship is obvious; it only applies to local content, as Australia has no jurisdiction or technology to apply censorship to information that is hosted outside the country. The Government promotes the use of commercial filtering software for this purpose. Implementing the Chinese technology framework is too crude for Australia, as this would interfere with the freedom of its citizens to access content that is legal and uncontroversial.

The Australian censorship legislation has symbolic value; the Government can say that it has implemented limitations

32 'The Shrinking Frontiers', *Online Journalism Review* <http://www.ojr.org/ojr/world_reports/1037922526.php>

33 Electronic Frontiers Australia, *Internet Censorship in Australia* <http://www.efa.org.au/Issues/Censor/cens1.html>

on the use of the Internet with the aim to protect community standards. There is no measurable effect on the availability of harmful content overseas when the user chooses not to use commercial filtering software. The legislation is an effort in managing perceptions; there seems to be a perception in some parts of the Australian community (especially among church leaders) that the Internet is an unsafe environment. To counter this notion the Government implemented legislation to create the new perception that something is being done by the Government about offensive content. The Australian censorship framework is a product of domestic politics, and has little to do with result driven policy.

There are indications that locally censored information has been moved overseas, as it is trivial to relocate a website to another jurisdiction.[34] Australia's censorship focuses primarily on websites and newsgroups.

Commercial Censorware. Censorware[35] is 'software which is designed to prevent another person from sending or receiving information (usually on the web).'[36] It is commercial filtering software that can be purchased by users, it allows the user to install filters that limit access to certain information on the Internet. In Australia ISPs[37] must make filtering software available to their customers at cost price. Examples of such software are WebSENSE, Net Nanny, CYBERsitter and Cyber Patrol.

Censorware is a popular alternative to government censorship, because it allows the user to choose if filtering is applied. It provides parents with a tangible tool to protect their children from offensive content.

Despite this promise, there are considerable problems with commercial filtering software. Overblocking or underblocking are a concern, because access to harmless information is often denied, or access is inadvertently granted to offensive content.[38]

A sample[39] of the mistakes that can be found in censorware:

- BESS blocked the homepages of the Traditional Values Coalition and Massachusetts Congressman Edward Markey.
- Cyber Patrol blocked MIT's League for Programming Freedom, part of the City of Hiroshima website, Georgia O'Keeffe and Vincent Van Gogh sites, and the monogamy-advocating Society for the Promotion of Unconditional Relationships.
- CYBERsitter blocked virtually all gay and lesbian sites and, after detecting the phrase 'least 21', blocked a news item on the Amnesty International website (the offending sentence read, 'Reports of shootings in Irian Jaya bring to at least 21 the number of people in Indonesia and East Timor killed or wounded').
- I-Gear blocked an essay on 'Indecency on the Internet: Lessons from the Art World', the United Nations report 'HIV/AIDS: The Global Epidemic', and the homepages of four photography galleries.
- Net Nanny, SurfWatch, Cybersitter, and BESS, among other products, blocked House Majority Leader Richard 'Dick' Armey's official website upon detecting the word 'dick'.
- SafeSurf blocked the homepages of the Wisconsin Civil Liberties Union and the National Coalition Against Censorship.
- SmartFilter blocked the Declaration of Independence, Shakespeare's complete plays, Moby Dick, and Marijuana: Facts for Teens, a brochure published by the National Institute on Drug Abuse (a division of the National Institutes of Health).
- SurfWatch blocked such human-rights sites as the Commissioner of the Council of the Baltic Sea States and Algeria Watch, as well as the University of Kansas's Archie R. Dykes Medical Library (upon detecting the word 'dykes').
- WebSENSE blocked the Jewish Teens page and the Canine Molecular Genetics Project at Michigan State University.
- X-Stop blocked the National Journal of Sexual Orientation Law, Carnegie Mellon University's Banned Books page, 'Let's Have an Affair' catering company, and, through its 'foul word' function, searches for Bastard Out of Carolina and 'The Owl and the Pussy Cat'.

