Background Paper

on

Freedom of Expression and Internet Regulation

for the

International Seminar on Promoting Freedom of Expression With the Three Specialised International Mandates

London, United Kingdom
19-20 November 2001

Introduction

The Internet has fast become a key instrument for the exercise of the right to freedom of expression. It combines within one medium both the right to receive as well as the right to express and disseminate information, ideas and opinions, be it in the form of writing, or through audio or video.

As a vehicle for expression, the Internet serves various functions. It is simultaneously a publishing tool and a communications tool, allowing millions around the world to communicate instantaneously at the cost of a local call. It brings the ability to broadcast to an audience of millions within the reach of everyone with access to a computer and a telephone line; it serves as a huge multi-media library of information on topics ranging from human rights to deep-sea exploration and it is being used as an important educational tool, with Universities offering courses over the Internet. Governments use it to make information available and even public health services have gone on-line to provide self-help information. Increasingly, traditional media such as newspapers and radio stations are also going 'online', thus enriching Internet content, providing a bridge between the 'paper-world' and cyberspace and ensuring world-wide access to local papers. In addition, the Internet has developed an important entertainment function, providing for example on-line movies, games or music events. It has also developed a crucial commercial function, with more and more businesses trading over the Internet, selling everything from computers to holidays to flowers. As has been noted, "the Internet is as diverse as human thought."[1]

However, it is precisely because of its diversity of content and ease of use that the Internet has become controversial. As with any other tool, it can be used for different purposes. On the one hand, for example, it allows up-to-date news about current events to emerge from countries where other communication means are heavily

[1] *ACLU v. Reno*, 929 F. Supp. 824, 830-849 (ED Pa. 1996) at 842 (District Court Opinion).

censored.[2] On the other hand, the Internet can be used to facilitate crime. In addition, because of the global nature of the Internet there are problems with regard to content. Material that is perfectly legal in the country where it is 'uploaded' may be illegal in the country where it is 'downloaded', for example because it is considered to be obscene or politically subversive. Increasingly, therefore, the case is put for stronger Internet regulation. This raises important issues with regard to the right to freedom of expression, and it is with these issues that this briefing paper is concerned.

This paper aims to draw out the most important questions with regard to Internet regulation and freedom of expression. First, it discusses the issue of Internet access. This includes the question whether public authorities are under a positive obligation to provide access, for example by providing Internet terminals in libraries or other public places, as well as a discussion of various measures that have been taken in countries such as Saudi Arabia and China to restrict access to the Internet. Second, this paper discusses the issue of content regulation, including through self-regulation by Internet Service Providers and the use of blocking and filtering software. Third, this paper will discuss the chilling effect that excessive monitoring and surveillance has on freedom of expression on the Internet, whether by the State or by private actors such as employers, and how anonymity software and encryption may be used to protect freedom of expression on-line.

These issues are all discussed in the context of the legal guarantee of the right to freedom of expression. This paper approaches the issues in terms of the function of the Internet as a tool to disseminate as well as to receive information. As a briefing paper, it does not attempt to provide definitive answers; rather, points for discussion are stated at the end of each section.

[2] This was illustrated for example by events earlier this year, when the truth about a deadly school explosion spread across Chinese chat rooms, disproving earlier official denials of responsibility and forcing Chinese Premier Zhu Rongji into a rare public apology: 'China's Willing Censors', Tom Malinowski, *The Washington Post*, 20 April 2001.

Providing Access

The growing importance of the Internet means that access has become an important public issue, in terms of both restrictions as well as measures to promote and even provide access. In some countries, such as the United Kingdom, the government has pledged to provide computers to all low income families to prevent exclusion from the 'information society'. The same issue is at stake internationally, where the growing poverty-gap between 'information-rich' and 'information-poor' countries means that concerted action is necessary to bridge the international 'digital divide'. At the same time, in a number of countries public policy actually has the effect of limiting Internet access, for example by requiring users to register. Such access restrictions may be imposed by the State, or even by private parties; there have been a number of cases where Internet Service Providers (ISPs) have acted independently to refuse access to certain users whom they deem 'undesirable.'

This briefing paper discusses both the extent of positive obligations to promote access and the compatibility of measures to restrict access with the right to freedom of expression.

Positive Measures

As the Internet grows more diverse and includes information on numerous socially important issues, access to the Internet becomes increasingly important. Recently, governments have become aware of this and have started to take action, both at the national and at the international level.

At the International Level

Although the Internet is spreading in the developing world, the vast majority of Internet users continues to be found in the Western world. The Secretary-General of the International Telecommunications Union has warned that "[w]ithout action on the part of the world community, there is a very real danger that the global information society will be global in name only; that the world will be divided into the 'information rich' and the 'information poor'; and that the gap between developed and developing countries will widen into an unbridgeable chasm."[3] These sentiments have been echoed by United Nations (UN) Secretary-General Kofi Annan, who has pointed out that "[t]here are more computers in the United States of America than in the rest of the world combined. There are as many telephones in Tokyo as in all of Africa."[4]

With their generally poor telecommunications infrastructure, African countries in particular are in danger of being left behind. Research predicts that three-quarters of Africans will never make a telephone call, let alone use the Internet,[5] and what access there is is largely restricted to a small elite in the capital cities. This is particularly worrying given the Internet's potential for free expression, democratic empowerment and general the advancement of human rights and development.[6]

There is no single barrier to access. Not surprisingly, a recent report by the G8 group of industrialised countries identified a strong correlation between Internet penetration

[3] 'World Telecommunications Development Report 1998', International Telecommunciations Union, p. 1

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

[5] O. Coeur de Roy, 'The African Challenge: Internet, Networking and Connectivity Activities in a Developing Environment', 18 Third World Quarterly 5 (1997), p. 883.

[6] See *The Right to Communicate: The Internet in Africa*, ARTICLE 19: London, 1999.

and economic wealth,[7] but many other factors play a role. Poor infrastructure and the high cost of telecommunications are important impeding factors in many countries,[8] particularly in situations where one company has a monopoly over telecommunications,[9] while in other countries there is an even more basic problem – the lack of cheap, accessible electricity.[10] In addition, there is a need for sufficient training, technical expertise and basic education.[11] Finally, it is important that there is a structure for the protection of legal rights, including the right to freedom of expression.[12]

Already, individual donor countries as well as international agencies have instituted several ICT (Information and Communications Technology) projects to address the problems. For example, some individual donor countries have pledged considerable aid to bridging the digital divide, with the Japanese Government recently promising $15 billion over five years as part of a "Comprehensive Co-operation Package to Address the International Digital Divide."[13] In terms of international programmes, the United Nations Development Programme operates a 'Sustainable Network Development Programme', under the umbrella of which individual projects are supported such as the Malawi Sustainable Development Network Programme which is aimed at providing affordable Internet access particularly in rural communities.[14]

But the scale of the problem means that co-ordinated action is necessary on a number of fronts. There is growing recognition of this fact. Most recently, the UN has set up an Information and Communications Technology (ICT) Task Force. This is to take the lead within the UN to formulate strategies for the development of information and communications technologies, putting them at the service of development by forging partnerships between the UN, private industry and financing foundations and donor countries, programme countries and other stakeholders.[15]

A similar awareness exists at the policy-making level. Most recently, the G8 adopted a report by its 'Digital Opportunity Task Force', including the 'Genoa Plan of Action' which recommends:[16]

- international partnerships should be established to facilitate the setting up of Internet exchange points and national ISP associations in the Least Developed Countries (LDCs),[17] and the specific needs of LDCs should be taken into account while planning regional Internet backbones;

---

[7] *Digital Opportunities for All: Meeting the Challenge*, Report of the Digital Opportunity Task Force (*DOT Force*), 11 May 2001.
[8] This is the case in many countries in Central and Eastern Europe, as well as in other countries as diverse as South Africa, Jordan, Egypt, and Polynesia.
[9] 'Understanding the Digital Divide', OECD Report 2001, (http://www.oecd.org/dsti/sti/prod/Digital_Divide.pdf).
[10] *The Public Force and the Digital Divide: A Report to the DOT Task Force*, The Public Voice, March 2001 (http://www.thepublicvoice.org).
[11] *Ibid*.
[12] *Ibid*.
[13] As reported by the UNDP Communications Programme (http://www.undp.org/dpa/frontpagearchive/july00/21july00/index.html).
[14] 'Internet comes to rural Malawi', *Daily Mail and Guardian*, 3 August 1999.
[15] The ICT Task Force was to have its first meeting in September 2001; this was postponed because of the attacks on the WTC in New York, and the Pentagon and State Department in Washington (http://www.un.org/esa/coordination/ecosoc/itforum/icttaskforce.htm).
[16] Genoa Plan of Action proposed by the Digital Opportunity Task Force and adopted by the G8 Heads of State in Genoa, 2 July 2001 (http://www.dotforce.org/).
[17] Forty-nine countries are currently designated by the United Nations as "least developed countries" (LDCs) (http://www.unctad.org/en/pub/ldcprofiles2001.en.htm).

- telecommunications equipment and service providers should be encouraged to work in co-operation with LDCs to reduce costs and aggregate demand;
- efforts to mobilise public and private support for a significant improvement of basic information and communication infrastructure should be encouraged;
- information and communications technology programmes should be included in existing bilateral and multilateral official assistance programmes as a strategic, cross-cutting theme, while heads of relevant organisations should co-ordinate more on approaches and initiatives in order to avoid duplication;
- joint stakeholder efforts such as the African Partnership Initiative should be encouraged to address the connectivity dilemmas faced by African countries, with a view to achieving or promoting sustainable solutions, focusing on issues relating to telecommunications infrastructure. In this framework, it should be taken into account that information and communication technologies are an important means of supporting urban-rural linkages and strengthening small farmers, as well as micro-enterprises and small businesses;
- inclusion of developing country stakeholders (international organisations, governments, private companies, NGOs, citizens and academics) in global fora relevant to information and communications technology;
- the software community[18] should be encouraged to develop applications relevant to developing countries.

