UNITED NATIONS **A**

General Assembly

Distr.
GENERAL

A/CONF.189/PC.2/12
27 April 2001

Original: ENGLISH

WORLD CONFERENCE AGAINST RACISM,
RACIAL DISCRIMINATION, XENOPHOBIA
AND RELATED INTOLERANCE

Preparatory Committee
Second session
Geneva, 21 May-1 June 2001
Item 6 of the provisional agenda

REVIEW OF REPORTS, STUDIES AND OTHER DOCUMENTATION FOR THE PREPARATORY COMMITTEE AND THE WORLD CONFERENCE

Report of the High Commissioner for Human Rights on the use of the Internet for purposes of incitement to racial hatred, racist propaganda and xenophobia, and on ways of promoting international cooperation in this area

GE.01-13724 (E)

CONTENTS

Introduction

1. In its resolution 1999/78, the Commission on Human Rights requested the United Nations High Commissioner for Human Rights to, inter alia, undertake research and consultations on the use of the Internet for purposes of incitement to racial hatred, racist propaganda and xenophobia, and to study ways of promoting international cooperation in this area.

2. This report initially describes the degree of Internet use worldwide and the ease with which persons can communicate with others across nations via this medium. It then describes how individuals and groups with racist beliefs and agendas have availed themselves of this rich communication resource to establish and strengthen ties amongst themselves and to make their racist materials, in increasing volume and with increasing sophistication, available online to Internet users.

3. The accelerating appearance of racist content on the Internet has prompted vigorous responses by a variety of agents, including Governments, international organizations and private organizations. Some of these efforts target the creators (or "authors") of racist content or the entities that store and facilitate access to (or "host") it. The aim, in the one case, is to get the creator to remove the content and, in the other case, to get the host to remove or otherwise block access to it. Other efforts focus on end-users, the ultimate recipients of the content. These efforts aim to empower end-users, for example by enabling them to know in advance about, and to avoid, sites with content they find objectionable or harmful. This report describes efforts of both sorts.

4. A number of national court systems, for instance, have targeted the creators of racist content and those hosting it. A French court held a United States Internet company liable for allowing access by French residents to illegal materials. A German court permitted prosecution of an Australian resident for posting illegal content outside Germany that was accessible by Internet users within Germany. An Australian commission directed the same Australian resident to remove his illegal material from a hosting provider within Australia. And a Canadian court is currently determining the applicability of a civil law provision targeting hate speech to a Web site hosted in the United States.

5. Some countries monitor Internet content that arrives on hosts located within their jurisdictions and condition the issuance of licences for such providers on their prohibiting access to illegal or harmful material. Some of these countries also criminalize or create civil liability for visits by end-users to prohibited sites.

6. Some efforts by private and quasi-private organizations also target content creators or hosting providers. One such effort involves the operation of "hotlines", to which persons can make complaints about Internet content that they believe is illegal or harmful. The hotlines examine the complaints and, if they agree that the material is improper, direct or request the offending hosting provider to prevent access to the material or to remove it. Another effort, by many organizations of Internet providers and by some individual providers involves the adoption of codes of conduct or rules that commit them to refusing to host illegal or harmful content, including racist content, and to removing such content once it appears at their sites.

7. Approaches by a number of private companies and groups focusing on protecting and empowering end-users include the development of filtering software and of content labelling. Filtering software products enable end-users to block access from their home or office computers to problematic content. Content-rating systems provide for electronic rating and labelling of Internet sites for content, enabling end-users to have a sense of what is at a site without having to access it, and therefore to avoid visiting sites they find objectionable.

8. Various international efforts, formal or informal, against racist content have implications both for the regulation of content creators and hosts, and for the empowerment of end-users. The International Convention on the Elimination of All Forms of Racial Discrimination, for example, directly addresses the "dissemination of ideas based on racial superiority or hatred", and thus implicates Internet-based racist content. The European Union has adopted an "Action Plan on Promoting Safer Use of the Internet". And numerous seminars and conferences, hosted by the Office of the United Nations High Commissioner for Human Rights (OHCHR), the Organization for Cooperation and Development (OECD) and others, have met to discuss and to encourage international cooperation, inter alia, in the fight against Internet-based racism.

9. Finally, organizations around the world have developed education and outreach strategies, available on the Internet, devoted in some or large measure to Internet-based racism. These sites are often interactive, informative and entertaining; they attempt to combat racist content by exploding racist myths, providing information about anti-racist organizations and encouraging visitors to join in the fight against racism.