---

34 Electronic Frontiers Australia, *Internet Censorship in Australia* <http://www.efa.org.au/Issues/Censor/cens1.html>

35 See glossary

36 <http://censorware.net/article.pl?sid=01/02/10/2241204>

37 See glossary

38 Marjorie Heins & Christina Cho, 'Internet Filters: A Public Policy Report', National Coalition Against Censorship (Fall 2001) <http://www.ncac.org/issues/internetfilters.html>

39 Marjorie Heins & Christina Cho, 'Internet Filters: A Public Policy Report', National Coalition Against Censorship (Fall 2001) <http://www.ncac.org/issues/internetfilters.html>

The PICS/ICRA Illusion – Filtering and Rating. Attaching labels to content on the Internet is often promoted as a way to protect children from harmful content, while at the same time not preventing adult access to that information. One of the ways that has been promoted to create a child-friendly Internet was the PICS initiative, the 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.'[40]

Content labelling mechanisms have often been promoted as the best compromise in censorship, as they provide a selective filtering mechanism where the user or parent can choose what type of information is filtered. It remains a popular alternative to censorship in government circles and with industry lobbyists. But it is unrealistic to have any expectations about labelling technology; the debate has been going on for more than seven[41] years and very little progress has been made. Discussions about content labelling are mostly theoretic, and the words 'if adopted' are often repeated.

Content labelling is unlikely to succeed because it suffers from the chicken and egg problem. As long as it is not widely used, users have no incentive to label the content on their website. And content labelling will never be widely used if insufficient users have labelled the content on their site. A user that today turns on label-based content filtering in their browser effectively blocks access to most of the Internet, not exactly a display of a user-friendly technology that is likely to be adopted spontaneously by large amounts of people.

An additional problem with any content labelling system is the integrity of the label that the user attaches to his or her site. If someone had the intention to sabotage and pervert the

content labelling system, he could mislabel offensive content as being suitable for all ages – with obvious effects.

There are quite a few concerns about content labelling in the civil liberties community. These concerns revolve around the fact that once information is labelled, it becomes very easy for a government to set up national systems of censorship based on these labels. Part of this concern has been 'that governments would enforce or coerce the use of PICS facilitated systems. The probability of mandatory self-rating and prosecution for inadvertently mis-labelling, or failing to label, became obvious.'[42]

Content rating and filtering is one of three pillars in the EU Safer Internet Action Plan, and eight million euros have been allocated to projects that study rating or facilitate and create rating and filtering technology.[43]

Child Pornography. In every debate about censorship child pornography is put forward as an argument in defence of online censorship. Child pornography and predatory behaviour are problems on the Internet, and can be encountered in obscure places. But it is not realistic to think that censorship is a solution. The illegal nature of the content causes it to be distributed underground, in chatrooms and transient newsgroups. The content and offenders are difficult to trace, and the communities that distribute it are not easily accessible to the general public.

Child pornography is a law enforcement problem. There is no country in the world where the distribution of this type of content is legal; it is the only content where a degree of global consensus has been reached. Law enforcement agencies

40 W3C Platform for Internet Content Selection <http://www.w3.org/PICS/>

41 Chronology: PICS development and Internet censorship proposals at <http://www.libertus.net/liberty/picsrisk2.html#1995>

42 'The Net Labelling Delusion: Saviour or Devil' <http://libertus.net/liberty/label.html>

43 EU Information Society, 'Safer Internet Action Plan' <http://europa.eu.int/information_society/programmes/iap/index_en.htm>

routinely investigate online child pornography, and are having a good success rate. Agencies are co-operating internationally to combat the problem. Law enforcement agencies have become proactive in recent years and undercover sting operations are used, such as the FBI's Innocent Images Task Force.[44]

Some Internet service providers have blocked access to certain newsgroups that are routinely used to exchange images containing child pornography.

Hotline Systems. In June 1996 a hotline was established in the Netherlands to combat child pornography online.[45] This hotline provides a facility for Internet users to report child pornographic content on the Internet. The hotline has a permanent liaison with the Dutch criminal investigation unit, and reports are forwarded to this unit. The hotline was a direct response to community concerns about child pornography on the Internet, and the fact that law enforcement agencies were unprepared to address this problem. Hotlines have since been established in Australia, Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Spain, Sweden, the UK and the USA.[46] The modus operandi of these hotlines varies, some hotlines will issue take-down notices, some will report illegal content to the police, some do both.

