May 1996 **Vol. 8, No. 2 (G)**

SILENCING THE NET

The Threat to Freedom of Expression On-line

SUMMARY

Governments around the world, claiming they want to protect children, thwart terrorists and silence racists and hate mongers, are rushing to eradicate freedom of expression on the Internet, the international "network of networks," touted as the Information Superhighway. It is particularly crucial now, in the early stages of vast technological change, that governments reaffirm their commitment to respect the rights of citizens to communicate freely. A G7 Ministerial Conference on the Information Society and Development to be held in South Africa from May 13-15, 1996 should be used as a platform to repudiate the international trend toward censorship and to express unequivocal support for free expression guarantees on-line.

Restrictions on Internet access and content are increasing worldwide, under all forms of government. Censorship legislation was recently enacted in the United States, the birthplace of the Bill of Rights as well as of this new communications medium and, for better or worse, a model for other nations' Internet policies. The Clinton administration claims the law will protect minors from "indecent" material and appears unconcerned that it will reduce on-line expression between adults to what may be deemed suitable for a child. Other democratic countries are following suit. The German phone company cut off access to all the sites hosted by an American Internet service provider (ISP) in an effort to bar Germans from gaining access to neo-Nazi propaganda on one of the sites it hosted. The governments of France and Australia have also indicated they may enact legislation to control Internet content.

Authoritarian regimes are attempting to reconcile their eagerness to reap the economic benefits of Internet access with maintaining control over the flow of information inside their borders. Censorship efforts in the U.S. and Germany lend support to those in China, Singapore, and Iran, where censors target not only sexually explicit material and hate speech but also pro-democracy discussions and human rights education.

Proposals to censor the Internet—wherever they originate—violate the free speech guarantees enshrined in democratic constitutions and international law. In the attempt to enforce them, open societies will become increasingly repressive and closed societies will find new opportunity to chill political expression.

Because the Internet knows no national boundaries, on-line censorship laws, in addition to trampling on the free expression rights of a nation's own citizens, threaten to chill expression globally and to impede the development of the Global Information Infrastructure (GII) before it becomes a truly global phenomenon. Democratic countries, including the U.S. and Germany, that are pushing for the development of the GII will lack legitimacy in criticizing efforts by China to eliminate information that "hinders public order" or by Vietnam, where the "the cultural aspect" is cited as a reason to censor connections to pro-democracy discussions abroad.[1]

An issue closely related to censorship is that of access, which is to a large extent determined by the existing telecommunications system. According to a 1995 report by the Panos Institute, a London-based international non-profit organization specializing in development issues,

> Access requires a telephone line. Forty-nine countries have fewer than one telephone per 100 people, 35 of which are in Africa. India, for example, has 8 million telephone lines for 900 million people. At a global level at least 80% of the world's population still lacks the most basic telecommunications.[2]

Opportunities to promote access have never been greater, however. New communications technologies are providing developing countries with an unprecedented means to leapfrog antiquated communication networks.

[1] According to Nghiem Yuan Tinh, deputy director of Vietnam Data Communication Company, "The Internet must be controlled, not only for technical and security reasons but from the cultural aspect." "Plan by Telecom Authority to Exercise Control Over Internet Disturbs Foreign Investors and Agency," *Financial Times* (London), September 19, 1995.

[2] *The Internet and the South: Superhighway or Dirt-Track?* (London: Panos Institute, 1995).

Limits on access are imposed by governments for a variety of reasons, including economic gain and political control. Some governments, including India and Saudi Arabia, have chosen to control the liberalizing effect of the Internet by denying access to entire segments of their populations, either through exorbitant charges or by confining access to select populations, such as universities. Rather than attempting to extend the Internet to a diverse group of citizens, these governments are striving to reap the economic benefits of Internet access without making it available to economically, socially, and politically disadvantaged groups, for whom it has the greatest potential for positive change. In some countries, such as Saudi Arabia, individuals who have Internet connections through foreign-owned corporations are able to elude these restrictions.

Even at this relatively early stage in the Internet's development, a wide range of restrictions on on-line communication have been put in place in at least twenty countries, including the following:

- **China**, which requires users and Internet Service Providers (ISPs) to register with authorities;
- **Vietnam and Saudi Arabia**, which permit only a single, government-controlled gateway for Internet service;
- **United States**, which has enacted new Internet-specific legislation that imposes more restrictive regulations on electronic expression than those currently applied to printed expression;
- **India**, which charges exorbitant rates for international access through the state-owned phone company;
- **Germany,** which has cut off access to particular host computers or Internet sites;
- **Singapore**, which has chosen to regulate the Internet as if it were a broadcast medium, and requires political and religious content providers to register with the state; and
- **New Zealand**, which classifies computer disks as publications and has seized and restricted them accordingly.

Privacy issues are closely related to the regulation of content and access. On-line communications are particularly susceptible to unauthorized scrutiny. Encryption technology is needed to ensure that individuals and groups may communicate without fear of eavesdropping. Lack of information privacy will inhibit on-line speech and unnecessarily limit the diversity of voices on the GII.

The Internet has the potential to be a tremendous force for development—by providing quick and inexpensive information, by encouraging discussion rather than violence, and by empowering citizens, to cite but a few examples. But this potential can be realized only if it becomes a truly global effort. Policy makers must make every effort to ensure that internationally guaranteed rights to free expression are extended to on-line communication and call for the repeal of censorship legislation. Without such commitments, individuals face the danger of seeing their rights eroded by the very technologies they are embracing.

This report recommends principles for international and regional bodies and nations to follow when formulating public policy and laws affecting the Internet, sets forth the international legal principles governing on-line expression, and, finally, examines some of the current attempts around the globe to censor on-line communication.

RECOMMENDATIONS

The meeting of the G7 countries (Britain, Canada, France, Germany, Italy, Japan, and the United States) in South Africa in May 1996 to discuss the development of the GII should be used as one platform to emphasize the importance of freedom of expression.[3] Regional agreements should clearly state that freedom of expression principles

[3] A UNESCO meeting was held in Madrid in March 1996 to discuss copyright protection on the Internet. To our

apply to electronic communication. These agreements should clarify that the Internet differs significantly from broadcast media in areas such as the level of choice and control afforded to the individual user. Because of such distinctions, it is important that the Internet not be subject to the same restrictions as are often imposed on broadcast media.

It is important to promote the universal application of two important free expression principles not yet codified in international law. The first of these is an explicit prohibition against prior censorship, that is, requiring official approval of communication before making it public. Such a practice has been used by repressive governments against the press and could be invoked against electronic communication. The second is an explicit prohibition against restrictions of free expression by indirect methods, such as the abuse of controls over equipment or broadcasting frequencies used in the dissemination of information; or by any other means tending to impede the communication and circulation of ideas and opinions. Controls over newsprint have frequently been used to silence critical publications. Governments are already modernizing their techniques to include modem lines and international Internet connections.

In its February 1995 letter to U.S. Vice President Al Gore on the eve of the G7 Ministerial Conference on the Information Society, Human Rights Watch joined with a number of other organizations in proposing the following principles regarding content, access, and privacy.[4] These principles are even more critical today, and we urge policy makers at the G7 conference in South Africa, and the framers of GII policy within other regional bodies and international organizations, to follow them.

Content Issues

Policy makers should take the initiative to expressly enshrine freedom of expression as a principle in the development of the GII. This should include:

- Prohibiting prior censorship of on-line communication on the GII.
- Demanding that any restrictions of on-line speech content be clearly stated in the law and limited to direct and immediate incitement of acts of violence.
- Requiring that laws restricting the content of on-line speech distinguish between the liability of content providers and the liability of data carriers.
- Insisting that on-line free expression not be restricted by indirect means such as excessively restrictive governmental or private controls over computer hardware or software, telecommunications infrastructure, or other essential components of the GII.
- Calling for the promotion of noncommercial public discourse on the GII.
- Promoting the wide dissemination of diverse ideas and viewpoints from a wide variety of information sources on the GII.
- Ensuring that the GII enable individuals to organize and form on-line associations freely and without interference.