This follows on from several UN initiatives, starting with the July 2000 High Level Segment of the UN Economic and Social Council which was devoted to addressing the 'digital divide'. A Ministerial Declaration was adopted which, as well as stating a number of national action points, stresses that "[m]arket forces … alone will not suffice to put information and communications technology in the service of development…collaborative efforts are required, involving Governments, multilateral development institutions, bilateral donors, the private sector, civil society and other relevant stakeholders…Such efforts should include transfer of technology to developing countries on concessional and preferential terms [and] the mobilisation of resources, public and private, at the national and international levels, and promoting capacity-building."[19]

This has been endorsed by the UN General Assembly, which on 18 September 2000 adopted its 'Millennium Declaration' stating that "the benefits of new technologies, especially information and communications technologies, in conformity with recommendations contained in the ECOSOC 2000 Ministerial Declaration, [should be] available to all."[20]

Issues for discussion

- **How can we ensure that international actors more actively support the goals of providing universal access?**
- **What specific measures should international actors take to support this goal?**

<u>At the National Level</u>

While the Internet has become an important tool for the exercise of the right to freedom of expression, it can be very expensive. One commentator estimates the

[18] Including open-source as well as the commercial community.

[19] Ministerial Declaration of the high-level segment on development and international co-operation in the twenty-first century: the role of information technology in the context of a knowledge-based global economy, UN Doc. E/2000/L.9, par. 12 (http://www.un.org/documents/ecosoc/docs/2000/e2000-l9.pdf).

[20] UN General Assembly, 'Millennium Declaration', UN Doc. A/RES/55/2.

yearly cost of access, assuming a computer dedicated to the purpose, at US$2500.[21] This means that access to the Internet is out of the reach of many, even in the richer countries in western Europe, North America and Asia. For example, in the UK, only one in twenty low-income families has access to the Internet compared to one in two for the better off. Realisation of this inequity has led many governments to start to make Internet access available in public places. In addition to the United States and Europe, where it is increasingly common to see Internet terminals in libraries, in a number of other countries ICT centres (Internet 'call centres') are being set up in local communities where commercial access through Internet cafes is not viable.

Over the last few years, there have been moves in some countries to incorporate the provision of hardware in social programmes. The UK Government has announced a programme to help low income families access the Internet, providing some 100,000 recycled computers to low income families.[22] The scheme included a £10m initiative to wire up local communities and to provide training opportunities, as well as tax free loans of computers from employers to employees.[23] Such initiatives are not restricted to Europe. In Nigeria, the National Association of Community Banks is financing a project in conjunction with a local ISP to take Internet services to the grassroots with the opening of Cybercafes in all communities,[24] and in many countries ICT Centres are being established in co-operation with agencies such as UNDP.

Providing effective access could go further. Governments can actively promote Internet publishing, particularly when this will contribute to providing local content. The G8 Genoa Plan of Action states that "local content on the Internet should be strengthened and encouraged, including by encouraging governments to provide freely-available access to State-owned information and local content, except where it is genuinely private or classified."[25] Likewise, community broadcasters or newspaper publishers could be granted preferential access to publish on the Internet, including the provision of the necessary hardware and software as well as training.[26]

In law, access to the Internet is a fast developing area. It is already well-established that access to the means of communication is vital to the exercise of the right to freedom of expression. In 1982, the Committee of Ministers of the Council of Europe adopted a Declaration stating that Member States should seek to achieve "the availability and access on reasonable terms to adequate facilities for the domestic and international transmission and dissemination of information and ideas." The European Court of Human Rights has subsequently affirmed that the right to freedom of expression "applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive information."[27]

---

[21] This includes the cost of the computer and necessary peripherals, ISP and telephone charges: G. Granger, 'Freedom of Expression and Regulation of Information in Cyberspace: Issues concerning Potential International Co-operation Principles', in *The International Dimensions of Cyberspace Law*, UNESCO, Ashgate Publishing, Aldershot: 2000, p. 108.
[22] 'Internet 'wake-up call', *BBC News Online*, 28 October 1999 (http://news.bbc.co.uk/hi/english/business/your_money/newsid_490000/490583.stm).
[23] HM Treasury Press Release, 11 October 2000 (http://www.hm-treasury.gov.uk/press/2000/p111_00.html).
[24] 'Community Banks Take Internet Services To Rural Areas,' *This Day*, 15 February 2001 (http://allafrica.com/stories/200102150324.html).
[25] Genoa Plan of Action, *op. cit.*
[26] See Principle 3, Part III of the African Charter on Broadcasting 2001, adopted in Windhoek, Namibia.
[27] *Autronic AG v. Switzerland*, 22 May 1990, Application No. 12726/87.

These legal developments are not restricted to Europe. The US Supreme Court has often stated that access to the means of communication falls within the First Amendment guarantee of freedom of speech,[28] while the Zimbabwean Supreme Court observed in 1988 that "[t]oday, television is the most powerful medium for communications, ideas and disseminating information. The enjoyment of freedom of expression therefore includes freedom to use such a medium."[29]

However, the right to freedom of expression goes further than simply prohibiting interference with the means of communication; it includes a positive obligation on the State to make available those means of communication which are particularly important. In telecommunications, for example, the State is under some obligation to ensure the availability of cheap and accessible telephone lines. In the United States, this 'universal service' goal was written into federal telecommunications law as early as 1934.[30] The EU Voice Telephony Directive requires that all persons reasonably requesting it should be able to obtain a connection to the fixed public telephone network at an affordable price; the connection provided should be capable of national and international calls, supporting speech, facsimile and/or data communications.[31] Similarly, the Zimbabwean Supreme Court has stated that "[a] government committed to the grant of affordable telephonic communication for its people in the rural areas must be prepared to bear a portion of the expense required to promote such a commendable endeavour. The remedy lies in subsidising this social need, not in impacting upon a fundamental human right."[32]

UN organs have stressed that governments should take action to make the Internet more accessible, including by bringing down the price of access. In his report to the UN Millennium Assembly, UN Secretary General Kofi Annan urged Member States to pursue a development agenda which includes a "review [of] policies in order to remove regulatory and pricing impediments to Internet access."[33] Responding to this, ECOSOC adopted a Ministerial Declaration recommending that national programmes be established which "promote access to information and communications technology for all by supporting the provision of public access points." This was endorsed by the UN Heads of State at the Millennium Assembly.[34] Within the Council of Europe, similar Recommendations have been adopted.[35]

Issues for discussion

- **To what extent should the State be under a positive legal obligation to promote and provide Internet access;**
- **Should the State be under an obligation to promote local content? If so, how?**
- **What specific measures should States take to promote universal Internet access?**

---

[28] E.g. *Red Lion Broadcasting Co. Inc. v. FCC (No 2)* (1969) 395 US 367; *City of Los Angeles and Dept of Water and power v. Preferred Communications Inc.* (1986) 476 US 488; *Metro Broadcasting Inc. v. FCC* (1990) 497 US 445.

[29] Quoted with approval in *Belize Broadcasting Authority v. Courtenay and Hoare* [1988] LRC (Const) 276, at 284.

[30] 47 USC 254, quoted in *Bridging the digital Divide: Internet Access in Central and Eastern Europe*, Global Liberty Internet Campaign (www.gilc.org), March 2000.

[31] Directive 98/10/EC, 26 February 1998, OJ L101/24, 1 April 1998.

[32] *Retrofit (Pvt) Ltd. v. Minister of Information, Posts and Telecommunications* [1996] 4 LRC 512, at 516.

[33] *Millennium Report*, *op cit.*, Key Proposals, http://www.un.org/millennium/sg/report/key.htm.

[34] United Nations Millennium Declaration, 18 September 2000, Doc. A/RES/55/2, Art. 20.

[35] See in particular Recommendation R(99)14 on Universal Community Service concerning New Communication and Information Services, 9 September 1999.

Restrictions on Access

In a number of countries, public policy has the effect of controlling access to the Internet. In certain States, access has been made virtually impossible because there is no national 'link' to the Internet. An individual in such a country who wants to use the Internet would have to dial up a foreign Internet Service Provider (ISP), thus incurring international telephone charges. In other countries, Internet users are required to register and Internet cafes and ISPs need to obtain a licence before being allowed to operate. At the same time, a trend is developing where groups or individuals are denied access to the Internet by private parties. There have been recent instances when ISPs have grouped together to deny access to users who are deemed likely to publish morally or otherwise undesirable material. Such restrictions, whether imposed by private parties or by the State, pose important questions with regard to the right to freedom of expression.

Prohibition of Access

The most overt and extreme way of restricting and censoring access to the Internet is by prohibiting access altogether. Today, North Korea and Afghanistan are among the last countries in the world not to have a link to the global Internet. It is apparent that the decision not to provide any Internet access is politically motivated. It is easy to establish a national gateway link to the global Internet backbone; even Sierra Leone, which ranks last on the UNDP development list, has one.[36]

In some other countries, Internet access is restricted to the government elite. This is the case in Burma, for example, where a only few privileged people (entrepreneurs and people close to the generals in power) can connect to the Internet, using the country's national telecommunications operator.[37] Until very recently, the situation in Afghanistan was similar; while there is no local link-up, Pakistani servers provided access via international lines to ministerial departments at 'preferential prices'.[38]

Registration and Licensing Requirements

Apart from an outright refusal to provide access, the most overt form of restricting access is to impose a requirement for all Internet users to register with the authorities, or to require Internet users to obtain a licence before being allowed to publish on the Internet, or even to use the Internet passively.