Hotlines provide an intermediate facility to report illegal content, as many law enforcement agencies do not yet provide quick and efficient mechanisms to report a complaint. One would expect government and law enforcement agencies to eventually take over the functions that hotlines are currently providing, because one usually reports a crime directly to a government agency, and not to a third party NGO.[47]

Hotline systems are one of three pillars in the EU Safer Internet Action Plan, and 1,975 million euros have been invested by the European Commission in hotline projects.[48]

Commercial Censorship – Intellectual Property and Copyrights

Peer-to-Peer. Software-piracy[49] has existed since the beginning of software. It has always been possible to find illegal copies of virtually any software product online. Illegal software is distributed through a variety of technologies, the World Wide Web, the Usenet newsgroups[50], the File Transfer Protocol[51], and more recently through peer-to-peer technology.

Software companies have learned to live with the fact that any copyright protection mechanisms will be broken, however sophisticated they may be. There are software patches[52] and tools available to break the copyright protection mechanisms of almost any available software product. It is a matter of pride for pirates to publish new software or software cracking tools[53] before, or just after, the product arrives in the shops.

It is only in recent years that content, such as music and screen content, has become digitized. Digitized content has very similar attributes to software, such as ease of online distribution and problems with copyright protection mechanisms that are routinely broken. Technologies such as Napster[54] and other peer-to-peer protocols, together with the arrival of broadband technologies in the home, provide a convenient and enormously popular method for the sharing of software, music and screen content among users.

---

44 'FBI Fights Child Pornography Online', *The Oregonian*, 20 November 2002 <http://www.oregonlive.com/news/oregonian/index.ssf?/xml/story.ssf/html_standard.xsl?/base/news/1037797091130520.xml>

45 <http://www.meldpunt.org/>

46 See the list of members of The Association of Internet Hotline Providers in Europe at <http://www.inhope.org/english/about/members.htm>

47 See glossary

48 EU Information Society, 'Safer Internet Action Plan' <http://europa.eu.int/information_society/programmes/iap/index_en.htm>

49 – 54 See glossary

The music industry counter-attacked by pursuing Napster and other companies such as Morpheus[55] and Kazaa[56] in the courts. Napster closed down, but peer-to-peer file sharing technologies fragmented into a dozen different networks and are more popular than ever. Most of these networks have no central point of control such as Napster had, making it impossible to litigate against a single entity to close down these networks.

'On July 25, 2002, Representative Howard Berman (D-Cal.) introduced a bill, H.R. 5211 in the House of Representatives that would give copyright owners the right to violate the law in their efforts to stop the unauthorized circulation of their works on peer-to-peer networks.'[57] If passed this bill would allow copyright holders to organize sabotage against copyright infringement, a form of state sanctioned cyber terrorism. The bill has not yet passed, and has been referred to the US Subcommittee on Courts, the Internet, and Intellectual Property.[58]

A recent research paper published by computer scientists working for Microsoft Corporation concluded that attempts to stop the swapping of copyrighted works on online peer-to-peer networks will not work.[59]

Denial of Service Attacks.[60] A denial of service attack is a form of censorship, because it disables access to information through sabotage and flooding.

Although H.R. 5211, if passed, will allow copyright holders the right to attack piracy, such attacks are already happening to some degree. On peer-to-peer networks one is likely to find many spoof files. Certain newsgroups, where pirated software is exchanged, are regularly bombed with thousands of empty messages.[61]

The best documented denial of service attacks against content on the Internet were organized by members of the Church of Scientology (CoS).[62] CoS members or sympathizers

have tried to permanently erase the newsgroup <alt.religion.scientology> by issuing forged control messages that remove the group from Usenet news servers around the world. When that failed, they bombed the newsgroup with thousands of duplicated messages, in order to silence the discussion among critics of the church. Individual messages from critics were also routinely cancelled (erased).

Search Engine Censorship. Search engines have become an important access tool to the Internet. It is the tool of choice for people to locate information, and for some people it has taken the place of the Universal Resource Locator (URL)[63] method of typing the entire address of a website.