Access Issues

---

knowledge, that conference represented the only U.N.-sponsored effort to address Internet regulation.

[4] The American Library Association, American Civil Liberties Union, Article 19, Center for Democracy and Technology, Electronic Frontiers Foundation, Electronic Privacy Information Center, People for the American Way, Privacy International also signed the letter.

GII policy should emphasize the importance of providing Internet access to everyone, regardless of geographic or other factors. This should encompass:

- Including citizens in the GII development process from countries that are currently unstable economically, have insufficient infrastructure, or lack sophisticated technology.
- Providing nondiscriminatory access to on-line technology.
- Guaranteeing a full range of viewpoints, by providing access to a diversity of information providers, including noncommercial educational, artistic, and other public interest service providers.
- Providing two-way communication and enabling individuals to publish their own information and ideas.
- Protecting diversity of access by establishing technical standards that can be applied easily in a variety of systems.
- Prohibiting discrimination on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Privacy Issues

Delegates to the G7 meeting and other meetings concerning policy on the GII should guarantee respect for the privacy of communication on the Internet by:

- Ensuring that personal information generated on the GII for one purpose is not used for an unrelated purpose or disclosed without the person's informed consent.
- Enabling individuals to review personal information on the GII and to correct inaccurate information.
- Providing privacy measures for information regarding on-line business transactions as well as content.
- Allowing users of the GII to encrypt their communications and information without restriction.

The above recommendations are also pertinent to individual governments in shaping their own policies with respect to on-line communication. In addition, the following recommendations apply to domestic Internet policies:

- To ensure that domestic Internet services are designed to ensure universal access, governments should provide full disclosure of information infrastructure development plans and encourage democratic participation in all aspects of the development process. They should also advocate widespread use of the GII and strive to provide adequate training. In addition, governments should urge citizens to take an active role in public affairs by providing access to government information.
- In order to guarantee the privacy of on-line communication, governments should put in place enforceable legal protections against unauthorized scrutiny and use by private or public entities of personal information on the GII. They should also oppose controls on the export and import of communications technologies, including encryption. In addition, governments should conduct investigations on the GII pursuant only to lawful authority and subject to judicial review.

BACKGROUND

The Internet began in the 1960s as a way of linking a U.S. Defense Department network and other communications networks. Over time, many other networks and users from around the world have connected themselves to the Internet. The U.S. still dominates the Internet in terms of users and content, but Canada, Europe, Australia, and New Zealand are also on-line in large numbers. Internet usage in much of Asia is increasing rapidly as well. The number of Internet users is believed to range between twenty and thirty million. More than 160 countries are reported to have links to the Internet, over one hundred nations with full access and the rest through e-mail.[5]

The Internet is composed of a number of different ways of organizing, transmitting and accessing data. Because of this multiplicity of systems, it is unlike any other single medium. Rather, it incorporates characteristics of several other media and communications systems, including print, broadcast, and postal systems. Electronic mail (e-mail) allows for one-to-one or one-to-many communication. Gopher sites provide text-only information arranged according to menus. The World Wide Web allows for the display of many types of information, including text, images, sound and video, as well as interactive communication.

A recognition by world leaders of the need to formulate policy for this powerful new medium prompted members of the G7 to hold a "Ministerial Conference on the Information Society" in Brussels in February 1995. At that conference, a number of principles were agreed to, including encouraging competition and private investment, defining an adaptable regulatory framework, providing open access to networks, ensuring universal access, and promoting equality of opportunity and diversity of content. Although freedom of expression was not highlighted in specific terms, to the disappointment of Human Rights Watch and other groups that had urged such an emphasis, it is implied in the final goal—promoting diversity of content—which can be achieved only by encouraging free expression for people all over the world.[6] In his keynote address to the conference, Vice President Gore, an active proponent of the GII, stated, "[Global communication] is about protecting and enlarging freedom of expression for all our citizens and giving individual citizens the power to create the information they need and want from the abundant flow of data they encounter moment to moment."

[5] Johanna Son, "Asia-Communication: Bumps Lie Ahead in Information Superhighway," Inter Press Service, December 14, 1995.

[6] Letter to Vice President Gore from Human Rights Watch, Electronic Privacy Information Center, ACLU, American Library Association, Article 19, Center for Democracy and Technology, Electronic Frontiers Foundation, People for the American Way, and Privacy International, February 16, 1995.

One of the main targets of the censors is Usenet, a system separate from the Internet but accessible from it, that "pump[s] upwards of 100 million characters a day into the system--nearly an encyclopedia's worth of writing."[7] Usenet comprises more than 9,000 "newsgroups" ─discussions or picture databases─on various topics, including the political and the sexually explicit. The groups are arranged under headings such as biz (business), comp (computers and related subjects), rec (hobbies, games and recreation), sci (science), soc ("social" groups, often ethnically related), talk (politics and related topics), and alt (for alternative, often controversial). Not all the newsgroups are available on all Internet host computers. Usenet came to prominent international attention most recently in late December 1995, when CompuServe, an on-line service of H&R Block, based in Columbus, Ohio, removed from all of its computers more than 200 Usenet computer discussion groups and picture databases that had provoked criticism by a federal prosecutor in Munich.[8] Three days later, the Chinese government echoed the Germans' actions by calling for a crackdown on the Internet to rid the country of pornography and "detrimental information."[9]

It should not be surprising that governments around the globe are anxious to control this new medium. Every communications advance in history has been seen by self-appointed moral guardians as something to be controlled and regulated. By 1558, a century after the invention of the printing press, a Papal index barred the works of more than 500 authors. In 1915, the same year that the D. W. Griffith film "Birth of a Nation" changed the U.S. cultural landscape, the U.S. Supreme Court upheld the constitutionality of an Ohio state censorship board created two years earlier, thus exempting motion pictures from free speech protection on the grounds that their exhibition "is a business, pure and simple, originated and conducted for profit...." The same view was applied in the early days of radio─entertainment programs were thought to be exempt from freedom of speech guarantees.

The Internet, as the first truly "mass" medium, is even more threatening than these earlier media. While few individuals and groups can publish books or newspapers, make a film, or produce a radio or television program, any person with a personal computer and a modem can communicate with a huge international audience. The implications of a real GII for the advancement of human rights and democracy are vast. When traditional means of communication broke down and the war in Sarajevo made it impossible for civilians to leave their homes without risking their lives, many citizens used on-line technology to communicate with family members, the international press, and humanitarian relief agencies. Human rights groups, political organizations, and builders of burgeoning democracies are using the Internet to communicate, educate, and organize. During the United Nations Fourth World Conference on Women, held in Beijing in 1995, women all over the world were able to feel a sense of participation because of regular postings on the proceedings. It is precisely because of the Internet's potential for increasing the political participation of the disenfranchised that governments are seeking to control it.

These initial achievements could easily disappear if the censors are allowed to have their way. Governments and other institutions that support freedom of expression must ensure that the Internet is granted the same guarantees that are given to other forms of individual expression. International law is clear on what electronic rights of expression must entail. Although international law does not address such communication specifically, the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights enshrine rights to freedom of expression, access, and privacy, which are relevant to the new medium. Article 19 of the Universal Declaration of Human Rights proclaims:

[7] Adam Gaffin, *EFF Guide to the Internet* (San Francisco: Electronic Frontiers Foundation, Revised December 4, 1995).

[8] The "banned" newsgroups were still available to CompuServe users who used the service to connect to computers that carried the newsgroups. Information on how to do this circulated quickly through the CompuServe system.