I. INTERNET USE AND RACIST SPEECH ON THE NET

10. The Internet is a worldwide network to which individuals can connect via their own personal computers or other electronic devices. There has been a great increase over the past few years both in the number of computers hosting Internet content and in the number of end-users. As of 2000, there were approximately 104 million Internet host computers.[1] This represents an enormous expansion from the Internet's modest beginnings: for example, in 1991, approximately one decade after the creation of the Internet Protocol (IP), the number of host computers was about 0.7 million; by 1996, this figure had increased to approximately 22 million.[2] Moreover, the number of persons estimated to use the Internet currently in some capacity or other is over 390 million.[3] Of these, roughly 70 per cent are from Europe, the United States or Canada; an additional 15 per cent are from Australia, China or Japan. It is expected that there will be as many as 774 million users worldwide by 2003.[4]

11. All that is needed for typical home users to connect to the Internet is a computer, a telephone line and a means of dialling out through it; moreover, in the vast majority of cases, such connections can be made for the mere cost of a local telephone call.[5] Once connected, users can connect to virtually any web page available on the World Wide Web. Additionally, they can communicate privately via email with persons located anywhere in the world; and they can communicate more publicly, by participating in "chat rooms" or by joining email groups. Finally, they can, at minimal cost, post content of their own creation on their own web pages, accessible by others from anywhere else on the Internet. They are not even restricted to posting their web pages on Internet service providers (ISPs)[6] located in their local jurisdictions; they can, rather, find ISPs in virtually any location they wish and post their web pages there.

12. These very characteristics that make the Internet an extraordinary communication resource make it an important resource for individuals and groups seeking to spread messages of racism and hate. Sometimes socially marginalized and geographically remote from each other, often not affluent and thus not able either easily to communicate with each other or to publish their hate messages in sophisticated media such as newspapers or broadcast media, such individuals and groups find the Internet a welcome ally.

13. For example, the Internet makes it relatively simple for like-minded racists and bigots, scattered around the world, to find each other. They can employ USENET, a network of thousands of public discussion groups: once there, they can initiate, or participate in, racist exchanges. Perfectly visible exchanges with overt racist content in fact occur daily on USENET, at sites with names such as *alt.politics.white-power* and *alt.revisionism*.[7] Similarly, these persons can employ electronic mailing lists to send email messages of racist hatred to each of the addresses on such lists. Once such connections between like-minded racists have been made, they can be maintained and reinforced through private email. In all these ways, racists are able to get the sense that their opinions are shared by others all over the world, thus reinforcing their commitment to their bigotry and fuelling their feelings of empowerment.

14. In addition to enabling them to communicate amongst themselves, the Internet provides these individuals and groups with the power to make their opinions available to the entire Internet public. Like anyone else, they may create their own web pages and post them on ISPs where any person connected to the Internet may have access to them. These sites may, and many in fact do, contain hundreds or thousands of pages of racist material. Many sites will have sophisticated accompanying graphics and music. They can be entertaining to visit, beguiling in their subtlety and effective in communicating their message.

15. There is no doubt that racists around the world have discovered that the Internet can be an attractive and effective medium for them. Just six years ago, only one racist hate site, named *Stormfront*, existed on the Internet. Within four years, according to one estimate,[8] there may have been as many as 2,000 such sites on the Net. Other estimates are somewhat lower. In any event, it is generally agreed that the number of racist sites available online is, at the very least, well into the hundreds. The Southern Poverty Law Center, for example, has recently estimated that the number of racist hate sites operated in the United States alone exceeds 350.[9]

16. Racists of all beliefs can find materials to their liking on the Internet. *Stormfront*, for example, greets the visitor with the logo "White Pride World Wide", and advertises that it is "a resource for those courageous men and women fighting to preserve their White Western culture … [and is] a forum for planning strategies and forming political and social groups to ensure victory". Moreover, in addition to providing content of its own, *Stormfront* hosts other racist sites. One such site, *Jew Watch*, contains articles and other writings on anti-Semitic themes, with such titles as "World War Two Slave Labor Issues and Greedy Jewish Lawyers" and "The Rothschild Internationalist-Zionist-Banking-One World Order Family". At certain Web sites, for example the one operated by Kahane.org, Arabs generally and Palestinians in particular are vilified.

17. Other sites champion Nazism, or specialize in Holocaust denial. *Our Legacy in Truth* (another site hosted by *Stormfront*) contains writings from "the National Socialist cause",

including “White Power”, and “The National Socialist Platform”. And at the *Zundelsite*, it is denied that there was an order at the highest levels for the genocidal killings of Jews and others, and asserted that far fewer people died in concentration camps than has been claimed by responsible historians. In addition, various sites offer for sale or trade racist and other extreme right wing material, including Mein Kampf and books denying the Holocaust.

18. Internet racist sites are tailored not only for “like-minded” adults, but for the not-yet-persuaded as well, including children. A site operated by the World Church of the Creator, for example, contains a so-called “kid’s page” with explicit racist content in story form. *Stormfront* too contains a “kid’s page”.

19. In sum, there is a substantial and flourishing network of Internet sites devoted to spreading racist propaganda throughout the “connected” world. Such sites attract the attention not only of racists themselves, but of innocent third parties, adults and children, who may only come across them accidentally, but who may well be susceptible to the hatred and lies to be found there. This very significant problem has attracted, increasingly, the attention of Governments, private groups and concerned individuals everywhere, and the past few years have seen vigorous responses to this growing phenomenon. These responses are detailed below.