Regulation of this kind may be found in Iraq, where citizens need to obtain a licence before being allowed to install a modem, satellite dish or fax at home, while the only ISP in the country is run by the Ministry for Information and Culture. There are now four Cybercafes in Baghdad, all under the direct authority of the Government. Independent entrepreneurs are not allowed to open this kind of business.[39] The current situation in China provides another example of this kind of regulation. Access to the Internet is heavily controlled, with the Government requiring both ISPs and individual users to register. Internet cafes need to obtain a licence from the People's Security Bureau (PSB) and are required to install a variety of monitoring and filtering packages (for further detail on this, see below).[40]

Under human rights law, registration requirements for publishers are of very doubtful legitimacy. In a recent case, the UN Human Rights Committee considered a law

---

[36] *UNDP Human Development Report 2001* (http://www.undp.org/hdr2001/).
[37] *The Enemies of the Internet*, RSF: Paris 2001, (http://www.rsf.fr/uk/homennemis.html).
[38] *Ibid*.
[39] *The Enemies of the Internet*, *op cit*.
[40] 'Freedom of Expression and the Internet in China: A Human Rights Watch Backgrounder', Human Rights Watch 2001 (http://www.hrw.org/backgrounder/asia/china-bck-0701.htm).

which required all publishers, no matter how small their publication, to register with central authorities. The Committee considered that such a requirement established "such [an] obstacle as to restrict the author's freedom to impart information".[41] There was no evidence that the measure was necessary for the protection of public order or for the protection of the rights of others. Therefore, the requirement constituted a violation of the right to freedom of expression. A registration scheme such as the Chinese one goes even further than this, requiring not only those who publish on the Internet to register with the police, but imposing a registration requirement on all users, including those who use the Internet passively. This poses a significant restriction on the right of Internet users freely to receive information as well as exerting a serious chilling effect on the right of Internet publishers to disseminate information. This is particularly so when, as is the case in China, registration and licensing schemes go hand-in-hand with extensive surveillance operations, which have a serious chilling effect on on-line speech and are driven by the political desire to suppress undesirable political speech.

Issues for discussion

- **Can a registration requirement for ISPs be compatible with the right to freedom of expression? What about for individual users?**

The Role of ISPs

In many countries, ISPs are being forced to police access to the Internet. In China, for example, ISPs are obliged by law to monitor their users and report any misuse to the authorities. While public authorities in many other countries refrain from such overt action, there is some pressure on ISPs not to host sites that contain undesirable content. A good example is the establishment of the Internet Watch Foundation (IWF) after the Metropolitan Police sent a letter to all United Kingdom ISPs, notifying them of a number of newsgroups that contained sexually explicit material and reminding them that the publication of obscene material is an offence in the UK.[42]

In other countries, ISPs have acted on their own accord. In Sweden, for example, the website Flashback (http://www.flashback.se) was refused access by all Swedish ISPs. Flashback is a website which allows discussion on controversial subjects such as nazism, paedophilia and Hell's Angels, as long as the communications comply with Swedish legislation. The site is now hosted by a foreign ISP.[43] Such action is increasingly likely in other countries, with ISPs including 'proper use' clauses in their customer contracts. The standard contract of the Danish ISP Cybercity, for example, includes the following: "Homepages must not contain any kind of pornography, racist expressions or expressions, which might degrade minority groups or people with certain sexual orientations".[44] Similarly, the terms of service of Yahoo!'s Geocities, one of the largest providers of free web-pages in the world, bind customers not to publish anything that is "harmful, threatening, abusive, harassing … or otherwise objectionable".[45] This is so broadly worded as to give Geocities free rein in censoring customers' sites.

---

[41] *Laptsevitch v. Belarus*, 20 March 2000, Communication No. 780/1997, para. 8.1 (http://www.unhchr.ch/tbs/doc.nsf/MasterFrameView/cc98a0722c3d4c62c125690c003636a2?Opendocument)

[42] A copy of the letter is on http://www.cyber-rights.org/documents/themet.htm; for a discussion of the policy issues see http://www.cyber-rights.org/reports/governan.htm.

[43] This case is discussed in *Internet and Freedom of Expression*, Rikke Frank Jørgensen, LL.M. thesis (unpublished), Raoul Wallenberg Institute.

[44] Quoted in *Internet and Freedom of Expression*, *op cit*.

[45] Section 5B, Member Conduct (http://docs.yahoo.com/info/terms/geoterms.html).

With ISPs increasingly taking part in self-regulatory schemes, it is likely that once a site has been refused by one provider, it will find it difficult to get hosted by another. The IWF operates a hotline for child pornography, non-consensual adult pornography and 'criminally racist' material.[46] The latest IWF Annual Report sets out the procedure: "The trained staff of the IWF investigate each report and make a professional judgement as to whether the reported material is indeed potentially criminal under UK law. If it is, and it is hosted by an UK Internet service provider, the relevant ISP is advised to remove the material."[47] If the hosting ISP is based abroad, the IWF will contact its counterpart in the relevant country. According to the published statistics, the vast majority of actioned reports concerned newsgroup postings (some 11,000 in 1999) and 220 reports concerned websites.[48]

It is undesirable that ISPs act on behalf of the police as censors for two reasons. First, ISPs are not judicially qualified to determine whether a certain website might contravene the law or whether an individual user might be likely to publish something that is considered to be illegal. When faced with a borderline case, they are likely to err on the side of caution and decide not to host the site. Second, there are no safeguards to ensure that ISPs do not abuse their powers, and there is no system to call ISPs to account. This is problematic, particularly since the ISP's actions will have an important impact on the right to freedom of expression of those who they decide to refuse access, as well as the right of others to receive information. Users whose access rights are summarily restricted by a private party can hardly be said to receive a 'fair trial'.

The European Court of Human Rights has held that the State is under a positive obligation to take action where a threat to freedom of expression comes from a private source. It is now well-established that:

> [I]n addition to the primarily negative undertaking of a State to abstain from interference in Convention guarantees, 'there may be positive obligations inherent' in such guarantees. The responsibility of a State may then be engaged as a result of not observing its obligation to enact domestic legislation.[49]

The Inter-American Commission on Human Rights similarly has held that the right to freedom of expression includes:

> [T]he freedom that the State should have guaranteed for [the victim] to express and impart his ideas, as well as the complementary freedom of all citizens to receive such information without illegal or unjustified interference.[50]

In a case in which a broadcaster had refused to carry advertising from an animal welfare campaign group in Switzerland, this meant that the State should have taken pro-active measures to protect freedom of political speech. In the instant case, this was particularly urgent because the threat came from a powerful private media group. A similar case could be made if a number of ISPs acting collectively under a

---

[46] See http://www.iwf.org.uk.
[47] *Annual Report 2000*, IWF: London 2001, p. 7.
[48] The statistics can be accessed at http://www.iwf.org.uk/hotline/stat/stat.htm.
[49] *Vgt Verein gegen Tierfabriken v. Switzerland*, 28 June 2001, Application No. 24699/94, para. 45.
[50] *Oropeza v. Mexico*, 19 November 1999, Report No. 130/99, Case No. 11.740 (Inter-American Commission on Human Rights), para 53.

self-regulatory scheme decided to refuse to host a particular website or organisation.[51]

Issues for discussion

- **What steps should States take to protect users against action by ISPs to limit their access to the Internet? In particular, how can unpopular, or even offensive, but legal speech be protected?**

[51] *Ibid.*

Regulating Content

One of the biggest strengths of the Internet – its variety of content – has simultaneously become a matter of some controversy. Governments in both Islamic and Western States have voiced great concern over the free availability on the Internet of pornography. The use of the Internet for criminal purposes has also been cause for concern. The US Attorney General has said: "While the Internet and other information technologies are bringing enormous benefits to society, they also provide new opportunities for criminal behaviour."[52] These are real and worrying concerns; the use of the Internet to promote paedophile activities, for example, constitutes a very real threat to the human rights of children and may legitimately be restricted.

However, any content regulation must not fall below the standards set by international human rights law, and must take into account the special nature of the Internet. In Europe, North America and Australia, there has been a considerable backlash against government attempts to regulate Internet content. Content restrictions are often seen as censorship, and the US Supreme Court has struck down various legislative proposals to restrict the availability of 'obscene' or 'indecent' material for this reason. A further problem with nationally-imposed content regulation is that a situation is developing whereby various countries each attempt to enforce their national laws over the global Internet. Crudely put, there is a perceived danger that the entire Internet might succumb to the standard of the least tolerant regulator. Third, enforcement of content regulation has led to questions of liability, particularly for Internet Service Providers (ISPs) who, in some countries, have been held liable for the content of Internet pages published by their customers. For these reasons, self-regulation has been hailed as the preferred alternative. Initially, this focused on the development of blocking and filtering software to enable 'parental control'. However, when this software began showing promise it was quickly co-opted by governments around the world. Other forms of self-regulation, including the operation of 'hotlines' for undesirable content and the development of a 'global ratings mechanism' have been criticised as representing government censorship in a corporate guise.

Legal Measures

International standards on content regulation

While States can legitimately take action to regulate Internet content, under international human rights law any limitations on expression must remain within the strict parameters set by Article 19(3) of the International Covenant on Civil and Political Rights:

> [Restrictions on the right to freedom of expression] shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.

This means that any restriction must meet a strict three-part test, as recognised by the Human Rights Committee. Any restriction must a) be provided by law; b) be for the purpose of safeguarding one of the legitimate interests listed; and c) be necessary to achieve this goal.

[52] US Department of Justice, 10 January 2000, Press Release 00-007.