[9] "China Cracks Down on Internet," Deutche Presse Agentur, January 1, 1996.

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[10]

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) guarantees this right as well, and notes that restrictions on this right "shall only be such as are provided by law and are necessary:

> "(a) For respect of the rights or reputations of others;

[10] Other relevant articles from the Universal Declaration of Human Rights include the following: "

> Article 7: All are equal before the law and are entitled without any discrimination to equal protection of the law.
>
> Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.
>
> Article 27: Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.

"(b) For the protection of national security or of public order (*ordre public*), or of public health or morals."[11]

The recently adopted Johannesburg Principles on National Security, Freedom of Expression and Access to Information[12] state that restrictions on freedom of expression are permitted only when "the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest."[13] According to the Principles, the burden of demonstrating the validity of the restriction rests with the government.[14] Criticism of the government or its leaders is protected.[15] In addition, a government must demonstrate that "the restriction imposed is the least restrictive means possible for protecting that interest."[16]

NORTH AMERICA

United States

[11] Other relevant articles from the ICCPR include the following:

Article 25 guarantees the right "to take part in the conduct of public affairs."

Article 26 states:

> All persons are equal before the law and are entitled without any discrimination to equal protection of the law....[T]he law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

[12] These Principles were adopted on October 1, 1995 by a group of experts in international law, national security, and human rights.

[13] For the purposes of the Principles, "a democratic society is one which has a government that is genuinely accountable to an entity or organ distinct from itself; there must be genuine, periodic elections by universal and equal suffrage held by secret ballot that guarantee the free expression of the will of the electors; political groups must be free to organize in opposition to the government in office; and there must be effective legal guarantees of fundamental rights enforced by an independent judiciary."

[14] Principle 1(c).

[15] Principle 7.

[16] Principle 1.3(b).

Hysteria about "cyberporn" was ignited in the U.S. after *Time* magazine published a cover story, complete with lurid photographs, asserting the wide availability of sexually explicit material on the Internet.[17] The article was based on the research findings (later acknowledged by *Time* to have been seriously flawed) of a student at Carnegie Mellon University. Nevertheless, this concern recently culminated in the enactment of the Communications Decency Act (CDA), an amendment to a sweeping telecommunications reform bill signed in February 1996.

The CDA criminalizes on-line communication that is "obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass an other person" or "obscene or indecent" if the recipient of the communication is under eighteen years of age "regardless of whether the maker of such communication placed the call or initiated the communication." Also prohibited is on-line communication to minors that "depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication."[18] The CDA would permit the U.S., for example, to seek the arrest of a European content provider whose sexually explicit material was seen as "indecent" or "patently offensive."

In letters to members of Congress and President Clinton, Human Rights Watch opposed the CDA, taking the position that "indecent" speech is protected by both the U.S. Constitution and international law. Human Rights Watch is also concerned that the effort to censor "indecent" communication could impede the work of our own and similar organizations which transmit graphic accounts of human rights abuses. Because of these concerns, in February, Human Rights Watch became a plaintiff in a lawsuit brought by the American Civil Liberties Union challenging the CDA on constitutional grounds. The suit is currently before a panel of judges. According to our affidavit,

> Some of the accounts [of abuses in Human Rights Watch reports] are necessarily graphic and explicit: torture, rape, mutilation, execution, mass murder are brutalities that must be discussed in detail if people are to understand the widespread human rights abuses occurring worldwide. Likewise, to address human rights abuses without discussing the violence of acts such as rape, torture, and bodily mutilation would be impossible. Human Rights Watch exposes the abuse in order to educate the public about the scope of current abuse and to prevent future atrocities.
>
> [T]he graphic nature of some of the eyewitness accounts, especially those dealing with sexual assault, may be considered "indecent" or "patently offensive" under this statute. For example, our July 1995 press release on slavery in Pakistan, posted at our gopher site [on the Internet], provides graphic and factual details on the ways in which bonded laborers have been tortured. The text relates that they have been "beaten with sticks, stripped naked, hung upside down, burned with cigarettes, beaten on the genitals and have had their legs pulled apart. Women prisoners are often held in custody indefinitely and suffer a consistent pattern of sexual assault, including rape." A March 1995 press release on abuses by Nigerian security forces in Ogoniland, posted at our gopher site, quotes the testimony of one woman, as follows: "K, a woman in her late thirties from the village of Bera, told Human Rights Watch that she had been raped by five soldiers in rapid succession on the morning of May 28, 1994. After locking K's 10-year-old son in a room, K recalled,
> the soldiers beat me with the butts of their guns, pushed me onto the ground, and kicked me. They tore off my wrapper, then my underwear. Two of them raped me through my anus, three the usual way. While one soldier raped me, another would beat me. I tried to scream, but they held my mouth. They said if I made too much noise they would kill me.

[17] Philip Elmer-Dewitt, "On a Screen Near You: It's Popular, Pervasive and Surprisingly Perverse, According to the First Survey of On-line Erotica. And There's No Easy Way To Stamp It Out," *Time*, July 3, 1995.

[18] U.S. Code, Title V, Subsection A, Section 502 "Obscene or Harassing Use of Telecommunications Facilities Under the Communications Act of 1934."

Our October 1993 report on the abuse of Burmese refugees from Arakan, posted on the newsgroup reg.seasia, relates abuses against women in language such as, "then the official grabbed her breast" (p. 12); "the CIC and the other official put their hands inside S.K.'s clothing and touched her all over her body, including her vagina" (p. 13); "...one policeman fondled S.K.'s breasts and struck S.K. on the back of then neck with a stick" (p. 13).

Clearly, obstacles to Human Rights Watch in reporting these atrocities in the United States are likely to be magnified for groups operating in more repressive states and attempting to post similar findings on the Internet.

Canada

In response to the debate about cyberspace, the Canadian government formed the Information Highway Advisory Council (IHAC) in 1994 to study and prepare an official statement on what directions the Internet should take in Canada. In September 1995, the council released its first report, which contained only vague recommendations. On the issue of content, it concluded that there should be controls on two primary targets: obscenity and racist/hate material.[19] It is illegal to spread "hate propaganda" and "obscenity" in Canada. Sexually explicit material is legal as long as it is not deemed obscene, that is, characterized by "undue exploitation of sex," meaning sex plus violence or degrading sex. Under a new law on child pornography that has not been tested by the Supreme Court, mere possession is illegal. According to David Jones, president of Electronic Frontiers Canada, "There are no new laws being proposed that apply *specifically* to the Internet."[20] That could change, however. On April 2, 1996, Justice Minister Allan Rock released a discussion paper inviting Canadians to present their views on regulating excessive violence in the media, including the Internet.[21]

ASIA

Asia now has over 1.5 million users, two-thirds of them in Japan.[22] Among the region's authoritarian nations, only North Korea and Myanmar are without any Internet connection.[23] Currently, most countries in Asia are connected directly to the U.S., rather than to each other, but new initiatives have proposed establishing an intra-Asia connection.

[19] Alana Kainz, "Information Highway: Advisory report leaves uncharted roads," *Ottawa Citizen*, September 28, 1995.

[20] E-mail correspondence from Dr. David Jones to Human Rights Watch, February 15, 1996.

[21] David Vienneau, "Rock seeks views on violence," *Toronto Star*, April 3, 1996.

[22] Johanna Son, "Asia-Communication: Bumps Lie Ahead in Information Superhighway," Inter Press Service, December 14, 1995.

[23] Philip Shenon, "Why Nations Fear the Net," *New York Times*, June 11, 1995.