II. GOVERNMENTAL RESPONSES TO INTERNET-BASED RACIST SPEECH

A. Cases in national courts

1. France

20. In November 2000, a French court granted a petition requiring Yahoo!, Inc. (Yahoo), a United States-based Internet company, to prevent French citizens from accessing certain content hosted on Yahoo’s sites - even though these sites had a physical presence outside of France.

21. The basic facts of the case are as follows. Among the many Internet services that it provides, Yahoo operates an automated online auction site from the United States, accessible to any person connected to the Internet. Available for sale at the site are items displaying the swastika and other Nazi symbols. Persons accessing the Internet from within France were able to access this site, either directly or indirectly, for example by connecting to Yahoo’s local French subsidiary, Yahoo.fr, which contained a link to the United States site.

22. The complainants in the case, the League against Racism and Anti-Semitism, and the French Union of Jewish Students, had petitioned the court to order Yahoo to “institute the necessary measures to prevent the display and sale on its site … of Nazi objects throughout the territory of France”.[10] Yahoo had argued that the petition should be denied on a number of grounds, including (i) that the French court did not have territorial competence to hear the case because the acts alleged - the operation of the auction site - took place in the United States and not in France and (ii) that it was technically impossible to identify, and to block access to the site by, Internet users who were resident in France.

23. In its initial order, the French court concluded, first, that the sale of such Nazi symbols violated French law prohibiting the sale of racially inciteful material. Second, it concluded that, by permitting that material to be viewed in France, Yahoo in the United States was committing a wrong in the territory of France. Third, the court concluded, provisionally, that Yahoo had the technical competence to prevent French Internet users from accessing the auction site. On the one hand, the court believed that Yahoo could identify the geographical origin of most visitors to the auction site from the visitor's IP address, and that it could block access to the auction by any person identified as being connected from French territory. On the other hand, Yahoo could deny access to any person who had reached the auction site via sites providing anonymity, by denying access to any visitor failing to reveal his geographical origin. Accordingly, the court granted the petition, ordering Yahoo to "take all necessary measures to dissuade and render impossible any access via [*toute consultation sur*] Yahoo.com" to the auction site by persons located in France.[11]

2. Germany

24. Germany has taken a number of steps, both judicially and legislatively, in the area of Internet-based hate speech. In the mid-1990s, the Munich Public Prosecutor inquired into the possibility of applying certain provisions of the Criminal Code both to ISPs that provide access to and host illegal speech, and to the creators of such speech. Potentially applicable Criminal Code provisions included the prohibition of defamation and denigration of the character of deceased persons, incitement to violence and hatred, and Holocaust denial. Specifically, the Prosecutor investigated CompuServe (a subsidiary of CompuServe in the United States) for its hosting of pornographic sites. In response to this investigation, and before any judicial proceedings, CompuServe removed the offending material from the Internet.[12] The following year, a German Internet firm, T-Online, elected to block all access to Web Communications, an ISP that hosted the *Zundelsite*, upon learning that German prosecutors were looking into the site.[13] In addition, the Public Prosecutor in Mannheim charged the creator of the site, Ernst Zundel, with violating the German prohibition on the depiction of violence. The Prosecutor noted that the ISPs that provided access to the Zundel Web site located outside Germany might be liable as well.[14]

25. In 1997, Germany passed into law the Act on the Utilization of Teleservices, commonly known as the Multimedia Act. The Act provides for criminal liability for ISPs that knowingly make illegal content available, if it is technically possible and reasonable for the ISP to refrain from doing so. The following year, Felix Somm, a managing director of CompuServe, was convicted of violating the Act for having provided access for German Internet users to illegal pornographic material.[15] This conviction was overturned by a Bavarian court in 1999; the basis for that court's decision was its finding that Somm could not reasonably have done more to block access to the site than he did. There was no suggestion, however, that the Act could not be applied to an ISP in a proper case.[16]

26. Most recently, in December 2000, the highest German court on civil affairs, the *Bundesgerichtshof*, expressly ruled that German law can be applied to foreigners who post illegal content on the Web in other countries, as long as the content can be, and is, accessed by persons within Germany.[17] The court reversed a lower court ruling in the prosecution of an Australian

Holocaust denier, Frederick Toben. Toben had been arrested in 1999 when, on a visit to Germany, he had distributed leaflets denying the Holocaust. The lower court had convicted Toben on the charge of offending the memory of the dead, but held that Toben could not be convicted under the law against inciting racial hatred because the inciting material existed on a foreign Web site. However, the *Bundesgerichtshof* concluded that German laws banning the Nazi party and any glorification of it could be applied to Internet content originating outside German borders but accessed from within Germany, and in particular to the content on Toben's Web site.