The first condition, that any restrictions should be 'provided by law', is not satisfied merely by setting out the restriction in domestic law. Legislation must itself be in accordance with human rights principles set out in the ICCPR.[53] The European Court of Human Rights, in its jurisprudence on the similarly worded ECHR provisions on freedom of expression,[54] has developed two fundamental requirements:

> First, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[55]

The second condition requires that legislative measures restricting free expression must truly pursue one of the aims listed in Paragraph 3, namely the rights or reputations of others or the protection of national security, public order ('ordre public') or of public health or morals.

The third condition means that even measures which seek to protect a legitimate interest must meet the requisite standard established by the term "necessary". The European Court of Human Rights has established that this is a very strict test:

> '[The adjective 'necessary'] is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable". [It] implies the existence of a "pressing social need".[56]

Furthermore, any restriction must restrict freedom of expression as little as possible.[57] The measures adopted must be carefully designed to achieve the objective in question and they should not be arbitrary, unfair or based on irrational considerations.[58] Vague or broadly defined restrictions, even if they satisfy the "provided by law" criterion, are unacceptable because they go beyond what is strictly required to protect the legitimate interest.

Internet content regulation that fails to pass scrutiny under any part of this test cannot be considered legitimate under international human rights law.

Legislating Internet content

Any legislation aimed at regulating Internet content should furthermore recognise that the Internet is not like any other medium. In many cases, it will not be possible to extend general norms to the Internet, or to apply the standards that are normally applied to, for example, broadcasting, to Internet content. The special nature of the Internet will need to be taken into account. With regard to defamation, for example, it should be recognised that a defamatory publication in the New York Times will have a different impact from a defamatory publication on an Internet site. And even within the Internet, it should be taken into account that a possibly defamatory publication on a large website like that of the BBC News will have a totally different impact from a

---

[53] *Faurisson v. France*, Decision of 8 November 1996, Communication No. 550/1993 (UN Human Rights Committee).
[54] Article 10(2) ECHR.
[55] *Sunday Times v. the United Kingdom*, Judgment of 26 April 1979, para. 49 (European Court of Human Rights).
[56] *Ibid.*, para. 59.
[57] *Handyside v. the United Kingdom*, Judgment of 7 December 1976, para. 49 (European Court of Human Rights).
[58] See *R. v. Oakes* (1986), 26 DLR (4th) 200, at 227-8, (Canadian Supreme Court).

possibly defamatory posting on an obscure newsgroup, or a personal homepage which attracts no more than a few visitors per week.

The best-known example of legislation that attempted to extend off-line standards to on-line conduct has been the United States Communications Decency Act (CDA), signed into law by the US President in February 1996 and struck down by the US Supreme Court in June 1997.[59] The main purpose of the CDA was to restrict access by minors to "patently offensive depictions of sexual or excretory activities" available over the Internet. The Act was immediately challenged and the relevant portions were eventually ruled unconstitutional because they restricted expression on the entire Internet to the level that would be appropriate for children. One of the problems was that the drafters of the CDA had failed to distinguish between the Internet and other forms of expression. Whereas in broadcasting or print media, restrictions can be placed with regard to time and manner of transmission, or the place of publication, this is not possible with regard to the Internet.[60] The special factors that are internationally recognised as justifying regulation of the broadcast media – such as the history of extensive government regulation of broadcasting,[61] the scarcity of available frequencies,[62] and its 'invasive' nature[63] - do not apply to the Internet.[64]

The decision reveals a number of important factors. First, it distinguishes the Internet from other media and explains that what may be appropriate for other media, for example broadcasting, may not be justified when applied to the Internet. Second, the decision indicates that it is not possible simply to lower the standard for all speech to what is suitable for children; this is not compatible with the right to freedom of expression. Third, it recognises that there is no Internet equivalent to 'the top shelf' in a Western book shop, or a 'watershed' time after which material that is unsuitable to minors may be shown. The Internet cannot be divided into different areas, some of which are accessible to adults only.

Issues for Discussion

- **How can rules rendering content otherwise illegitimate be applied to the Internet without undermining its potential to promote the right to freedom of expression? What specific regulatory measures could be employed?**

Conflict of laws

One of the most important distinguishing features of the Internet is its global nature. Something that is uploaded in a small room in Bishkek, for example, is immediately accessible throughout the world. However, there are no globally agreed rules on Internet content; generally speaking, every country is free to enforce its own standards, provided that these do not fall below the threshold set by international human rights law.

This has led to some unexpected cases. Recently in the Australian State of Victoria, a local businessman was able to sue Dow Jones for on-line defamation – even

[59] *Reno v. American Civil Liberties Union*, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997). For a succinct account of the CDA saga, see Y. Akdeniz, *Sex on the Net*, South Street Press, Reading: 1999, p. 27-30.
[60] *Reno v. American Civil Liberties Union*, *op cit*, at p. 17-21.
[61] See, for example, *Red Lion Broadcasting Co. v. FCC*, 395 U. S. 367, 399–400 (US Supreme Court).
[62] See, e.g. *Informationsverein Lentia v. Austria*, 28 October 1993, Application Nos. 13914/88, 15041/89, 15717/89, 15779/89, 17207/90 (European Court of Human Rights).
[63] E.g. *Sable Communications of Cal., Inc. v. FCC*, 492 U. S. 115, 128 (US Supreme Court).
[64] *Reno v. American Civil Liberties Union*, *op. cit*, at p. 22-24.

though the Dow Jones website is created in New Jersey. It was argued on behalf of the defendant that entrenching current defamation laws on the net would have a chilling effect on free expression, and that the court should not accept it was right to erect a 'firewall' to prevent Australians knowing via the net what people in other countries were reading and saying about businessmen. However, the judge ruled that "publication takes place where and when the contents (are) comprehended by the reader". This meant that Australian law was applicable, even though the article discussed the US securities market, had been written by an American reporter for US consumption and had been uploaded in New Jersey. It is possible that, had the case been tried in the US courts, it might have been dismissed. The problem is not restricted to Australia; similar cases have been heard in Germany and France.[65] These cases are particularly difficult to resolve when it concerns two countries whose laws would both pass scrutiny under international human rights standards.

It has been argued that "the global nature of the Internet should give new relevance to the concept 'regardless of frontiers' found in human rights instruments."[66] Already, there have been cases before the European Court of Human Rights in which the trans-border availability of material was an issue. In the Spycatcher case, Judge Martens remarked that "in this 'age of information', information and ideas cannot be stopped at frontiers any longer."[67] The case concerned the continuing injunction on the publication in the UK of details taken from a book written by a former member of that country's Security Service, which was freely available in other countries in the United States and Europe. The same point was made by judges Pettiti and Farinha in their Joint Opinion: "In the era of satellite television it is impossible to partition territorially thought and its expression or to restrict the right to information of the inhabitants of a country whose newspapers are subject to a prohibition."[68]

Some inspiration might be drawn from satellite broadcasting regulation. In this area, too, there is a problem of global content that is potentially subject to a multitude of different national legal systems. The World Trade Organisation has been firmly opposed to the application of strict national content regulation of satellite broadcasting; it advocates a much lighter touch. This is in recognition of the fact that it would be unnecessarily restrictive if national governments were to attempt to enforce domestic law over a trans-national medium. This does not mean that the answer necessarily lies in the establishment of global, or even regional content norms. The European Union 'Television Without Frontiers' Directive[69] recognises that even within the relatively small region that is the European Union, there are no uniform standards of public morality. As the EFTA Court explained in 1997, "the mental and moral development of minors forms an important part of the protection of public morality, an area where it is not possible to determine a uniform European conception."[70] It might be more fruitful to seek to achieve a solution by agreeing common rules on jurisdiction, such as those which are found in regional treaties such

[65] For example, see *The People v. Felix Somm*, 17 November 1999, File no. 20 Ns 465 Js 173158/95 (Munich Regional Court); *UEJF and Licra v. Yahoo!*, 20 November 2000, No. 00/05308 (Tribunal de Grande Instance de Paris).
[66] GILC Position Paper, at http://www.gilc.org.
[67] *Observer and Guardian v. the United Kingdom*, 26 November 1991, Application no. 13585/88, Separate Opinion, Judge Martens, at para. 12.3.
[68] *Ibid*, Partly Dissenting Opinion of Judge Pettiti, joined by Judge Pinheiro Farinha.
[69] Directive 89/552/EEC, 3 October 1997, as amended by EU Directive 97/36/EC
[70] *TV 1000 Sverige AB v. Norway*, 12 June 1998, Case E-8/97, OJ C275, 3 September 1998, p. 6, at para. 26.

as the EEC Convention on Jurisdiction and the Enforcement of Judgments in Civil and commercial Matters.[71]

Issues for discussion

- **How can the desire of governments to apply legitimate national laws to the Internet be reconciled with the need to prevent a lowest common denominator on the Internet? What specific mechanisms can be developed in this area?**

ISP Liability

The question whether Internet Service Providers (ISPs) should be held liable for content that is published by their subscribers has recently become controversial. ISPs argue that because they provide access to thousands, or even millions, of users, usually as a purely commercial service, it is impossible for them even to monitor the content of their servers, let alone police them. Others argue that there should be some form of liability if an ISP has been warned that there is illegal content on their servers but they fail to take action.

At present, different measures have been taken in different countries, and even within some countries there is a different rule depending on the nature of the case (civil/criminal). In civil cases in the United Kingdom, ISPs are liable for third party postings if they are aware of the content of the material and failed to take 'reasonable steps' to remove it.[72] The problem with such a rule is that it is likely to lead to ISP self-censorship as well as various other practical problems. For example, ISPs may receive a large number of alerts from individuals notifying them that hate speech are on their servers. A requirement for them to examine the material, decide whether it qualifies as, for example, hate speech and remove it will be excessively onerous in view of the large amount of alerts they are likely to receive. Moreover, ISPs are in a purely commercial relationship with their users and, if challenged, they have little reason to protect them. Therefore, they are likely to err on the side of caution and remove most if not all of the material that is challenged.