Some Asian governments, including Pakistan, are choosing to control the Internet's effects mainly by limiting its availability. A senior scientist at Pakistan's state-owned National Institute of Electronics has noted that Internet access would be limited by the small number of nodes and hosts available to users and by the intervention of service providers who could stop undesirable discussion groups and electronic messages.[24] In India, where commercial Internet access was launched in mid-1995, only the state-owned phone company, VSNL, has been allowed to provide international Internet services, in order to maintain the government's monopoly on long-distance phone services.[25] According to guidelines issued by the Department of Telecommunications (DoT) based on the antiquated Indian Telegraph Act of 1885, an ISP must ensure that nothing objectionable or obscene is carried on the network, but it is not clear that these have been enforced. In late January 1996, the DoT decided to allow commercial access, but all companies will have to route their services through VSNL.[26]

Thailand's National Electronics and Computer Technology Center (Nectec), an official agency responsible for information technology policy, recently called upon local ISPs to police their own sites for sexually explicit material. It also said that subscribers and operators are required to agree not to show anything considered indecent or they will face criminal prosecution.[27] In the Philippines, Internet censorship measures have been introduced in the legislature.[28]

In early March 1996, member nations of the Association of Southeast Asian Nations (ASEAN) said they planned to set up a regulatory body to deal with the flood of information technology; they also voiced concern about pornography and disinformation.[29]

China

Commercial Internet accounts became available in China in mid-1995, but at prices far beyond the means of all but the wealthiest. In June 1995, China's telecommunications minister stated that "as a sovereign state, China will exercise control on the information" entering China from the Internet. "By linking with the Internet, we do not mean the absolute freedom of information."[30] Many Usenet newsgroups, including those classified as alt, rec and soc, were reportedly not allowed on Chinese Internet host computers, but the comp and sci hierarchies were apparently provided.[31]

The Hong Kong-based China Internet Corporation (CIC), principally owned by China's state-run Xinhua News Agency, offers Chinese business subscribers only limited access to business-related information. Users have access to information generated outside China, but only after it has been screened in Hong Kong. According to James Chu, CEO of CIC, customers can be assured their e-mail will not be screened or bugged by mainland "unless you have broken the law."[32]

---

[24] Ajoy Sen, "Some Asian Nations Give Internet Mixed Reception," Reuters, June 13, 1995.

[25] Spaeth, Anthony, "'National Security,' the Vietnamese Government Wants to Control Internet Access," *Time*, October 16, 1995.

[26] C. T. Mahabharat, "VSNL Monopoly on Internet Access to End," Newsbytes News Network (Stillwater, Minnesota), March 1, 1996.

[27] Nigel Armstrong and I.T. Daily, "Thai Group on Porn Trail," Newsbytes News Network, February 26, 1996.

[28] Ninez Cacho-Olivares, "My Cup of Tea—Pornography on the Net," *Business World* (Manilla), March 18, 1996.

[29] Ramthan Hussein, "Singapore Deputy Premier Defends Curbs on Internet," Reuters, March 9, 1996.

[30] Teresa Poole, "China seeks to make the Internet toe party line," *The Independent* (London), January 5, 1996.

[31] E-mail from Peng Hwa Ang, Singapore, to Human Rights Watch, November 1995.

[32] Rhonda Lam Wan, "Xinhua Affiliate to Offer E-mail," *South China Morning Post* (Hong Kong), October 6, 1995.

ChinaNet, based in Beijing and Shanghai, which became available in May 1995, provided commercial Internet access. Control of Internet access accounts was extremely tight, and people wishing to open them were required to register at the Postal Ministry. Fairly quickly, black market permits became available.[33]

On January 1, 1996, several days after CompuServe cut off access to 200 Usenet newsgroups, Xinhua News Agency, China's official medium, reported that the government had called for a crackdown on the Internet to rid the country of unwanted pornography and "detrimental information."[34] A joint statement issued by the State Council and the Communist Party Central Committee said effective measures had to be adopted to solve the problem of uncontrolled information. The leadership also reportedly summoned the Chinese suppliers of Internet connections, and on January 15, the biggest supplier announced a "moratorium" on new subscribers.[35] According to press reports, officials said that as many as 70,000 people were using the Internet through 7,000 accounts, and that the high volume was more than the current system could handle.[36]

On January 23, a cabinet session chaired by Premier Li Peng adopted draft rules governing links to the Internet. The cabinet reiterated its provisional approval for global computer links but declared it "imperative" to formulate rules to govern China's use of the new technology.[37] On February 4, Xinhua announced that the new Internet regulations required existing computer networks to "liquidate" and "re-register," and to use only international channels provided by the Ministry of Posts and Telecommunications, the Ministry of Electronics Industry, the State Education Commission and the Chinese Academy of Sciences.[38]

As the *New York Times* reported:

> Neither organizations nor individuals are allowed to engage in activities at the expense of state security and secrets," [Xinhua] said. "They are also forbidden to produce, retrieve, duplicate or spread information that may hinder public order. The transmission of pornographic or obscene material was also expressly banned.[39]

In mid-February, the Ministry of Public Security ordered all those who use the Internet and other international computer networks to register with the police within thirty days.

Hong Kong

[33] "Net Spreads a Web of Uncertainty," *South China Morning Post*, December 14, 1995.

[34] "China cracks down on Internet" Deutsche Presse-Agentur, January 1, 1996.

[35] "Economic News—A Blackout," *The Economist* (London), January 20, 1996.

[36] "Jammed Capacity Halts Sale of Internet Accounts," Economist Intelligence Unit (London), February 8, 1996.

[37] Paul Eckert, "Britain Raises Concerns About China Media Measures," Reuters, January 24, 1996.

[38] Martyn Williams, "China Issues Regulations to Control Internet, Newsbytes News Network, February 6, 1996.

[39] Seth Faison, "Chinese Tiptoe into Internet, Wary of Watchdogs," *New York Times*, February 5, 1996.

Hong Kong has not drafted any policy or released any official statements regarding Internet censorship. The 1987 Obscene and Indecent Articles Ordinance does not specifically discuss on-line communication, but the ordinance reportedly applies to communication on the Internet.[40] The Hong Kong government's Recreation and Culture Branch, which oversees on-line media, recently commissioned a study of on-line communication. Its secretary said that developments in other countries, including the United States, would be taken into account.[41]

There are currently more than fifty Hong Kong ISPs, and some censor content, including Hong Kong SuperNet, one of the largest Hong Kong ISPs, which voluntarily ended access to sexually explicit material on Usenet in March 1995.[42] Star Internet followed suit in November, by blocking about twenty newsgroups with erotic text and pictures.[43]

In March 1996, Commissioner of the Television and Entertainment Licensing Authority Peter Cheung Po-tak said that controls on the Internet should ensure a "minimum degree of decency" to protect children and said the best solution would be for ISPs to regulate themselves.[44]

Singapore

In Singapore the Internet is treated as a broadcast medium, regulated under the Singapore Broadcasting Authority Act of 1995, which established the Singapore Broadcasting Authority (SBA). Singapore allows three service providers: Singnet, which is part of Singapore Telecom, Pacific Internet and Cyberway. The government claims that it does not currently censor e-mail, but in 1994 it disclosed that it had searched individual accounts to try to identify those who had downloaded sexually explicit material. After businesses expressed alarmed about the security of their information, authorities said they would refrain from conducting such searches in the future.

The main means of censorship up to now has been to control access. In addition, sexually explicit material and news have been censored by the Ministry of Information and the Arts, the government body in charge of media censorship. Fewer than half of Usenet newsgroups are available through Singnet. Currently there are no widespread uniform guidelines or procedures for restricting use of any Internet services, and local administrators have to make arbitrary decision on access.

[40] Nigel Armstrong and IT Daily, "First Hong Kong Porn Charge Could Take "Weeks," Newsbytes News Network, August 3, 1995.

[41] Eric Lai, "Cyberporn a threat to freedom of expression," *South China Morning Post*, January 23, 1996.