3. Australia

27. Like Sweden and the United States (see below), Australia has recently enacted a law that specifically targets problematic Internet content. Specifically, an amendment to the Broadcasting Services Act came into force on 1 January 2000. The amended Act prohibits Internet content that would be classified as RC ("Refused Classification") or X by the Australia Classification Board and it implements a system by which Australian citizens can lodge complaints with the Australian Broadcasting Authority (ABA) about actual or suspected RC or X classifiable content.[18] In the event that the ABA determines, after having received a complaint, that the content complained of is RC or X, it is directed to issue a "final take-down notice" to the hosting ISP (or an interim take-down notice, should the ABA determine that the content has not yet been classified, but that it would be classifiable as RC or X). The Act requires an ISP to comply with the take-down order. If the ISP does not comply, it is subject to prosecution. Finally, the Act is not restricted to ISPs that are physically located within Australia: with respect to RC- or X-rated content hosted outside Australia, the Act directs the ISP to "take all reasonable steps to prevent end users from accessing the content".[19]

28. RX-classified content can include racist content. As recently explained by the Attorney-General of Australia material on the Internet "which promotes, incites, or instructs crime or violence against a particular ethnic group … will be refused classification [i.e., would be classified RC] by the Australian Broadcasting Authority" and would be banned.[20] Such material, if brought to the attention of the ABA, would be ordered removed from the hosting ISP.

29. In addition to operating the system just described, Australia has seen the application of an existing law, the Federal Racial Discrimination Act, to attempt to shut down an Australian racist site. The Act is administered by the Human Rights and Equal Opportunity Commission, whose decisions are not binding.

30. The Commission recently heard a case involving the same Australian Web site that had resulted in Frederick Toben's conviction in Germany. The site, containing material denying the Holocaust, was found by the Commission to contain "vilificatory, bullying, insulting and offensive" material, in breach of the Act. The Commission ordered the material to be removed from the site.[21]

31. Initially, Toben refused to comply with the Commission's order. However, a committee of management of the Executive Council of Australian Jewry has asked the Australian Federal Court to enforce the order.[22] A decision has not been reached at the time of writing.

4. Sweden

32. The Act on Responsibility for Electronic Bulletin Boards was enacted in Sweden in 1998. The definition of "bulletin board" in the Act is sufficiently broad to encompass material hosted by ISPs. The Act requires ISPs to monitor content under some circumstances and to remove or make otherwise inaccessible content that is "obviously such as is referred to in the Penal Code", including the provision prohibiting "racial agitation". ISPs violating the Act are subject to civil penalties.[23]

5. Canada

33. Canadian law has a number of anti-hate and anti-racist speech provisions. In particular, in addition to Criminal Code provisions, section 13 of the Canadian Human Rights Act, a civil measure, targets the telephonic communication of messages that are "likely to expose [persons to] hatred or contempt" based, among other things, on their race. The Act creates a Human Rights Tribunal, which hears cases alleging violations of the Act.

34. In 1997, a Tribunal convened to hear a complaint brought against Ernst Zundel, a Canadian, based on the accessibility from within Canada of the *Zundelsite*, which is located on a server in the United States. Among the Principal issues that the Tribunal was called upon to decide were (i) whether the Internet is a "telephonic device", (ii) whether Zundel could be said to control the site, given that it existed physically outside Canada, and (iii) whether the site, in denying the Holocaust, among other things, promotes hatred.

35. The case has been ongoing for three years. At this juncture, the applicability of section 13 of the Canadian Human Rights Act, as well as the jurisdiction of the tribunal, have been upheld by a Canadian federal court. Final arguments on appeal have just been heard and a decision is awaited.[24]

6. United States of America

36. The United States Congress attempted to address specifically the problems posed by certain problematic Internet speech, by enacting the Telecommunications Act of 1996. One of the provisions of the Act targeted the conveying of certain content by an "interactive computer service". Specifically, the Act prohibited the sending of information depicting sexual activities to any person under 18 years of age in terms that were "patently offensive as measured by contemporary community standards". The aim of this provision of the Act was to prohibit the display by an ISP to a minor of pornographic and indecent materials.

37. The United States Supreme Court determined that this provision of the Act violated the free speech guarantees of the First Amendment of the United States Constitution and on this basis struck the provision down.[25] As will be seen immediately below, this decision by the Court has direct consequences for the legality of regulating racist Internet content in the United States.

38. In its decision, the Court acknowledged that the transmission of obscenity and child pornography to minors was illegal under an already-existing federal law. But the provision of the Act before it, the Court explained, went beyond prohibiting obscenity and pornography to

minors. It also prohibited "patently offensive" material which could "cover large amounts of non-pornographic material with serious educational or other value".[26] Moreover, the provision could apply to communications between groups consisting mainly of adults, for example in a chat room, if even one minor were present electronically in the room. Because the communication of at least some "patently offensive material" between adults was a form of speech protected by the First Amendment, and because such speech could easily be curtailed by the provision, the Court concluded that it could not let the provision stand, writing that "[a]s a matter of constitutional tradition, ... we presume that governmental regulation of the content of speech [on the Internet] is more likely to interfere with the free exchange of ideas than to encourage it".[27]

39. This case has immediate consequences for the prospects of regulation by the Government of the United States of Internet-based racist speech occurring on sites hosted in the United States. The United States Supreme Court has made it clear that, like much speech that is "patently offensive", racist speech is protected by the First Amendment.[28] If, as that Court has said, the transmission over the Internet of patently indecent sexual materials is protected by the First Amendment, then so is the transmission of racist materials. Thus, it is not to be expected that the United States will enact legislation regulating such Internet content.