CoS is a litigious organization, and lawyers are often used to intimidate critics and other organizations in order to prevent dissemination of copyrighted or critical materials. In May 2002 the church 'threatened to sue Google[64] for contributory copyright violations for merely listing links to Web pages that, the Scientologists said, illegally published copyrighted passages. The church demanded that Google remove the links to the site, Operation Clambake[65], from its automated search results.'[66] The request resulted in the removal of an entire website, xenu.net, from the

---

55, 56 See glossary

57 The Berman P2P Bill: Vigilantism Unbound <http://www.eff.org/IP/P2P/20020802_eff_berman_p2p_bill.html>. A copy of the bill can be found at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h5211ih.txt.pdf>

58 Bill Summary & Status for the 107th Congress, H.R. 5211 status <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR05211:@@@X>

59 BBC News <http://news.bbc.co.uk/2/hi/technology/2502399.stm> Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, *The Darknet and the Future of Content Distribution* <http://crypto.stanford.edu/DRM2002/darknet5.doc>

60 See glossary

61 See alt.2600.warez newsgroup

62 – 65 See glossary

66 'Scientology, Google and the First Amendment', *San Jose Mercury News Editorial*, 2 May 2002 <http://www.siliconvalley.com/mld/siliconvalley/business/columnists/3185788.htm>

Google search archive. CoS typically requests removal of all content on a site, alleging 'wholesale, verbatim copyright infringement'.[67] Once Google became aware of the discrepancy between the alleged copyrighted works, and the actual copyrighted works, it quickly restored access to most of the blocked website.

Harvard Law School researchers found at least one hundred sites missing from search results when accessing Google sites meant for French and German users.[68] Google does not include certain websites in the French and German versions of its search engines, in particular neo-Nazi or white supremacy sites that have content that might be deemed illegal to publish in France and Germany.

China in late August blocked access to the Google and altavista Internet search engines for a brief period[69], diverting users to local Chinese search engines instead.

Actions against Online Censorship – Routing around Censorship. Online censorship is a technological battle. Online censorship becomes more sophisticated every day, but so do the tools that circumvent filtering.

Mirroring.[70] Mirroring of information is the oldest form of anti-censorship technology. When a website gets censored, people usually mobilize to copy the content of that site to dozens of other websites around the world. There are many examples of such mirroring in the short history of censorship on the Internet. Mirroring is an extremely effective technique against censorship, and also very easy to apply. The censor would have to block all the mirrors of a site to completely prevent access to the controversial information.

IP Rotation. In 1995 the entire XS4ALL website, hosting thousands of users, was blocked by German Internet providers in an attempt to block access to a radical magazine on that site. The block consisted of a refusal by German ISPs to route to

the IP address of the XS4ALL website. As a countermeasure XS4ALL employed an IP rotation mechanism that changed the IP address of the website every couple of minutes.[71]

Triangle Boy. Safeweb, a company that received funding from In-Q-Tel, the CIA's venture fund[72], released software called 'Triangle Boy'. The software is a peer-to-peer application that volunteers download onto their PCs. A user that has been denied access to any website by a censor can use the Triangle Boy software to circumvent the censorship.[73] Currently the Triangle Boy software only provides access to the *Voice of America*, because this service is blocked by the Chinese Government.

Peekabooty. 'The goal of the Peekabooty Project is to create a product that can bypass the nation-wide censorship of the World Wide Web practised by many countries.'[74]

'Peekabooty uses a complicated communications system to allow users to share information while revealing little about their identity. When a node receives a request for a web page it randomly decides whether to pass this on or access the page itself. It also only knows the address of its nearest partner. This makes it difficult to determine who requested what information and is designed to protect users from anyone trying to infiltrate the system from inside.'[75]

---

67 'Google Restores Church Links', *Wired News*, 22 March 2002 <http://www.wired.com/news/ebiz/0,1272,51257,00.html>

68 See Jonathan Zittrain and Benjamin Edelman, *Localized Google Search Result Exclusions. Statement of Issues and Call for Data* <http://cyber.law.harvard.edu/filtering/google/>

69 'The Shrinking Frontiers', *Online Journalism Review* <http://www.ojr.org/ojr/world_reports/1037922526.php>

70 See glossary

71 Message from Felipe Rodriquez to Michael Schneider about censorship countermeasures <http://www.xs4all.nl/~felipe/WWW.old/press/schneider.html>