[42] Maggie Farley, "Hong Kong's Remedy for Subversive Use of Cyberspace—Pull the Plug," *Los Angeles Times*, April 25, 1995.

[43] Lai See, "No Cyber-Sex Please, as Squeaky-Clean Star Internet Takes Axe to Animal Acts," *South China Morning Post*, November 24, 1995.

[44] Glenn Schloss, "Hint on Internet Porn Laws," *South China Morning Post*, March 29, 1996.

The minister of information and the arts told Parliament that "Censorship can no longer be 100 percent effective, but even if it is only 20 percent effective, we should still not stop censoring....We cannot screen every bit of information that comes down the information highway, but we can make it illegal and costly for mass distributors of objectionable material to operate in Singapore."[45] Colonel Ho Meng Kit, the CEO of the SBA, the committee that oversees content on the Internet, said objectionable material could be censored through three main channels: technology, legislation, and licensing. He stated that only ISPs would be targeted and noted, "[Censorship] may not always be effective but it makes a statement about the nature of Singapore society and the values it wants to uphold."[46]

Although authorities initially stated that they would not heavily censor political criticism, they have reportedly shifted from watching for sex-related material to watching for "misinformation." Some topics recently discussed on the newsgroup soc.culture.singapore ranging from Michael Fay's caning to the case of a Filipino maid convicted of double murder sparked the formation of a government administrative committee, which has started Singapore Infomap, a Web site, to provide "correct" information and rebut "inaccurate" information.

In early March, the government announced more severe censorship measures, including the licensing of all ISPs and a requirement to use filtering software. The measures are meant to prevent Singaporeans from accessing sexually explicit material and hate literature, and will also cover politics and religion. The government also announced that World Wide Web content providers would have to register with the SBA, and that three categories of Web pages would be scrutinized: those operated by political parties, electronic newspapers targeting Singapore, and pages concerned with politics or religion.[47] In April, the regulations tightened further. The SBA announced that it was setting guidelines, to become effective in June 1996, for Internet content providers. According to the preliminary guidelines, those with Web sites must ensure they do not encourage abuse or distribute objectionable information, such as sexually explicit material. Sponsors of discussion groups may have to register with the SBA. Internet content providers and ISPs will be responsible for what is transmitted. The rules also require Internet service providers to institute an acceptable use policy.[48]

Indonesia

Indonesia's first commercial provider, Indonet, began operation in late 1994. A number of others soon followed, and the country now has numerous ISPs. The more established electronic bulletin board networks also draw extensively from the Internet. The Internet is more free than any other mass medium in Indonesia, and there are no laws, regulations or ministerial decrees concerning its use. *Tempo*, a news weekly that was closed by the government two years ago, recently established a site on the Web, with the blessing of the minister of information who agreed "there are no regulations against it," but warned that "maybe the House [of Representatives] will want to discuss legislating the Internet."[49] At this stage, however, the government has chosen to compete with opposing views by establishing its own Web sites.

Armed Forces spokesman Brig.-Gen. Surwarno Adiwijoyo told Reuters news agency that the military had suggested to the Communications Ministry the need for some sort of "toll gate" to "black out" news that could damage

[45] "Singapore defends censorship in Internet age," Reuters, July 7, 1995.

[46] Jimmy Yap, "Singapore Takes Aim at Cybersmut," *Straits Times* (Singapore), July 30, 1995.

[47] "Singapore—Government Clamps Down on Internet and Supports Its Future," Telenews Asia (Rozelle, Australia), March 21, 1996.

[48] "Singapore Sets Rules for Internet Providers, TV Singapore," Reuters, April 14, 1996.

[49] "*Tempo* on Internet is okay: Harmoko," *Jakarta Post*, March 13, 1996, as reported on the Indonesia-L mailing list, March 13, 1996.

culture or affect security.[50] It has also suggested registering uses and users, he said. At present, private ISPs do not carry all Usenet groups, but this is reportedly done in the interests of conserving disk space and because of the language barrier.[51]

Malaysia

The Malaysian Institute of Microelectronic Systems (Mimos), the nation's sole Internet provider, has experienced a huge demand, with an average monthly increase of 22 percent since it began service in late 1994. As of October 1995, there were some 30,000 users. In April 1996, Mimos announced that it would appoint eight new ISPs to help ease congestion.

[50] Jim Della-Giacoma, "Politics, Not Sex, Indonesian Internet Concern," Reuters, November 16, 1995

[51] E-mail from John MacDougall, April 9, 1996.

Usenet newsgroups are heavily censored. The "acceptable use" policy at Jaring, the main Malaysian Internet line, states that "members shall not use Jaring network for any activities not allowed under any Law of Malaysia."[52] The government reportedly realizes that on-line censorship may not be effective. Prime Minister Datuk Seri Dr. Mahathir Mohamad has warned Malaysians that "It depends on the culture. If the culture is weak, we will be the victims. But if we use it in a way that can increase our knowledge, we will get many benefits from the Internet."[53] However, in March 1996, Information Minister Datuk Mohamed Rahmat announced that a new regulatory body would be set up to monitor the Internet and that those criticizing the government "will face the music."[54]

In reaction to Malaysian students abroad criticizing Malaysia on the Internet, the government has considered various ways to curb such dissent, according to the information and education ministers, and the education minister proposed cutting scholarships of offending students.

South Korea

In South Korea, about half of all Internet users are affiliated with universities or the government. The nationally run telephone corporation, Korea Telecom, started service in June 1994, and there are a number of other commercial providers.

The government has decided to censor computer networks, according to statements by communications officials in October 1995. The decision was reportedly made out of growing concern regarding children's access to sexually explicit and other undesirable material. Local computer networks will be asked to prohibit access by local subscribers to banned sites, according to the Information and Communications Ethics Committee of the Data and Communications Ministry. Sexually explicit material will be banned, along with information deemed "subversive," such as instructions on making bombs and drugs. Computer games and other software are already censored. Details, such as punishments, have reportedly yet to be worked out.[55]

Vietnam

[52] Charles A. Gimon, "Internet Censorship Around the World," *Info Nation* (Minneapolis, MN), July 1995.

[53] Lokman Mansor, "Dr. M, Ramos Have a Chat Via the Internet," *Business Times* (Kuala Lumpur), January 18, 1996.

[54] Ian Stewart, "Internet Curbs in the Pipelines," *South China Morning Post*, March 13, 1996.

[55] "South Korea to Censor Computer Communications Networks," AP Worldstream, October 20, 1995.

The state-owned telecommunications company Vietnam Datacommunications Company (VDC) had planned to launch Internet service earlier this year, but it reportedly put off the opening day because officials decided to first draft regulations on allowable Internet links and users. Internet regulations will reportedly comply with the government's existing censorship regulations. Pham Dao, director of VDC, said that an Internet firewall would be installed to screen out transmissions from specified senders or news resources—cutting out much of the anti-government commentary carried by dissident groups, including support for jailed Buddhists and dissidents.[56] It appears likely that the Ministry of Culture and Information will monitor on-line content and that Interior Ministry will be in charge of monitoring Internet national security issues.[57] Nguyen Ngoc Canh of the General Directorate of Posts and Telecommunications, which sets communication policy, said competing domestic services likely will be allowed as long as Vietnam Datacommunications Company monitors a single outside link.[58]

Until recently, Vietnam's Internet service was made available through the Institute of Information Technology, which exists mostly for the benefit of academics and nongovernmental organizations. A VDC official told the press that the organization's effort to control the Internet "is the requirement from our leaders, our government. The Internet must be controlled, not only for technical and security reasons but from the cultural aspect."[59] The government is reportedly worried about sexually explicit material from foreign countries and about "foreign organizations" transmitting information. Some overseas Vietnamese groups have distributed anti-government tracts in Hanoi. Prime Minister Vo Van Kiet was recently the victim of "spamming" (an e-mail barrage) by anti-communist dissidents in the U.S.[60]