B. Governmental regulative efforts

40. Many countries require ISPs serving local computer users to operate under State licences, and have conditioned the granting of such licences on the regulation of objectionable content.

41. For example, in March 1996, the Singapore Broadcasting Authority (SBA), the government agency that regulates broadcasting in Singapore, put in place a comprehensive scheme of Internet legislation designed to protect local values.[29] These regulations apply, inter alia, to ISPs that provide content for economic, political or religious purposes on the Internet - and thus, have potential application to racist speech. The regulations require any entity that wishes to operate as an Internet provider in Singapore to obtain a license. Any Internet sites that the SBA determines contain improper content must be "blacklisted" by any licensee. In addition, ISPs are required to use their best efforts to ensure that their services are not used for any purpose that is "against the public interest, public order or national harmony".

42. The regulations are enforced in part by the use of servers operated by the Government - in technical terms, "proxy servers".[30] ISPs are required to route their customers through the Government's servers which, in turn, deny access to blacklisted sites. Any ISP that fails to follow the regulations is subject to licence suspension or fines. Moreover, any user who visits prohibited sites is subject to penalties, including jail terms. However, it is to be noted that in the typical situation, users without the appropriate proxy settings cannot access the Internet and those with such settings will have their access to prohibited sites blocked.

43. China has adopted a very similar strategy, monitoring Web sites for objectionable content and requiring ISPs to route their users through government proxy servers. In addition, in October 2000, the Government of China implemented formal regulations imposing monitoring responsibilities on ISPs themselves.[31] The regulations prohibit the release or dissemination of,

among other things, information instigating ethnic hatred or discrimination. ISPs are required to maintain logs of the information posted on their sites and must turn them over to authorities upon demand. Violators face fines of as much as US$ 120,000 and closure.[32]

44. Some other countries have implemented, or are planning to implement, the same kind of system. The Government of Viet Nam promulgated regulations in May 1996 according to which all ISPs must register with, and are subject to inspection by, the Government. The Government has said it is committed to shutting down ISPs that permit access to content harmful to national interests.[33] In Bulgaria, the Committee of Posts and Telecommunications recently stated its intention to make local ISPs subject to general licensing and added that Internet content should be scrutinized for, among other things, racist content.[34]

III. INTERNATIONAL RESPONSES

45. A number of coordinated governmental responses to Internet-based racism have emerged. Some of these are formal; some are informal.

46. In the former category is the application in this context of the International Convention on the Elimination of All Forms of Racial Discrimination. Article 4 (a) of the Convention provides that State parties "shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred [and] incitement to racial discrimination" and article 4 (b) provides that States parties "shall declare illegal and prohibit … organized and all other propaganda activities, which promote and incite racial discrimination". In 1985, the Committee on the Elimination of Racial Discrimination noted in its General Recommendation VII that article 4 is of a mandatory nature.

47. Eighteen States parties have made reservations to or declarations concerning article 4. A number of these States have emphasized the requirement under article 4 that, when adopting legislation pursuant to article 4 (a), (b) or (c), States must have "due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5" of the Convention. Two countries, Japan and the United States, have asserted, in reservations, that they accept obligations under article 4 only to the extent that such obligations are compatible with their respective Constitutions.

48. Another formal effort is the Action Plan on Promoting Safer Use of the Internet, adopted by the European Union by decision in 1999 (Decision).[35] This Plan, covering a four-year period from January 1999 to December 2002, is meant to deal with "harmful and illegal content carried over the Internet". It contains the following specific goals:

(a) Establishing a European network of hotlines. The Decision recognizes that the responsibility for prosecuting the creators of illegal content would remain with national law-enforcement authorities; the principal function of the hotlines would be to reveal the existence and location of illegal material. The Decision takes note of the existence of hotlines in some European States,[36] but notes that, in addition to the need to establish more of them, there is a need to establish mechanisms for the exchange of information between these organizations.

(b) Encouraging self-regulation and codes of conduct. To this end, the Decision foresees the development of guidelines at the European level for codes of conduct, including "a system of visible 'quality-Site Labels' for Internet Service Providers".