For these reasons in some countries, such as the United States and Germany, ISPs have been afforded far-reaching protection from liability for postings by third parties.[73]

Issues for discussion

- **Should Internet Service Providers, having been notified that potentially illegal material is present on their servers, be liable for that content if they take no steps to remove it?**

Filtering and Blocking by Law

For some time, filtering and blocking technologies have been promoted as a technological alternative to the enactment of national laws regulating Internet content. Whilst initially developed as tools to help parents control which sites their children can access (hence names as 'Net-nanny' and 'Cyber-sitter' for the first

---

[71] EEC Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, adopted in Brussels, 27 September 1968, OJ L 299 31 December 1972, p. 32 (Consolidated Version).

[72] *Godfrey v. Demon Internet Ltd* [1999] 4 All ER 342. See also the recent High Court ruling in *Venables and Thompson v. News Group Newspapers Ltd.*, 10 July 2001, QB (not yet published).

[73] Section 230 of the US Communications Decency Act (although this does not apply to child pornography or to copyright-related matters); Section 5(3) of the German Information and Communications Services Act.

commercially available packages), in many countries there are now moves to require such software to be installed at public terminals, or to install filtering software at ISPs or national gateways. These developments pose important questions in the context of freedom of expression.

First, most commercially available filtering mechanisms continue to be both over-inclusive, for instance filtering out anti-racism or gay-rights websites, and under-inclusive, inasmuch as they fail to detect a significant amount of illegitimate material. A recent study in the United States found some of the sites of the following human rights organisations were blocked by widely-used filtering devices: Amnesty International, the American Kurdish Information Network, the International Gay and Lesbian Human Rights Commission, Dalitsan (an organization working to protect the rights of "Untouchables" in India), the Milarepa Fund (an organization which raises awareness about human rights violations in Tibet) and Human Rights and Tamil People.[74] While filtering software continues to improve and the manufacturers are open to suggestions for improvement, these vagaries of impact are of doubtful compatibility with any principle of freedom of expression.

One way to by-pass the under- and over-inclusiveness issue would be to rate all sites according to a standardised system. Such a system could be voluntary or government imposed. The Australian government has taken the first steps towards imposing a system which mandates blocking of Internet content based on existing national film and video classification guidelines. The Broadcasting Services Amendment (Online Services) Bill places sweeping restrictions on adults providing or gaining access to material deemed unsuitable for minors as determined by Australian film and video classification standards. The United States Government has argued for similar measures. In its unsuccessful defence of the Communications Decency Act, it argued that the use of an Internet "tagging" scheme would serve as a defence to liability under the Act. This scenario would have required online speakers to tag material as indecent in a manner that would facilitate blocking of such content. Various big industry players, including AOL, Bertelsmann, Netscape and Microsoft, have now come together to work on a voluntary 'global ratings system' (discussed below, under 'Self Regulation').

Second, while filtering software was initially promoted as a tool that could be used by parents at home, there is now a trend whereby blocking and filtering software is installed at libraries and on other public terminals. Proponents of the installation of filtering software on such systems argue that particularly where Internet terminals are provided as a public service, the State has a right to ensure that the terminals are used for socially relevant purposes rather than to access pornography. Opponents argue that this constitutes State-licensed censorship, which is always unacceptable.

Software similar to that used in parental control technology is used in some countries to exclude politically undesirable content from the web altogether. China is the best-known example of this practice. A 'Great Wall' has been erected on the national gateways, blocking access to any sites the government deems undesirable. This includes the BBC and CNN websites, as well as the websites of NGOs such as Amnesty International and freechina.org. An even more restrictive system is in place in Saudi Arabia. Although little detail is available on how the system works, one press report has claimed that an internal committee has decided on a list of acceptable

[74] B. Haselton, 'Amnesty Intercepted: Global Human Rights Groups Blocked by web Censoring Software', reprinted in *Filters and Freedom 2.0: Free Speech Perspectives on Internet Content Controls*, Electonic Privacy Information Center, Washington DC: 2001, at p. 79.

Internet sites; any other sites are blocked by default.[75] Blocking software is also in place in India, where the Government-owned service provider controls all international Internet gateways. In the last week of June 1999, at the height of the Kashmir crisis, Indian Internet users in India were unable to access the online news site of the Pakistan Daily Dawn, which was known for its independent coverage of the crisis.

A national strategy to block access to sites that are deemed undesirable clearly constitutes prior censorship, which is presumptively invalid under international human rights law. In a case involving the black-listing of books, the Inter-American Commission on Human Rights stated that such measures restrict both the right of the authors to disseminate information, and the rights of others to receive information.[76] The European Court of Human Rights held, in a case involving a refusal of the Austrian Government to distribute certain magazines to members of the army, that a selective interference with the right to freedom of expression "could … only have been justified by imperative necessities since exceptions to the freedom of expression must be interpreted narrowly."[77] Even self-imposed filtering in a public place such as a school or library raises serious questions regarding the right to freedom of expression. Such measures limit the right to receive information of those who are dependent on public terminals to access the Internet, depriving them from a wide range of information on topics that may be controversial or unpopular and hence filtered out. At the moment, US legislation that mandates the use of filtering software in government-funded libraries is being challenged in the courts on precisely these grounds.[78]

Finally, all filtering schemes, whether mandatory or self-imposed, pose important questions with regard to openness, transparency and accountability. At present, there is very little detail with regard to the operation of filtering software, the list of sites blocked, and the technical systems employed to decide which sites to filter out.[79]

Issues for discussion

- **Can a national filtering or blocking strategy which does not require prior approval of the courts ever be legitimate as a form of prior censorship?**
- **Is a policy to install filtering and blocking software on public Internet terminals compatible with the right to freedom of expression?**

Non-Legal Measures

Industry self-regulation

Because of the many difficulties associated with mandatory content regulation of the kind described above, self-regulation has been hailed by many western countries as the answer. This carries few of the disadvantages of mandatory content regulation;

---

[75] Quoted in *Al-Jazeera* newspaper, 6 May 1998, as reported in *The Internet in the Mideast and North Africa – Free Expression and Censorship*, Human Rights Watch: New York 1999, p. 53.

[76] *Pathfinder v. Grenada*, 1 March 1996, Report No. 2/96, Case No. 10.325 (Inter-American Commission on Human Rights).

[77] *Vereinigung Demokratischer Soldaten Osterreichs and Gubi v. Austria*, 19 December 1994, Application No. 15153/89 (European Court of Human Rights), at para. 37.

[78] ACLU Press Release, 26 July 2001 (http://www.aclu.org/news/2001/n072601c.html).

[79] *Who watches the watchmen: Part II – Accountability and Effective Self-Regulation in the Information Age*, Cyber-Rights & Cyber-Liberties (UK) report, September 1998 (http://www.cyber-rights.org/watchmen-ii.htm).

no special criminal offences are created and no country would be attempting to enforce its national laws on the global Internet. There is considerable enthusiasm for the concept within the industry and governments in Western countries are cautiously supportive. In countries where use of the Internet is tightly controlled, no truly self-regulatory schemes can at the moment be said to exist; content regulation is required by law.

However, self-regulatory schemes, too, pose difficult questions with regard to the right to freedom of expression. Some existing schemes have been set up with government support, and the establishment of at least one self-regulatory scheme has been prompted following 'suggestions' by the police that self-regulation might be beneficial to the Internet industry. This raises serious questions with regard to the independence of such schemes. Second, and more fundamental to the right to freedom of expression, there are questions of self-censorship, and censorship by commercial parties on behalf of the State. In practice, ISPs appear increasingly willing to comply with requests that they shut down sites, or that they block access for their users to a particular site or group of sites. In Switzerland, for example, the three largest ISPs recently announced that they will block access to a server which is alleged to host 754 racist or anti-Semitic sites. This decision was taken after the ISPs received notification of the sites' content from 'Children of the Holocaust', a Basel-based NGO that runs an 'observatory' of racist Internet sites.[80]

All these issues have come to the fore with the creation in 1996 of the Internet Watch Federation (IWF) in the United Kingdom.[81] Although this is a voluntary association of the major players in the UK Internet industry, its creation was prompted by a letter sent by the police, threatening, in effect, that unless ISPs took action to restrict the availability on the Internet of illegal pornography, prosecutions would follow.[82] The IWF was subsequently set up in consultation with the police and the Home Office. This raises questions as to their independence, even if formally government has no representation on the IWF's board. Part of the IWF's remit is to 'take down' material reported to it that is judged 'criminal'. In the period since its creation in 1996 until 2000, it has dealt with a total of 162440 reports, of which 25790 items were found to be hosted in the UK and have been taken down.[83] These are significant numbers, and raise the question which criteria the IWF uses to determine whether or not an item is 'potentially illegal'. There is no judicial determination by an independent body.

In addition, there is an evolving trend of industry 'stealth blocking', where ISPs take a decision to block certain sites without notifying their customers or the sites involved. For example, between August and December 2000, the 'Global Internet Liberty Campaign' (GILC), a coalition of various Internet rights groups, found that it could no longer send e-mail to one of its member organisations. It transpired that the member organisation had been blacklisted by GILC's ISP.