AUSTRALIA AND NEW ZEALAND

Australia has been considering regulating the Internet since 1993. In August 1994, the Department of Communications and the Arts released a report, "Regulation of Computer Bulletin Board Systems," which called for regulations. A year later, the recommendations in that report were updated and released in the "Consultation Paper on the Regulation of On-line Information Services." One of the goals elucidated in the consultation paper was "to protect freedom of expression, especially with regard to private communication between adults, while at the same time limiting children's exposure to harmful or unsuitable material." It proposed a system of self-regulation reinforced by legislative sanctions. Objectionable material was defined in the consultation paper as material that "depicts, expresses, or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that it offends against the standards of morality, decency and proprietary generally accepted by reasonable adults to the extent that the material should be refused classification." Restricted material was defined as "material that [is] unsuitable for seeing, reading or playing by persons under 15."[61]

---

[56] "Vietnamese Net Provider to Censor Inbound Transmissions," Telecomworldwire, January 11, 1996, and Jon Auerbach, "Fences in cyberspace; Governments move to limit free flow of the Internet, *The Boston Globe*, February 1, 1996.

[57] Peter Mears, Radio Australia, March 24, 1996, as reported in "Help Sought from Singapore in Policing the Internet," BBC, March 26, 1996, and "Government to use foreign software to police Internet users," Agence France Presse, March 24, 1996.

[58] Kathy Wilhelm,"Vietnam—Net or Not," AP, January 4, 1996.

[59] "Vietnam: Plan by Telecom Authority to Exercise Control Over Internet Disturbs Foreign Investors and Agencies," *Financial Times* (London), September 19, 1995.

[60] Larry Lange, Developing Nations and the Internet, *Informationweek* (Manhasset, New York), October 2, 1995.

[61] "Consultation Paper on the Regulation of On-line Information Services," Australian Department of Communications and the Arts, July 7, 1996 (URL: http://www.dca.gov.au/paper_2.html)

In August 1995, the minister for communications and the arts directed the Australian Broadcasting Authority (ABA), an independent federal authority responsible for the regulation of the broadcasting industry, to investigate the content of on-line information and entertainment services and report to him by June 30, 1996. The resulting ABA "issues paper" became available in December 1995, with an invitation for comments to be submitted by the public until mid-February. The paper discusses various issues involved in the development of a code of practice, the adoption of a classification scheme, enforcement of a code, and blocking offensive sites.

Electronic Frontiers Australia, a nongovernmental organization working for rights of Internet users in Australia, submitted a response to the issues paper, arguing a number of points, including that the Internet, because of its interactivity, significantly differs from broadcast media. "[C]lassification of content is unnecessary and in most instances impossible to police," it pointed out. The EFA also urged the government to consult with the industry and "develop a grasp of the realities of the on-line service industry."[62]

Some state governments, including those of New South Wales, Queensland, Victoria, Western Australia, Northern Territory, and Tasmania, have already passed or are planning to introduce on-line censorship legislation.[63] In early October 1995, eighteen people were being questioned and fifteen computers seized across the state of Queensland for alleged involvement with child pornography, based on the state's Classification of Computer Games and Images Act (1995). In Victoria state, the Classification (Publications, Films & Computer Games Enforcement) Bill, which has passed two houses of Parliament and awaits enactment, makes it an offense to use an on-line network to transmit "objectionable" material to minors.[64] Victoria's bill has passed two houses of Parliament. A similar law in Western Australia went into effect on January 1, 1996. Both leave primary censorship in the hands of service providers, and seek to punish senders of information deemed "objectionable"—and senders of information classified as "restricted" to minors—according to broad definitions contained in the legislation.[65] ISPs are liable only if they knowingly permit objectionable material to be transmitted on their network. An even more extreme bill now before the parliament in New South Wales will hold individuals and ISPs responsible for objectionable material, which includes not only sexually explicit information but also drug- and crime-related material. All state laws are subject to change when new federal laws are adopted.

New Zealand

Restrictive Internet legislation was proposed in Parliament in 1994, but, according to Stephen Bell, an Internet activist in New Zealand, it "is widely perceived as more or less dead" at present because of unrelated political developments.[66] Under the legislation, the New Zealand Technology and Crimes Reform Bill, all users would be cut off from any site that transmitted a single piece of objectionable material to a single user. Those found in violation of the law could be fined thousands and lose the use of a telephone for up to five years.

---

[62] Kimberly Heitman, "ABA Inquiry Submission," Electronic Frontiers Australia, February 16, 1996.

[63] Michael Sharp, "Internet Porn Pedlars Face Jail," *Sydney Morning Herald*, April 3, 1996, and John Davidson, "New Moves on Internet Porn Laws," *Australian Financial Review* (Sydney), April 3, 1996.

[64] Mike van Niekerk, "Censor Moves to Shackle Net," *The Age* (Melbourne), February 13, 1996.

[65] For example, the Western Australia bill defines "restricted material" to be that which a reasonable adult, by reason of the nature of the article, or the nature or extent of references in the article, to matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena, would regard as unsuitable for a minor to see, read or hear."

[66] E-mail from Stephen Bell to Human Rights Watch, February 1996.

Under current law, computer disks are treated as "publications," and may be censored as such under the Films, Videos and Publications Classification Act of 1993. If authorities find one example of the more serious grade of "objectionable" material, as defined by the Act,[67] they may arrest and shut down an ISP.[68]

[67] "Objectionable" is defined to include that which "describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good."

[68] E-mail to Human Rights Watch from Stephen Bell of New Zealand, February 7, 1996.

Apparently fearing possible liability, several universities and Internet providers have been blocking access to newsgroups dealing with erotica.[69]

MIDDLE EAST

The Middle East is coming on-line in increasing numbers, but many governments are hoping to control access to sensitive political and religious discussion as well as sex-related material. Bahrain went on-line in December 1995 through Batelco, the government-run phone company, after installing an expensive system to block access to certain Internet-related sites[70] GlobeNet, a U.S. firm, won a contract to provide Internet service in Jordan in 1995 and was asked by authorities to install a special screening facility to control sexually explicit material.[71] Kuwait is planning to launch a new Internet service soon, but a Communications Ministry official told the press that the new ISP "must ensure that no pornography or 'politically subversive' commentary is available in Kuwait." There is no new content-related legislation planned at present.[72] In Abu Dhabi, an Internet club "ha[s] agreed to ban sex, religion and politics on the Internet to respect the local laws."[73] Police in the United Arab Emirates recently held a seminar on combating political dissent and sexually explicit material.[74]

In Morocco, the state Office National des Postes et Telecommunications (ONPT) brought the Internet to the nation on November 16, 1995. ONPT has secured an agreement with the commercial companies that will provide the service. Charges will be fixed, and a convention has been signed to govern all aspects of the Internet's operation. The service has been targeted at the banking and insurance sectors, universities, and multinational corporations.[75]

Iran

The first Iranian Internet line was opened in 1992 by the Institute for Studies in Theoretical Physics and Mathematics through a link to Vienna.[76] The government helped with funds. Internet users, still mostly at universities, now number around 30,000.[77]

[69] Internet Australasia, August 1995 (URL: http://www.interaus.net).

[70] Richard Moore, "Huge Demand for Internet Link," *Egyptian Gazette* (Cairo), January 11, 1996.

[71] London Observer Service, "Many Arab nations seek Internet curbs," *Milwaukee Journal Sentinel*, January 8, 1995.

[72] "Kuwait to boost Internet service but plans censorship," Agence France Presse, April 11, 1996.

[73] Michael Georgy, "Internet Fever Sweeps Gulf," Reuters, April 4, 1996.

[74] Ibid.