(c) The development of filtering and ratings systems, with the aim of making content easier to identify. The Decision acknowledges the existence of a number of such systems, but notes that, at present, their sophistication level, and their uptake by European content providers, is low. The Decision contemplates that the rating systems to be developed should be internationally compatible, pursuant to international agreement, and expects a concerted effort to encourage use of such systems by content providers.[37]

(d) Implementation of a "European campaign and an information and awareness action programme" to protect minors from being confronted with harmful content. The Decision contemplates awareness initiatives building on "dissemination of information from access providers to customers" in addition to the development of educational materials.[38]

49. In addition to these formal international efforts, an increasing number of international meetings and conferences have witnessed the participation of Governments, NGOs, and industry groups in efforts directed towards regulation of Internet content, including racist content. Examples include seminars conducted by OHCHR in 1997 (expert seminar on the role of Internet in the light of the provisions of the International Convention on the Elimination of All Forms of Racial Discrimination[39]) and 2000 (expert seminar on remedies available to the victims of acts of racism, racial discrimination, xenophobia and related intolerance and on good national practices in this field[40]); the Forum on Internet Content Self-Regulation, co-hosted by the OECD and the Business-Industry Advisory Committee in 1998;[41] the Internet Content Summit, hosted by the Bertelsmann Foundation and INCORE in Munich in September 1999;[42] the Stockholm International Forum Combating Intolerance in Stockholm in January 2001;[43] the conference entitled, "The Internet and the Changing Face of Hate: An International Dialogue", organized by the German Federal Ministry of Justice, the Friedrich Ebert Foundation, and the Simon Wiesenthal Centre, in Berlin in June 2000; and the annual INET conferences operated by the Internet Society.[44]

IV. APPROACHES BY INDUSTRY AND OTHER PRIVATE ORGANIZATIONS

A. Hotlines

50. Organizations in various countries have adopted, sometimes in concert with their national Governments, a hotline approach to combating illegal and harmful Internet speech, including (in many instances) racist speech.

1. The Netherlands

51. In 1997, the Complaints Bureau for Discrimination on the Internet in the Netherlands (MDI) was founded. Initially it was a volunteer organization; now, however, it is State-funded. Internet users in the Netherlands who believe they have found content on the Internet that violates Netherlands law[45] can notify MDI about the site where such content can

be found. Upon receiving a complaint, MDI examines the content complained of. If MDI determines that the content violates law, it directs the hosting ISP to remove it. Usually, the ISP complies. For example, in 1999, 158 "illegal expressions" out of 178 were removed from the Internet.

52. MDI works closely with the National Expertise Centre on Discrimination, part of the Attorney's Office. In the event that an ISP does not remove offending content after being so directed, MDI may prevail upon the Centre to prosecute the person or persons responsible for posting the content. Moreover, there is a likelihood that an amendment to the Netherlands Law on Computer Criminality will shortly come into force. Under this amendment, Netherlands ISPs that host illegal content and that refuse to remove it after being so directed by MDI may be subject to criminal liability under certain circumstances.[46]

2. United Kingdom of Great Britain and Northern Ireland

53. A similar arrangement exists in the United Kingdom. In 1996, the Internet Watch Foundation (IWF), a body funded by local ISPs, was created, pursuant to an agreement between industry, government and law enforcement agencies. Like MDI, IWF fields complaints about illegal Internet content. Also like MDI, when IWF determines that certain content violates United Kingdom law, it asks the hosting ISP to remove it. Although the ISP is not required to remove the content, if it complies with the IWF request, it is shielded from prosecution. While IWF was initially created in an effort to combat Internet-based child pornography, the Home Office last year requested IWF to expand its mandate to include racist content that would violate the law.[47]

3. Other hotlines in Europe; INHOPE

54. A number of other European hotlines have been established in the past few years. Among those whose focus includes racist speech are the FSM (Voluntary Self Control for Multimedia Service Providers) in Germany, which targets "racist or fascist material" as well as pornography, and the ISPA (Internet Service Providers Austria) in Austria which deals with, among other things, "right wing radicalism".

55. Most hotline organizations in Europe belong to a hotline association, called INHOPE (Internet Hotline Providers in Europe). The principal focus of INHOPE is on child pornography Web sites. However, it has taken explicit note of the growth of racist content on the Internet and its mission "to protect young people from harmful and illegal uses of the Internet" appears to contemplate efforts against racism as well. In pursuit of this mission, INHOPE is committed "to facilitat[ing] cooperation between European Internet hotline providers", to establishing and resourcing current and new hotlines, and to fostering Internet safety awareness and education in Europe.[48]

B. Codes of conduct and other voluntary restraints

56. Numerous associations of ISPs have voluntarily adopted codes of conduct for their Internet operations. These codes cover a wide range of matters, from principles of "netiquette",

to confidentiality measures, to conditions to be specified in agreements with users, to principles of content regulation. In many such codes, the latter principles include commitments to prohibit the hosting of racist sites.

57. One such association is EuroISPA, which describes itself as "the pan-European association of the Internet services providers' associations of the countries of the European Union".[49] Its members include ISP organizations in Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, the Netherlands and the United Kingdom.