72 Safeweb Website <http://www.safeweb.com/investors.html>

73 Safeweb Website <http://www.safeweb.com/tboy_service.html>

74 About the Peekabooty Project see <http://www.peek-a-booty.org/pbhtml/modules.php?name=Content&pa=showpage&pid=1>

75 'Peekabooty Aims to Banish Internet Censorship', *New Scientist*, 19 February 2002 <http://www.newscientist.com/news/news.jsp?id=ns99991948>

Peacefire.exe. 'Peacefire.org was created in August 1996 to represent the interests of people under 18 in the debate over freedom of speech on the Internet.'[76]

Peacefire created a Windows program, peacefire.exe that disables any popular Windows filtering censorware such as SurfWatch, Cyber Patrol, CYBERsitter, Net Nanny, X-Stop, PureSight and Cyber Snoop.

Internet Freedom Act. On 2 October 2002, US House Policy Chairman Christopher Cox and US House International Relations Committee Ranking Member Tom Lantos introduced legislation to counter Internet jamming and blocking around the world.[77]

When passed 'the United States will develop and implement a comprehensive global strategy to combat state-sponsored and state-directed Internet jamming. The Office of Global Internet Freedom, established within the International Broadcasting Bureau, will tap both private sector and government resources to help Internet users to avoid government censors and state persecution.'[78] The bill will, if passed, provide 50 million US dollars to help software companies develop anti-censorship software.[79]

Camera Shy. 'Camera/Shy is the only steganographic[80] tool that automatically scans for and delivers decrypted content straight from the Web. It is a stand-alone, Internet Explorer-based browser that leaves no trace on the user's system and has enhanced security.'[81]

Camera Shy is an application that enables stealth communications. Software like this can be useful in countries where e-mail communications are regularly monitored and censored, such as happens in China.

Proxy Relays. One of the easiest ways to circumvent censorship is to use a relaying proxy server. Proxy servers are a technology that was invented to speed up web traffic. It is an

intermediate server cache between the user and the web server, and popular content is cached on these servers. By configuring a web browser to use a relaying proxy server, government censorship systems can be bypassed.[82]

Akamai[83] can be used to bypass Internet censorship, and a description of how this can be done was written by Bennett Haselton.[84] Many large corporations use Akamai to optimize their Internet traffic distribution, the websites of these companies can be accessed by creating a special URL that uses Akamai as a relay server. This technique is in essence the same as using a proxy relay server for circumvention.

> He halted and, with bewildered and horrified eyes, stared round him at the khaki mob, in the midst of which, overtopping it by a full head, he stood. 'How many goodly creatures are there here!' The singing words mocked him derisively. 'How beauteous mankind is! O brave new world …'
> *Aldous Huxley – Brave New World*

Conclusions. The Internet is a reflection of the global society that we live in. The anarchist cookbooks are there, and so are the holocaust revisionists and consumers of bestiality. The availability of such content is a consequence of living in a global information and communications environment. In a global

76 About Peacefire see <http://www.peacefire.org/info/about-peacefire.shtml>

77 Bipartisan, Bicameral Bill Stops Internet Jamming <http://policy.house.gov/html/news_release.cfm?id=111>

78 Bipartisan, Bicameral Bill Stops Internet Jamming <http://policy.house.gov/html/news_release.cfm?id=111>

79 'China's Cyberwall Nearly Complete', *Wired News* <http://www.wired.com/news/politics/0,1283,56195,00.html>

80 See glossary

81 Project Camera Shy, summary <http://sourceforge.net/projects/camerashy/>

82 Relaying proxy servers, see <http://www.cexx.org/anticens.htm>

83 See <www.akamai.com>

84 Bennett Haselton, *Using Akamai to Bypass Internet Censorship* <http://www.peacefire.org/bypass/Proxy/akamai.html>

environment effective online censorship can only be implemented in strongly repressive environments or in situations where there is some form of global consensus and co-operation.

Implementing any kind of online censorship is a technological battle, any censorship technology can, and will, be defeated. To get a feeling for the inventiveness of people in defeating technological restrictions one only has to look at the history of software piracy, where companies have employed increasingly sophisticated protection mechanisms, only to see them cracked within days by skilled hackers. Implementing censorship has become a technological battle that cannot be won, except in extremely repressive regimes.