[75] John Cooper, "The Middle East Gets Caught in the Internet," *Middle East Economic Digest* (London), December 4, 1995.

[76] Stuart Wavell, "Closed Societies Opened by Internet Genie," *Sunday Times* (London), September 3, 1995.

[77] Ibid.

The government also sponsors a network whose chat rooms allow on-line dialogue between only two subscribers at a time, and private ISPs also exist. Access to the Internet is relatively unregulated, but its increasing popularity will likely result in greater government control. One private network had its lines cut by the Telecommunications Company (TCI) of Iran in August 1995. TCI may have been reacting to reports that the network was being used by young people for sex chats, or it may have been trying to reduce competition to its own network service.[78]

Saudi Arabia

In Saudi Arabia, Internet access has been confined to universities and hospitals. All local accounts, which automatically note the material accessed, are open to inspection by the Ministry of the Interior. Government officials have justified their reluctance to permit large-scale access on the grounds that there is a need to protect people from pornographic and other harmful effects. Existing pornography laws apply to the Internet, but loopholes are available: large foreign companies are increasingly offering their unmonitored Internet access to Saudi business acquaintances, and commercial members of the GulfNet are also free from scrutiny.

Internet access will reportedly be made available to businesses in 1996, but reportedly with strict controls. Mohammed Benten, a dean at King Fahd University for Petroleum and Minerals in Dhahran, told a local newspaper, "Here in the kingdom, with our strict rules and regulations, we will see the Internet being accessed only for constructive objectives."[79] Minister of Posts, Telephones and Telegraphs Dr. Ali Al-Johani said in February 1996 that, although the Internet was beyond government control, authorities were investigating how it could be regulated.[80]

EUROPE

The European Union is considering adopting some Internet-related controls. In late January 1996, a European Union Consultative Commission on Racism and Xenophobia said it "hope[d] the EU [would] take all needed measures to prevent Internet from becoming a vehicle for the incitement of racist hatred." It also called for the "creation of protective judicial measures."[81] It urged all member states to follow the example of Germany, which has been trying to censor racist and pornographic messages. France joined the call for regulation in early February, when the French minister for information technology announced that France would request members of the EU to draft new legislation to cope with legal issues posed by the Internet. It is believed that France's reaction has to do with the recent posting on the Internet of the banned book, *Le Grand Secret*, by Claude Gubler, the late President Mitterand's physician.[82]

EU culture and telecommunications ministers met informally in Bologna, Italy in late April 1996, to discuss Internet regulation. At the meeting, France proposed the drafting of a global convention on Internet regulation. The ministers agreed to ask the European Commission, the executive body of the EU, to draw up a report on the question. The Commission is reportedly supposed to determine whether the EU should deal with this issue, or whether the issue should proceed directly to international negotiations.[83]

---

[78] Cooper, "The Middle East Gets Caught in the Internet," *Middle East Economic Digest.*

[79] Faiza S. Ambah, "Dissidents Tap the 'Net to Nettle Arab Sheikdom," *Christian Science Monitor*, August 24, 1995.

[80] Saleh Al-Dehaim, "Panel Formed to Study Telecom Privatization," *Arab News*, January 31, 1996, as reported in *Moneyclips*, February 21, 1996.

[81] "EU Group Calls for Curb on Racism on Internet," Reuters, January 29, 1996.

[82] Sylbia Dennis, "Banned Mitterand Book on the Net Ignites French Government," Newsbytes News Network, February 5, 1996, and "French plan to stifle Internet freedom," *New Media Age*, February 8, 1996.

[83] "EU/Media—Commission Studies Mechanism for Preliminary Notification of National Draft Legislation on Internet—ICRT's Position," Agence Europe (Brussels), April 26, 1996.

That same week in Strasbourg, Irish Minister of State for European Affairs Gay Mitchell called on the EU to investigate controls on the transmission of child pornography on the Internet at a joint meeting organized by UNICEF and the Council of Europe, to discuss the commercial exploitation of children.[84]

The European Commission reportedly plans to draft a discussion paper on interactive services, including the Internet, which may lead to a directive that may include content regulation. The European Commission is considering a regulation requiring EU member states to send draft national legislation affecting the Internet to the EU in order for member states to vet the laws before they are adopted. The European Commission is reportedly divided over how to standardize Internet policies of its member states. The European Parliament has introduced changes to the EU's broadcasting law to extend its scope to the Internet, but that approach is strongly opposed by many in the computer industry.[85]

United Kingdom

The UK has not yet enacted any Internet-specific censorship legislation but has relied, instead, on existing laws banning obscenity. Gay groups, however, reportedly feel they are being victimized. An organizer for the London-based group, S&M Gays, for example, told the press that "The police seem to have great difficulty in distinguishing between gay men and pedophiles."[86] The group closed down its computer bulletin board, fearing that it might become a police target.

In its recent proposals for media ownership, the UK government suggested that the media industry regulator could have some influence over the content of the Internet. An inter-departmental group was set up in March 1995 to examine tackling such issues as sexually explicit material on the Internet.[87] A new defamation bill extending libel to computer networks was introduced in February 1996; it provides a defense for ISPs as long as they are do not knowingly permit a defamatory statement to be made over their networks. On-line service providers have asked the government for further clarification on their responsibilities under the legislation.

In March 1996, British Trade and Industry Minister Ian Taylor said the UK was seeking a voluntary approach to regulation of content on the Internet. The Internet Service Providers Association (ISPA), a voluntary grouping of service providers to be formally launched in May 1996, is drawing up a code of practice that will cover fair trading issues, and Taylor said that he expected the code to cover "both illegal and undesirable material." He added, "The only alternative to voluntary action ... is increased political pressure for legislation in various areas. That pressure may get increasingly hard to resist."[88]

France

On March 15, 1996, French ISPs were subpoenaed after a French Jewish student organization brought charges against them for alleged "complicity" in making available propaganda that denies the Holocaust; such propaganda is illegal in France. A decision was to be reached in April, as this report went to press.

Germany

Germany and CompuServe have both been criticized for their roles in the CompuServe censorship episode. CompuServe and the German officials involved have made conflicting statements regarding who actually made the

[84] Patrick Smyth, "Mitchell Argues for World Wide Register of Paedophiles," *Irish Times* (Dublin), April 26, 1996.

[85] Fiona McHugh, "European Commission Makes Moves to Co-ordinate Policing of EU Cyberspace," *Media and Marketing Europe* (London), April 3, 1996.

[86] Liberty, "Caught in the Net," *Agenda* (London), June 1995.

[87] Cath Everett, "Internet Pedophile Case Exposes Gaps in the Law," *Computing* (London) , January 4, 1996.

[88] "UK Back Voluntary Web Censorship," *New Media Age* (London), March 28, 1996.

decision to censor Usenet newsgroups. As far as Human Rights Watch has been able to determine, a task force was set up by the Bavarian minister of the interior at police headquarters in Munich in 1994 to search for on-line child pornography. The task force obtained a search warrant to investigate the Munich CompuServe office on November 22, 1995. The search was reportedly more like a visit, in which the authorities told the company of their concerns and CompuServe agreed to comply. Two days later, CompuServe's German managers reportedly stated that they would support German authorities' fight against pornography in cyberspace. On December 8, the authorities gave them a list of more than 200 suggested newsgroups with a letter saying "...it is left to CompuServe to take the necessary steps to avoid possible liabilities to punishment." CompuServe then made the decision to take all the groups off its servers, apparently without making the effort to look at them. Among the groups it "banned" were discussion groups for homosexuals and the news service Clarinet, which was not even on its servers.