58. EuroISPA's general aims include promoting the interests of Europe within the global Internet and delivering the benefits of the Internet to its users while at the same time meeting the legitimate concerns of parents and others about the potentially harmful content that may reside on certain Web sites. The codes of conduct of its various members reflect these general goals. Some include commitments to the specific goal of combating harmful content, including racist content. For example, the code adopted by the French *Association des fournisseurs d'access et de services Internet* (AFA) provides that its members (i.e., ISPs in France) should be on guard for "manifestly illegal" content, by means of being aware of the criticisms of users, monitoring particularly popular web pages, and "automatically detecting" suspicious words.[50]

59. An association of ISPs in Japan, the Telecom Services Association ("Telesa") operates under a Guideline for Codes of Practice for Internet Service Providers.[51] Article 7 of this Code provides that ISPs should specify in their user agreements that users should not dispatch illegal or harmful communication, including (according to the accompanying explanation) "information which ... slanders, and discriminates others". This article also directs members who have knowledge that a sender has dispatched harmful or illegal information to the public, to request the sender to refrain from dispatching the information to attempt to prevent users from receiving the information, and, if necessary, to terminate the sender's ISP services. In addition, members are directed to monitor and collect relevant information about contents that have been the subject of complaints.

60. The Internet Industry Association (IIA) in Australia, in conjunction with the ABA, and in observance of the Broadcast Services Act, has detailed the steps that member ISPs should take with respect to content regulation, pursuant to the IIA goal of "facilitat[ing] end-user empowerment ... [for taking] greater control for content accessible via the Net". These steps include taking reasonable steps to encourage commercial content providers to use appropriate labelling systems and to provide appropriate filters. Because, as noted above, racist content is likely to receive an RC rating from the ABA, such content will be targeted by the labelling and filtering systems to which the IIA is committed.[52]

61. Finally, the Code of the Canadian Association of Internet Providers provides that members should "make a reasonable effort to investigate legitimate complaints about alleged illegal content". In addition, the Code commits members to educate the public about Internet-related and technology issues.[53]

62. While, as yet, no association of ISPs in the United States has developed regulations regarding racist speech, a few important United States-based ISPs have developed individual policies on their own in this area. Among free web-based hosting services that have adopted

such policies is Angelfire, whose rules provide that "pages cannot contain, or contain links to, any of the following: nudity, sex, pornography, foul language, hate propaganda". In fact, Angelfire had, previous to the promulgation of these rules in 1998, hosted some sites with racist material; these sites were removed once the new rules became effective.[54]

63. Some important fee-based hosting providers in the United States have adopted similar policies. Like Angelfire, America Online changed its formerly permissive policy in 1997. It now prohibits "hateful language" and attacks based on "a person's race, national origin, ethnicity or religion". As a result of this change, AOL removed some Web sites from its servers. Another provider, Prodigy Internet, bans "blatant expressions of bigotry, racism and/or hate".[55]

64. Finally, it should be noted that numerous private organizations devoted to the eradication of racism have exerted and continue to exert pressure on ISPs to ban racist content. To take just a single example, the Simon Wiesenthal Center recently successfully pressured Yahoo to remove several Web sites with racist materials; and it is currently working with Amazon.com and Barnesandnoble.com to stop them from selling literature by the founder of the American Nazi Party.

C. Filtering software

65. Various software products have been developed to enable end-users to combat the problem of racist and other problematic Internet speech. Some such products block access to (or "blacklist") sites that the user or manufacturer identify as undesirable. Others only permit access to (or "whitelist") sites that the user or manufacturer deem desirable. Most of these products provide an initial list of sites containing problematic material. End-users are sometimes able to add or delete sites to the list as they see fit. When a user who does not possess the password to disable the software enters the Universal Resource Locator (URL) or IP address of a site on the list, the software prevents the computer from accessing the site.

66. Other filtering products work on the basis of "keyword" searches. Certain words are predetermined to be strong signs of racist or other problematic content; again, end-users can usually add or delete words from the list. A typical such product is *Net Nanny*, which works by automatically blocking a host computer in the event that any of the words in its built-in glossary are encountered during an Internet search. This automatic block-out can only be overridden by someone who possesses the applicable password.

67. Many of these filtering products, including *SurfWatch*, *Cyber Patrol*, *Net Nanny*, *CyberSitter* and *HateFilter*, have application specifically for hate speech and are generally inexpensive.

D. Rating systems

68. Rating systems are intended for use in conjunction with browser-based and stand-alone filtering technologies. In the typical situation, a content creator rates or categorizes the content on his site. (Alternatively, and as noted below, parties other than the content creators may rate content at sites of interest to them.) The rating is, in one way or another, available to the end-user's filtering system, which determines, based on the rating and its filtering criteria, whether it will provide access to a particular site.

69. A number of different rating systems were developed in the mid 1990s, but they were somewhat inconsistent with each other and they were not particularly popular with end-users. Beginning with the inception of the Internet Content Rating Association (ICRA) in 1999, however, the rating system effort has taken on momentum.