A key problem for self-regulatory bodies is how to determine whether a site is 'potentially illegal.' This led to proposals that Internet publishers should be required to rate their sites according to content. In May 1999, the major industry players formed the 'Internet Content Rating Association' (ICRA) to "try to create the first world

[80] 'Nazi web platform blocked by Swiss Internet Service Providers', *SwissInfo*, 19 February 2001 (http://www.swissinfo.org/sen/Swissinfo.html?siteSect=111&sid=584058).
[81] For more on the IWF, see http://www.iwf.org.uk.
[82] The letter can be seen at http://www.cyber-rights.org/documents/themet.htm.
[83] *Annual Report 2000*, *op cit*. The Annual report speaks of a total of 16244 reports; we assume this is a typing error.

standard" on Internet content. An 'Internet Content Summit'[84] was held in September 1999, organised by ICRA together with INCORE (Internet Content Rating for Europe), and a "Memorandum on Self-Regulation of Internet Content" was adopted. The Memorandum contains practical recommendations for governments, industry and users to work together in developing a new culture of responsibility on the Internet. Its creator, Yale professor Jack Balkin, acknowledged that the rating system proposed in the Memorandum would not represent a global standard: "There can be no [common] description for blasphemy in Saudi Arabia…Neither can hate speech or political speech be satisfactorily rated…It's a leaky system, [but] it's the best you can do."[85]

At the policy level in the US and Europe, there is strong support for self-regulation.[86] Within the Council of Europe, the Committee of Ministers recently adopted Recommendation R(2001)8, which strongly advocates the establishment of self-regulatory mechanisms in all Member States.[87] While reaffirming and stressing the importance of the continued development of new communications and information services to further the right to freedom of expression, it notes that these should not "prejudice the human dignity, human rights and fundamental freedoms of others - especially of minors." But bearing in mind different standards in different countries, particularly with regard to the criminal law, as well as the fact that self-regulatory initiatives for the removal of illegal content are already under way in several Member States, it recommends that it should be left to a forum of Internet actors to establish regulatory mechanisms.

In the context of freedom of expression, self-regulatory schemes pose several further questions. First, and most important, is the issue of industry-censorship. Many have criticised the proposals because it would simply replace government censorship with industry censorship. The US-based Center for Democracy and Technology criticised the ICRA plans as "jeopardising free expression on the Internet [by] promoting a single, comprehensive global rating system developed with government involvement or backed by government enforcement" which, "in the name of self-regulation" would encourage ISPs to collaborate with governments to control speech that is legal but "considered offensive by some". To an extent, this is worse than government censorship; there are no accountability or transparency mechanisms nor are there any safeguards to prevent over-zealous censorship by the industry. Second, with regard to the proposed rating mechanism, the question has been asked how this can be enforced. Human rights activists have expressed concern that "the imposition of civil or criminal penalties for 'mis-rating' … is likely to follow any widespread deployment of a rating and blocking regime."[88] Third, while the industry proposals are promoted as setting a 'global standard', this claim is untenable. What is proposed is a western standard, and arguably an American one. None of these questions have been tested in court yet.

Issues for discussion:

---

[84] http://www.bertelsmann-stiftung.de/internetcontent/english/frameset_home.htm.

[85] Quoted in M. Heins, 'Filtering Fever', reproduced in *Filters and Freedom 2.0: Free Speech Perspectives on Internet Content Controls*, *op cit*., p. 23.

[86] For EU policy, see the 'Safer Internet Action Plan' described at http://europa.eu.int/information_society/programmes/iap/index_en.htm.

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

[88] Global Internet Liberty Campaign, *Member Statement Submitted to the Internet Content Summit* (http://www.gilc.org/speech/ratings/gilc-munich.html).

- **Is self-regulation the preferred way to regulate Internet content? How can current schemes be improved?**

Self-regulation at home

The least intrusive mechanism for controlling what appears on your computer screen is through 'self-regulation at home'. There are various ways to achieve this. Filtering mechanisms can be installed on home computers. Instead of imposing strict controls on what individuals can upload and make available on the web, filtering software would leave the choice to the user. A concerned parent can simply install some software on the computer that filters out and blocks access to any content s/he deems unsuitable to children (based on parameters fed in by the user). Although this software still suffers from the drawbacks described above, if installed voluntarily at home they do not represent government control, and people can decide for themselves whether or not to install them.

In addition, there now exist several self-styled 'family-friendly' ISPs, such as ViaFamily Online, who advertise on the basis that they provide a filtered Internet service.[89] Families who sign up with these services make a conscious choice not to have access to part of the Internet, and accept voluntarily the risk that the ISP may block certain sites that are legitimate.

However, even these measures still raise problems with regard to the right of children to freedom of expression as guaranteed under both the ICCPR and the Convention on the Rights of the Child. As an alternative, a parent can choose to tackle the problem of the availability of 'undesirable' material on the Internet through education or supervision.

Issues for discussion:

- **Is 'self-regulation at home' the preferred way forward to control Internet content?**

[89] See http://www.viafamily.com/.

Monitoring and Surveillance

The previous chapters discussed access regulation and content restrictions; monitoring and surveillance operations are the third way by which governments have attempted to control the flow of information over the Internet. In most countries, such monitoring has not been a new phenomenon; often, existing laws and practices on the interception of telecommunications have simply been extended to the Internet. Surveillance tactics are not solely used by States. In recent years, private actors have become involved, particularly in the workplace. In the United States, the majority of big companies now monitor their employees' use of the telephone and Internet.[90]

Surveillance and monitoring practices have a serious chilling effect on on-line expression. If an Internet user suspects that his or her on-line movements are monitored, he or she will exercise caution with regard to statements made or sites visited. Technology can provide some solace; anonymity and encryption tools are constantly developing and improving, and aim to protect users' online rights of privacy and freedom of expression. However, their success in doing so has meant that governments have tried to restrict the use of such software.

This chapter discusses monitoring and surveillance measures that have been proposed or taken in a number of countries, as well as recent attempts to regulate the use of anonymity and encryption software.

State Monitoring

States implement surveillance systems for different reasons. In countries such as Iraq, China or Belarus, law enforcement agencies are alleged to engage in wide-scale monitoring activities to prevent individuals within their jurisdiction from discussing politically damaging issues. In countries such as the United States or The Netherlands, monitoring takes place for law enforcement or national security-related purposes and interception warrants are granted only for these purposes.

While it is right that law enforcement agencies should have the tools they need to detect and prevent crime, the problem with much of the legislation that has recently been adopted in many countries is that it is too widely drafted and there are too few independent controls on its use.[91] In the wake of the 11 September attacks on the World Trade Centre in New York, there has been a flurry of legislative activity in the United States and in Europe to increase State powers to intercept electronic communications. In the United States, the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism USA (PATRIOT) Act of 2001' expands Internet monitoring capabilities.[92] In the same vein, the EU Council of Justice and Home Affairs Ministers has called on the European Commission (the main drafter of legislative proposals within the EU system) to "submit proposals for ensuring that law enforcement authorities are able to investigate criminal acts involving the use of electronic communications systems and

[90] 'Corporate Snooping on Rise: Active Monitoring of Employees Rises to 78%', *ABCNews.com*, 18 April 2001 (http://more.abcnews.go.com/sections/business/dailynews/snooping_010418.html).
[91] See, for example, the Human Rights Audit by JUSTICE and the Foundation for Information Policy Research of the Regulation of Investigatory Powers Bill, on-line at http://www.fipr.org.
[92] See, in particular, Sections 209, 210, 214, 216, 219 and 220 of the USA (PATRIOT) Act.

to take legal measures against their perpetrators."[93] However, these proposals have been criticised from various quarters. The EU Council's own Legal Service has warned that EU governments already have all the powers they need under existing law and that no extensions are required.[94] The American Civil Liberties Union has published a critical analysis of the USA Patriot Act, pointing out that it unnecessarily lowers the threshold for accessing Internet communications data while minimising judicial oversight over the authorisation and execution of surveillance warrants.[95] In the UK, newspapers report that new powers to intercept will not be restricted to anti-terrorist investigations; communications data gathered in the course of an investigation will also be available to police investigating minor crimes, as well as for tax collection and public health and safety purposes.[96]

These criticisms of recent legislation come in addition to long-standing suspicions that western security agencies abuse their monitoring powers. A January 1998 Report published by the Scientific and Technological Option Assessment (STOA) unit of the European Parliament provides a rare glimpse into one international surveillance system referred to as ECHELON. According to the report, ECHELON forms part of a system encompassing the UK, US, New Zealand and Australian governments and has been primarily designed to monitor non-military targets for commercial purposes, including governments, organisations and businesses.[97] Admissions that the system indeed existed followed,[98] and the European Parliament adopted a Resolution and a Report calling upon the EU Member States to provide their citizens with appropriate guarantees of privacy and confidentiality and to support the use by their citizens of encryption software.[99]

In other countries, it is an open secret that the Internet is being monitored. It is reported that in the United Arab Emirates and Saudi Arabia, software has been installed on ISP servers which can be used by the authorities to track which computer terminals were accessing which web sites and for how long.[100] While authorities in the U.A.E. deny monitoring individual Internet use, in Saudi Arabia users who attempt to access a blocked site receive a message on their screens warning that all access attempts are logged.[101]

In a separate and worrying trend, ISPs and Internet cafes in certain countries have been forced to take on the role of 'monitor'. An extreme example of such a situation is to be found in China, where ISPs and Internet cafes are under a legal obligation "to provide to the Public Security organisation information, materials and digital documents, and assisting the Public Security organisation to discover and properly

---

[93] Conclusions adopted by the Council (Justice, Home Affairs and Civil Protection), Brussels, 20 September 2001, Doc. SN 3926/6/01 REV 6 (http://ue.eu.int/Newsroom/).
[94] Opinion obtained by Statewatch, as reported in Statewatch News Update, November 2001, http://www.statewatch.org/news/.
[95] Available at http://www.aclu.org/congress/l110101a.html.
[96] 'Police get sweeping access to net data', *The Guardian*, 7 November 2001 (http://www.guardian.co.uk/Archive/Article/0,4273,4293489,00.html).
[97] For general information see http://www.echelonwatch.org.
[98] The admission was made in a Parliamentary Briefing Paper from the Dutch Minister for Defence, released in January 2001; see 'Witte oren van NSA luisteren alles af' (*The red-hot ears of the NSA listen to everything*), *De Volkskrant*, 24 January 2001 (http://www.volkskrant.nl).
[99] European Parliament Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), 11 July 2001, Doc. A5-0264/2001 PAR1; EP Resolution R5-0440/2001.
[100] *The Internet in the Mid-East and North Africa*', *op. cit*.
[101] *Ibid*.