China has the most comprehensive censorship system and is having a degree of success with its implementation; this is being achieved by employing 30,000 people and using a mix of technological and repressive instruments. It is not certain that China will be able to keep up this censorship framework in the next decade. Savvy Internet users in China are not affected by the censorship; they can use technological tools and solutions to circumvent it, although there is always the risk of informers or active government surveillance of their activities

For a democratic nation there are no simple solutions. No democratic nation has come close to sanitizing the Internet in order to uphold the local community standards. The debate about content labelling remains just that: a debate. Despite EU investments and studies into content labelling technologies, there are no indications that the technology will provide us with a Holy Grail of online filtering. It is more likely that the online community will ignore labelling technology, because there are no incentives to start using it.

Sometimes the job of the politician consists of managing the perceptions of the electorate. From that point of view it is perhaps understandable that so many proposals have been

made to sanitize the Internet. But implementation is another thing altogether, and most plans that aim to clean up the smut on the Internet are either technically unfeasible or they require a form of global consensus among users and publishers of content or need enormous resources. Despite years of debate about filtering offensive content on the Internet no actions have actually led to a changed environment in any of the democratic nations. Odds are that this will remain so in the coming decade.

If there is consumer demand for filtering, for example to protect minors, then companies will jump at this opportunity to provide products and services that meet the demand. Products are already available, and although none of them are perfect, at least having these products gives the consumer the autonomy of making the decision to censor himself and his family. In any government sanctioned censorship framework that choice is taken away, with the likely side effect of censoring legal and uncontroversial content.

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 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.

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.

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.

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.

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

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 1936 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.

Jennifer Jenkins is the Interim Director of the Center for the Public Domain at Duke University, USA, and is a specialist in intellectual property rights who received her J.D. and M.A. in English from Duke. She was one of the lawyers involved in defending the publication of the novel *The Wind Done Gone* in Suntrust v. Houghton Mifflin, and in a variety of other intellectual property cases. She is also a filmmaker and musician. Her video on appropriation and intellectual property, *Nuestra Hernandez*, was shown at the New York University conference 'A Free Information Ecology in the Digital Environment' and at the Duke University 'Conference on the Public Domain'.

Verena Metze-Mangold, Ph.D., is Head of the Co-ordination Department of the Hessischer Rundfunk, Frankfurt and Vice-president of the German UNESCO Commission. She studied Political Science, Sociology and History at the University of Marburg and graduated with honours. She has journalistic experience in broadcasting and in print media and was head of the Protestant Medienakademie, Frankfurt, (1976-1987) and of the Communications Department of the Public Broadcasting Station, Frankfurt.
Ms. Metze-Mangold represented the German Government at the advisory conference on the South African Constitution, where she presented models of freedom of information acts and a broadcasting law, as well as at the Stability Pact Conference on media development in Eastern and South-Eastern Europe in May 2001. She is the author and editor of several books and numerous articles on international media development.

Felipe Rodriquez founded the first Dutch Internet service provider XS4ALL in 1993, and acted as its CEO until 1997. In his role as CEO, Mr. Rodriquez was involved in a number of high profile disputes concerning Internet politics. He worked together with the Belgrade-based radio station B92 to broadcast its radio signal live on the Internet after it was censored by the Milosevic regime. He co-founded the Amsterdam Digital City Network in 1994. In 1995, he created the Dutch ISP Association and chaired it until 1997. In 1996 he conceived the first Internet hotline (www.meldpunt.org) to combat the distribution of child pornography on the Internet. He is currently a member of the boards of various organizations and companies.

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 is 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. Homepage: <www.spaink.net>

Sandy Starr (Sandy.Starr@spiked-online.com) 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 is also a member of the UK & Ireland Working Group of RightsWatch (www.rightswatch.com), a European Commission research project which investigates copyright regulation. He writes for publications ranging from the *Times Literary Supplement* to *The Sun* newspaper, and is a contributor to the book *The Internet: Brave New World?*

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.

Karin Spaink
Verena Metze-Mangold
Páll Thórhallsson
Sandy Starr
Jennifer Jenkins
Felipe Rodriquez

www.osce.org/fom