As with other instances of Internet censorship, the ban was an ineffective effort to comply with the demands of an ill-informed authority. CompuServe users still of course had access to the Internet and could therefore connect to other host computers that carried the forbidden newsgroups. In February, CompuServe again provided access to the 200 formerly censored newsgroups, except for five groups. The Bavarian minister of justice recently claimed that CompuServe's new Cyber Patrol software does not meet the company's obligations under German law because the company has an obligation not to supply illegal material to German citizens.

Moving from sexually explicit material to hate speech, in January 1996, Deutsche Telekom (DT), the national telephone company, blocked users of its T-Online computer network from accessing Internet sites used to spread anti-Semitic propaganda, which is a crime in Germany. Authorities also announced that they were expanding their investigation to America Online and Deutsche Forschungsnetz, the national scientific research network. The company was responding to demands by Mannheim prosecutors who were investigating Ernst Zuendel, a German-born neo-Nazi living in Toronto. DT also blocked access to a Santa Cruz, California computer service, Web Communications, that also provides access to Zuendel's site. Web Communications stated that although it did not agree with Zuendel, it was not the company's policy to censor its users. A DT spokesman said that access to certain providers was blocked while government prosecutors investigated on-line neo-Nazi material. The lack of organized monitoring by DT is reflected in the fact that Zuendel's Web site was still available through CompuServe at the same time as it was "banned" through Web Communications.[89]

[89] Reuters, January 25, 1996, and "German Service Cuts Net Access," *San Jose Mercury News* (San Jose, California), January 27, 1996.

Rita Suessmuth, president of the Bundestag, the German parliament, was recently quoted in German newspapers as saying, "The information superhighway must not be allowed to become a forum for those who defile children." She added, "Freedom of expression reaches its limit when human dignity is violated and violence is promoted."[90] The government reportedly disagrees with her assessment, however. Justice Minister Edzard Schmidt-Jortzig said in late March 1996 that the government would introduce Internet censorship legislation before the summer recess. The legislation will seek to punish an ISP only if it knowingly permits illegal material on its service, but will not expect ISPs to be responsible for all the content on their servers.[91] The legislation is expected to face opposition from the regional states, who plan to contest the measure on constitutional grounds and may propose a more restrictive law.[92]

LATIN AMERICA

Internet censorship has not become a major issue in Latin America. Latin America is fully connected, except for Paraguay, Haiti, Belize and Cuba. In May 1996, Cuba, which at present has only e-mail service, will hold its first national telecommunications and informatics conference, Ariadna '96, to discuss the Internet. Jesús Martínez, director of the Center for Automated Information Exchange, the server for Cuba's largest e-mail network, says that regulations affecting electronic information connections and security are being studied "that do not anticipate including individuals."[93] He also told the press that Cuba was "studying regulations about connections and security."[94] Rosa Elena Simeon, the minister of science, technology and environment, said in January that Cuba must learn how to "use the Internet's capabilities and advantages while reducing its risks and disadvantages as much as possible."[95] Guyanese officials also reportedly announced that the government "would move to prevent any 'unauthorized installation' of Internet services—and added that they were studying ways of regulating links."[96]

AFRICA

> [In February 1995] South Africa's Deputy President Thabo Mbeki pointed out to the G7 conference of wealthy countries that there were more telephone lines in Manhattan, New York than in the whole of sub-Saharan Africa." Half of humanity has never made a telephone call," he said.[97]

In Africa, access, technology and training are the huge hurdles to cross before censorship will be a major issue. As of late 1995, fewer than ten countries were directly connected to the Internet. In those countries, however, government control and censorship have already asserted themselves. As in Asia and the Middle East, some countries, such as Botswana, that have Internet access do not allow private ISPs to operate. The reason is reportedly not so much

[90] "Bundestag Seeks World Curbs on Internet Child Porn," *Media Daily* (Wilton, Connecticut), February 13, 1996.

[91] Andrew Gray, "Germany Plans Bill to Punish Internet Indecency," Reuters, March 29, 1996.

[92] *Ibid.*

[93] Dalia Acosta, "Cuba—Communications: Government Wary of Internet," Inter Press Service, January 30, 1996.

[94] "Learning to Fear the Internet," *Latin American Weekly Report* (London), February 15, 1996.

[95] Dalia Acosta, "Cuba—Communications: Government Wary of Internet," Inter Press Service.

[96] "Learning to Fear the Internet," *Latin American Weekly Report*.

[97] The Internet and the South: Superhighway or Dirt Track?, op. cit.

one of content control, but of money. The government is anxious not to lose the revenue from its monopoly on telecommunications services.

In the southern African country of Zambia, where Internet access is limited, the February 5 Internet edition of *The Post*, a daily and one of Zambia's most important opposition voices, was banned by President Chiluba under the State Security Act. The charges relate to a report based on leaked documents, revealing secret government plans to hold a referendum on the adoption of a new constitution. It remained on the Web site for two days until the police warned the ISP, Zamnet Communications, that it would be liable.[98]

CONCLUSION: PRINCIPLES OF FREE EXPRESSION ON THE GII

Rather than striving to control content on the Internet, democratic governments should be working to ensure that the GII becomes truly global, and to motivate citizens to become more involved in decision making as they organize, debate, and share information unrestricted by geographic distances or national borders. It has already been shown that the GII has the potential to:

- permit individuals with common interests to organize themselves in forums to debate public policy issues;
- provide instant access to a wide range of information;
- increase citizen oversight of government affairs;
- decentralize political decision making;
- empower users to become active producers of information rather than passive consumers.

As noted above, although the extraordinary potential for a GII has been suggested by existing on-line communications networks, the present on-line community is still quite limited. Only countries with a sophisticated telecommunications infrastructure are able to take full advantage of on-line technology. Even in countries with advanced telecommunications infrastructures, only persons with access to equipment and training can take advantage of new information resources. General illiteracy remains the primary obstacle to computer literacy. And while the GII may foster an unprecedented sharing of cultural traditions, current users of on-line technology are primarily American or northern European, affluent, white, and male.

To maximize the GII's potential to promote democracy, it must adopt and expand upon international standards of free expression. National and international guarantees of free expression should be expressly extended to the Internet.

[98] David Lush, Media Institute of Southern Africa, "Action Alert Up-Date--Zambia," February 16, 1996.

ACKNOWLEDGMENTS

This report was researched and written by Karen Sorensen, on-line research associate at Human Rights Watch. Her work was based in part on a letter prepared by 1995 Bradford Wiley Fellow Ann Beeson, for the GII conference in Brussels. The report was edited by Gara LaMarche, associate director of Human Rights Watch. We wish to acknowledge the leading role played by several nongovernmental organizations in fighting Internet censorship in the United States—including the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), the Center for Democracy and Technology (CDT), and Computer Professionals for Social Responsibility (CPSR). We especially wish to thank Marc Rotenberg of the Electronic Privacy Information Center (EPIC) for his comments on this report. Similar organizations have been formed in other countries, including Electronic Frontiers Canada and Electronic Frontiers Australia. Human Rights Watch hopes by issuing this report to contribute to the effort to afford on-line communication the same protections as other media.

Human Rights Watch

Human Rights Watch is a nongovernmental organization established in 1978 to monitor and promote the observance of internationally recognized human rights in Africa, the Americas, Asia, the Middle East and among the signatories of the Helsinki accords. It is supported by contributions from private individuals and foundations worldwide. It accepts no government funds, directly or indirectly. The staff includes Kenneth Roth, executive director; Cynthia Brown, program director; Holly J. Burkhalter, advocacy director; Barbara Guglielmo, finance and administration director; Robert Kimzey, publications director; Jeri Laber, special advisor; Gara LaMarche, associate director; Lotte Leicht, Brussels office director; Juan Méndez, general counsel; Susan Osnos, communications director; Jemera Rone, counsel; and Joanna Weschler, United Nations representative. Robert L. Bernstein is the chair of the board and Adrian W. DeWind is vice chair.