handle incidents involving law violations and criminal activities related to computer information networks."[102] In practice, ISPs and Internet cafes have appointed their own monitors. For example, Sohu.com, a Nasdaq registered portal based in Beijing, monitors chatrooms and bulletin boards, deleting any objectionable content.[103] In many Internet cafes, managers have similarly appointed 'censors'. In Beijing's Feiyu Internet Café, these censors walk along the 800 computer units and read over the shoulders of the clients. Under rules issues by the Bureau of Industry and Commerce, the management of Feiyu is under an obligation to report all violators to the police. Similar legislation exists in Russia, where rules requiring ISPs to provide the security service with complete access to users' e-mail were challenged by one ISP based in Volgograd (all other ISPs complied). The rules, known as System of Efficient Research Measures 2 (SORM-2), were written by the Russian Federal Security Services and the State Communications Agency in 1998. Ultimately, the challenge never made it to court; the threat to revoke the ISP's licence was withdrawn.[104]

It is apparent that excessive monitoring and surveillance exerts a chilling effect on the right to freedom of expression. As the UN Special Rapporteur on Freedom of Expression has stated, "in the interception of communications a fair balance and proportionality should be maintained, with a view to safeguarding private communications and avoiding unnecessary restrictions on the use of encryption on the Internet."[105]

There exists a wealth of caselaw and national practice, from international institutions as well as from national jurisdictions, on which safeguards are needed to maintain the 'fair balance and proportionality' referred to by the Special Rapporteur.[106] The European Court of Human Rights has laid down a number of principles. First, all surveillance operations require a clear basis in law, and the laws must be readily accessible and sufficiently precise so that citizens will be aware of the circumstances in which they apply:

> [T]he requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and

---

[102] Management Measures of the PRC Regulations for the Safety Protection of Computer Information Systems (Jisuanji xinxi wangluo guoji lianwang anquan baohu guanli banfa.), in Jisuanji Ji Wangluo - Falu Fagui (*Computers and Internet -Laws and Regulations*), Falu Chubanshe, Beijing: 1999, p. 99. These regulations were published in full by some Internet cafés. See also the website of Feiyu, an Internet café in Beijing at http://www.feiyu.com.cn/wangba/fagui/jisuanji.htm.

[103] Article 15 of the September 2000 "Measures For Managing The Internet Information Services" lists eight categories of prohibited content, including criticism of the PRC Constitution and topics that damage the reputation of the State.

[104] Anne Nivat, 'BSK, the provider that says "niet"', *The UNESCO Courier*, March 2001 (http://www.unesco.org/courier/2001_03/uk/doss12.htm).

[105] Report of the Special Rapporteur, Visit to the United Kingdom of Great Britain and Northern Ireland, UN Doc. E/CN.4/2000/63/Add.3, 11 February 2000, para. 73.

[106] For an overview of international best practice and caselaw as well as recommendations on how to design a 'fair' surveillance system, see JUSTICE, *Under Surveillance: Covert Policing and Human Rights Standards*, London 1998 (http://www.justice.org.uk). Further comparative material may be found in a consultation paper by the Irish Law Reform Commission, *Privacy: Surveillance and Interception*, Dublin: 1996.

> the conditions on which the [authorities] are empowered to resort to this secret and potentially dangerous [measure].[107]

Moreover, the Court has stressed that "[i]t is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."[108] Second, surveillance operations have to be 'necessary' – "[an] adjective [that is] not synonymous with 'indispensible', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'reasonable', or 'desirable'"[109] – and proportionate, allowing the State to take only such measures as are strictly required to achieve the required objective. Finally, there must be safeguards built-in to the legislative framework to prevent abuse of surveillance capabilities:

> This assessment … depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law.[110]

Issues for discussion

- **What safeguards are necessary to avoid abuse of the monitoring capability of the State?**

Workplace Monitoring

Monitoring email and internet use in the workplace is relatively easy. If the organisation is networked, software can be installed centrally to track and monitor employees' Internet movements. If the organisation is not networked, software can be installed on individual computers. The software can analyse an organisation's entire email traffic phrase-by-phrase, drawing conclusions whether an individual message is 'legitimate company business' or not, it can be instructed to search for particular words or phrases, and some software can even analyse communication patterns.[111] Use of this software may be in addition to 'regular' filtering software as described above. Managers give a variety of reasons for installing the software, including to protect trade secrets, to prevent sexual harassment incidents, or to ensure that employees do not waste company time.

In the United States, it was estimated in April 2001 that nearly 80 percent of major companies monitor their employees' use of the Internet.[112] Strict action is sometimes taken. In August 2000, for example, Dow Chemical fired 24 employees and disciplined a further 235 for sending pornographic or violent emails, or for having

---

[107] *Malone v. the United Kingdom*, 2 August 1984, Application No. 8691/79 (European Court of Human Rights), para. 67.
[108] *Kruslin v. France*, 24 April 1990, Application No. 11801/85 (European Court of Human Rights), para. 33.
[109] *Handyside v. the United Kingdom*, 7 December 1976, Application No. 5493/72 (European Court of Human Rights), at para. 48.
[110] *Klass and others v. Federal Republic of Germany*, 6 September 1978, Application No. 5029/71 (European Court of Human Rights), para. 50.
[111] As described in Privacy International, *Privacy and Human Rights 2000* (http://www.privacyinternational.org/survey/).
[112] 'Corporate Snooping on Rise: Active Monitoring of Employees Rises to 78%', *ABCNews.com*, 18 April 2001 (http://more.abcnews.go.com/sections/business/dailynews/snooping_010418.html).

accessed such material on the Internet.[113] Xerox and the New York Times have dismissed workers in similar incidents. Cases such as these raise important questions: who decides which Internet sites are 'inappropriate'? What if employees are sent pornographic email by accident, maliciously, or as 'spam' (advertising sent by email)?

The phenomenon of 'workplace monitoring' can act as a restriction on workers' exercise of their right to freedom of expression. Employees who know that their email may be read by others and that their surfing habits are monitored will be careful in what they say or which sites to visit. However, it appears that standards on workplace monitoring are unresolved. In the United States, judges in the 9th US Circuit Appeals Court recently brought a temporary halt to the practice of Internet monitoring of court employees, over fears that it might be illegal under US law.[114] The monitoring was reinstated a week later and in August it was recommended that monitoring software be installed at all Circuits.[115] This Recommendation was severely criticised by some judges, who argued that it was invasive of the right to privacy.[116]

The European Court of Human Rights, on the other hand, has long held that workplace monitoring constitutes an interference with the right to respect for private life, which is protected under Article 8 ECHR and in similar terms under Article 17 ICCPR:

> [I]t is clear … that telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 para. 1.[117]

Accordingly, people have a 'reasonable expectation of privacy' at work, and any monitoring can take place only if it is 'in accordance with the law' and 'necessary in a democratic society' in pursuit of a legitimate aim. In none of the cases before it has the European Court considered separately the free expression issues arising from workplace monitoring; it considers that these are included in the privacy issues and requires sufficient safeguards to prevent abuse of monitoring powers.[118]

The International Labour Organisation (ILO) in 1997 adopted a Code of Practice on the Protection of Workers' Personal Data. On the issue of workplace monitoring, it provides:

> "5.16 Workers should not be monitored on a continuous basis, unless this is specifically justified for safety reasons. In such cases, workers should be informed about all methods of monitoring.
>
> 5.17 All forms of secret monitoring, including telephone tapping, video surveillance and electronic voice and mail searches should be strictly prohibited unless there is credible evidence of criminal activity or other serious wrongdoing.

---

[113] 'You've Got Offensive Mail: Dow Chemical Fires 24 Workers Over E-Mail Content,' *ABCNews.com*, 15 September 2000, at http://more.abcnews.go.com/sections/tech/dailynews/dowchemical000915.html.

[114] 'Judges Turn Off Monitoring – On their Own Computers', *Newsfactor.com*, 9 August 2001, at http://www.newsfactor.com/perl/story/12659.html.

[115] Press Release from the Administrative Office of the US Courts on Internet Monitoring of Judges & Judiciary Employees, Aug. 13, 2001.

[116] See for example the letter sent by Judge Edith H. Jones (5th Circuit), at http://www.eff.org/sc/judiciary.

[117] *Halford v. the United Kingdom*, 25 June 1997, Application No. 20605/92.

[118] *Ibid*, at para. 72;

> 5.18 Monitoring of individual workers or groups of workers to assess their performance should take place only if the workers are informed in advance of the means to be used, the time schedule and the data to be collected."[119]

Issues for discussion

- **In what circumstances can workplace monitoring be justified?**
- **What safeguards are necessary to avoid abuse of an employer's monitoring capability?**

Anonymity

Protection of anonymity is central to both the right to freedom of expression and to the right to respect for private life. Particularly in those countries where there is heavy State monitoring, anonymity tools can allow users to communicate with the outside world without fear of identification and reprisals. Anonymity tools have many other advantages, for example allowing anonymous whistle-blowing or on-line counselling, or allowing users to join in all forms of discussions. In addition, many human rights organisations, both nationally and internationally, rely on anonymous email to communicate with their contacts around the world. Examples include Burmese dissident groups and the Mexican Zapatistas. Users of the Critical Path AIDS Project's website, of Stop Prisoner Rape ('SPR') in the United States and of the Samaritans in the United Kingdom rely on anonymity. Many members of SPR's mailing list would not be involved were it not for guaranteed anonymity, such is the stigma of prisoner rape. It is fair to say, as one observer notes, that the use of anonymity tools by all these organisations "isn't incidental to their work, it's a key aspect of their strategy."[120]

The use of anonymity software has been criticised from different quarters. While the governments of countries such as China criticise it for allowing their citizens to bypass national firewalls, in other countries anonymity tools have been attacked for helping criminals to communicate freely. For example, a March 2001 White House report states that "[i]ndividuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections..."[121]

However, any restrictions on the use of anonymity tools will impact on the right to freedom of expression. Various courts have recognised that anonymity is an important pre-condition for the exercise of the right to freedom of expression, as well as of other rights. The principle was reaffirmed by the United States Supreme Court in a 1995 case involving the distribution of a leaflet opposing a proposed school tax levy:

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Great works of literature have frequently been produced by authors writing under assumed names. Despite readers' curiosity and the public's interest in identifying the creator of a work of art, an author generally is free to decide whether or not to disclose her true identity. The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern

[119] *Protection of workers' personal data: An ILO Code of Practice*, Geneva, ILO 1997.
[120] Yaman Akdeniz, 'The Privacy Issue: Anonymous Now', *Index online*, Issue 3 2000 (http://www.indexoncensorship.org/300/akd.htm).
[121] *The electronic frontier: the challenge of unlawful conduct involving the use of the Internet*, A Report of the President's Working Group on Unlawful Conduct on the Internet, March 2000, on-line at http://www.usdoj.gov/criminal/cybercrime/unlawful.htm.

> about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."[122]

Acting on this a US district judge has struck down State legislation that prohibited anonymous speech as overbroad and unconstitutionally vague.[123] The court held that the restriction on the use of anonymity was unacceptable. Although the restriction furthered a legitimate State interest (fraud prevention in this case), the legislation was not narrowly tailored to achieve it, "sweep[ing] innocent, protected speech within its scope."[124]

A recurring recent issue has been whether and to what extent the anonymity of users who post defamatory or otherwise unlawful messages on Internet message boards or chat rooms should be protected. In a recent case in which a plaintiff sought disclosure of the identity of an Internet user who had posted messages that were allegedly damaging to the plaintiff's business, the New Jersey Court of Appeals proposed a four part test:[125]

- The court should first require the plaintiff to attempt to notify the anonymous posters that their identities are being sought, preferably through a posting in the same forum where the impugned messages were first posted, and give the defendants an opportunity to oppose the request.
- The court must require that the plaintiff identifies the exact statements alleged to be unlawful.
- The court must then decide both whether the complaint establishes a *prima-facie* case and whether the plaintiff has sufficient evidence to support this case.
- Finally, "the court must balance the defendant's First Amendment right of anonymous free speech against the strength of the *prima facie* case and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to proceed."[126]

In a recent case in the UK, an ISP was ordered to disclose the identity of one of its users who was found to have posted *prima facie* defamatory comments.[127] The judge stressed that he was "satisfied that … the content of the postings … is plainly defamatory…[and] of a very serious nature, calling into question the claimant's solvency and the competence and integrity of its management and directors. [It] presents a very considerable threat to the claimant. The potential audience is vast [and without] geographical limit."[128] Although the judge did not require that the claimant should have attempted to notify the poster that his or her identity was sought to be disclosed, the balancing test is similar to the one proposed by the New Jersey Court of Appeals.

---

[122] *McIntyre v. Ohio* (1995) 115 S. Ct. 1511.
[123] *ACLU v. Miller* (1997) 977 F. Supp. 1228 N.D. Ga.
[124] *Ibid.*
[125] *Dendrite Int. Inc. v. John Does nos. 1-14*, 11 July 2001, File No. A-2774-00T3, New Jersey Superior Court, Appellate Division (http://www.citizen.org/documents/dendriteappeal.pdf).
[126] *Ibid.*, at p. 3-4.
[127] *Totalise plc v Motley Fool Ltd* [2001] EMLR 29, [2001] All ER (D) 213 (Feb), *The Times Law Reports*, 15 March 2001 (QB) (http://www.thetimes.co.uk/article/0,,12-99112,00.html).
[128] *Ibid.*, from Tape Transcript of Smith Bernal Reporting, pp. 11-12, (http://www.lawtel.com).

The European Court of Human Rights has affirmed the fundamental status of anonymity in the context of journalists' protection of sources. In *Goodwin v. the United Kingdom*, the Court recognised that the role of the press as a watchdog in a healthy democratic society can be undermined if journalists are not allowed to keep the sources of their information confidential. It stated that "[w]ithout such protection, sources may be deterred from assisting the press in informing the public on matters of public interest."[129]

Issues for discussion

- **What restrictions on the use of anonymity tools on the Internet would be compatible with the right to freedom of expression?**
- **Under what conditions, if ever, should ISPs or others be required to disclose the identity of a user?**

Encryption

There has been a rising demand for strong encryption as a means of guaranteeing confidentiality of telecommunications. Software freely available over the Internet produces encryption so strong it would take current computers millions of years to decode keys only several hundred digits long. The message can still be intercepted, but without the decryption key it will contain nothing but a seemingly meaningless series of symbols. The value of such a tool to human rights organisations around the world is immense, allowing them to communicate with correspondents in countries where email is likely to be intercepted and read by the authorities without fear of reprisals. ARTICLE 19, for example, relies on PGP, one of the strongest tools available, to communicate with its representative in Belarus.[130] In the last few years, encryption tools have also received strong support from the commercial sector as they are indispensable for the development of on-line commerce and secure payments over the Internet.

In spite of its value as a commercial as well as a freedom-enhancing tool, governments continued until recently to use export controls or other national laws to limit public access to strong encryption technologies. Encryption was seen as military technology not to be sold to others. This was significant because the strongest and most user-friendly encryption tools were designed in the US; export controls meant that they could not be made available to interested parties outside the country.[131] Only recently have governments begun to relax export controls, mainly because of the strong commercial lobby.[132] But as development and export controls were relaxed, other laws have been tightened up. The US authorities, in particular, have fought a lengthy rearguard action against the spread of 'uncrackable' cryptographic tools. A number of proposals have been put forward, from the mandatory installation of decryption hardware in all telecommunications equipment to a requirement for all users of encryption to lodge their keys with central government agencies, but none of these proposals have been survived. In the United Kingdom, the Regulation of Investigatory Powers Act 2000 mandates yet another system, requiring Internet users to hand over their encryption keys when asked to do so. Critics have pointed out that

[129] *Goodwin v. the United Kingdom*, 22 February 1996, Application No. 17488/90, para. 39.
[130] 'Pretty Good Privacy' (PGP) is an encryption package that can be downloaded for free and is widely regarded as 'uncrackable'.
[131] Phil Zimmerman, the inventor of PGP, was for a long time under threat of prosecution for allegedly exporting it, which he denied.
[132] For example, the Pro-CODE (Promotion of Commerce in a Digital Era) Bill introduced in US Congress by Senator Burns (http://www.aclu.org/issues/cyber/priv/priv.html).

the Act's provisions on key disclosure fall foul of the right not to incriminate oneself, while the Act as a whole has a chilling effect on the right to freedom of expression.[133]

Such regulation appears at odds with the undeniable value of encryption as a tool that enhances freedom of expression on the Internet. It also contradicts the recent call from the European Parliament that Member States should support encryption:

> [The European Parliament urges] the Commission and Member States to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software;
>
> Calls on the European institutions and the public administrations of the Member States systematically to encrypt e-mails, so that ultimately encryption becomes the norm.[134]

A similar recommendation has been adopted by the Committee of Ministers of the Council of Europe.[135]

Critics of regulation of encryption point out that attempts to restrict encryption are futile in any event. Even if the use of encryption software were banned completely, other technologies exist that are even harder to detect and crack. For example, steganographic software allows the user to 'hide' messages in the 'digital noise' that is contained in image files. If properly encoded, it is impossible to detect that a message is hidden in such a file.[136]

Issues for discussion

- **Are any restrictions on the use of encryption compatible with the right to freedom of expression?**
- **What about the various rules relating to handing over encryption keys? What safeguards are necessary to prevent abuse of the power to require keys to be handed over?**

Conclusion

The Internet offers great potential for the exercise of the right to freedom of expression and freedom of information. However, like any tool for expression, it can be used in good and in bad ways. Attempts over the last few years to regulate Internet content as well as access to the Internet have tended to focus on restricting the availability of certain content and, in some cases, restricting access to the Internet altogether. While it is acknowledged that freedom of expression is not an absolute right, this briefing paper has identified a number of areas where regulation has been too heavy-handed. The Internet should not be used by governments as an excuse for introducing new technologies of control or for curtailing existing liberties. Although the right to freedom of expression can be restricted, the circumstances under which this may be done have to be narrowly circumscribed. This is the case for expression on the Internet as it is in any other forum. Given the *ad hoc* nature of many national initiatives, it is necessary that international mechanisms give a clear

---

[133] See, for example, the 'Human Rights Audit' of the Bill commissioned by JUSTICE and the Foundation for Information Policy Research, *op. cit*.
[134] European Parliament Resolution R5-0440/2001, paras. 29-34.
[135] Recommendation R(99)5 on the protection of privacy on the Internet, adopted on 23 February 1999.
[136] For further information on steganography, see http://www.outguess.org.

indication of the extent to which regulation of the Internet is compatible with the international legal guarantee of the right to freedom of expression. In addition, this paper has identified a number of areas where positive action may be needed, to promote access to the Internet as well as the development of local content. Here, too, international mechanisms can play an important role by indicating the extent of positive action.