70. ICRA is an independent non-profit organization based in Europe and North America. Its members include some of the largest Internet companies and research entities, including AOL, Inc., British Wireless, UUNet, Microsoft, IBM, Novell, Bell Canada, T-Online International AG, Cable & Wireless, and the Bertelsmann Foundation. Other member organizations include IWF, EuroISPA and the Parents Advisory Group for the Internet.[56]

71. ICRA has been involved in an effort to develop and implement an objective and culture-neutral rating system that may be adopted by content providers and employed widely by end-users. The system was inaugurated on 13 December 2000.[57]

72. The system uses PICS (Platform for Internet Content Selection) from the Worldwide Web Consortium,[58] which enables the association of labels with content. The typical situation contemplated involves a content creator visiting the ICRA Web site and there filling in a questionnaire. Questions in the questionnaire bearing on possible racist content include whether the content might be perceived as setting a bad example for young children and whether it promotes harm against people. ICRA suggests that the questionnaire can be adapted to varying individual and cultural needs.

73. Once the content creator submits the questionnaire to ICRA, the system generates a short code representing a content label, which the content creator adds to his site. The computer of any visitor to the site will register the content label and the end-user will thereby be informed as to the nature of the content there.[59]

74. Once sites are labelled for content, lists of sites to be avoided (or to be visited) can be constructed based on site labels. In principle, anyone, including users themselves, can construct lists of disapproved (or approved) sites.[60]

75. To complete the system, ICRA this year will launch a filter which will allow end-users to set their own controls, for example to ensure that access to sites on their own selected blacklists is blocked.[61]

V. CRITICISMS OF THE ABOVE APPROACHES

76. Each of the responses to Internet-based racist speech documented above has been the subject of criticism. For present purposes, it is convenient to divide these responses into the two main categories described at the outset. In the first category are attempts to combat racist sites by either eliminating the content or preventing access to the site at the ISP level. Prosecutions of content creators and hosting providers, as well as the use of proxy servers and the use of hotlines, fall into this category. The second category of responses focuses on the end-user. They include the development and use of filtering software, and the development of content rating systems (as noted, often in conjunction with such filtering software).

A. Challenging the content creator and the host provider

77. As noted, in various countries it is possible to prosecute or fine the creators of racist Web sites. However, the most substantial problem here is that the creator of content must actually be within the law enforcement reach of the prosecuting jurisdiction. For example, Mr. Toben, an Australian citizen and resident, was only arrested by the German authorities when he was visiting Germany. A country that prohibits certain racist speech will obviously not be able to bring within its jurisdiction for the purposes of prosecution a national and resident of another country who creates and posts on ISPs in his country racist content not prohibited there. Of course, the possibility of extradition remains, but only where the countries involved have similar laws prohibiting racist content.[62]

78. The use of proxy servers is also problematic. One quite basic difficulty, one shared with end-user filtering methods as well, arises from the fact that proxy servers typically work by possessing lists of URLs of Web sites to which they will not grant access because the content at the sites is harmful or illegal. The difficulty is that it is very easy for content providers simply to shift their Web sites to different addresses. Moreover, new sites appear on the Internet at an estimated rate of 40,000 per day.[63] Thus, the "blacklists" that the proxy servers employ to "screen out" racist and other harmful content are virtually guaranteed to be under-inclusive.

79. The hotline approach, targeting the offending Web site and its hosting ISP, is also quite limited, for reasons already described. First, the creator of racist content who lives outside the jurisdiction, and the hosting ISP, should it be located outside the jurisdiction, are outside the reach of the hotline. Second, in the event that the hosting ISP is within the jurisdiction, a hotline's success in inducing it to block access to the problematic site may not solve the problem of users accessing the content: as before, the content creator may simply remove his site to another ISP, with the result that his content is available within the hotline's jurisdiction once again. No doubt hotlines will meet with some success in their efforts; it cannot be expected, however, that they will eliminate the accessibility of racist content from their jurisdictions.

B. End-user approaches

80. Some countries attempt to induce end-users to refrain from accessing racist and other materials by criminalizing such access. However, the end-user has at his disposal a number of devices to shield his Internet activities. By use of such Web sites as Anonymizer, he can request access to a web page while maintaining his anonymity. Such a user will be able to gain access to prohibited sites, but his identity will be concealed from those monitoring his activities.[64] In addition, the end-user may request web pages as email attachments (a number of different online services provide for this); in this way, the end-user never actually visits the site and will again evade those monitoring improper site visits.

81. End-user filtering techniques are subject to difficulties of their own. Those that function by blocking selected files containing URL names preselected by the user or manufacturer will tend to be under-inclusive because they simply cannot keep up with the rapidly expanding number of new Web sites coming into existence daily. And, as already explained, Web site creators are able to switch their site addresses once the sites have been "blacklisted".

82. Filtering systems that function by means of keyword searches can also be under-inclusive. But, it should be pointed out that they can be over-inclusive as well. On the one hand, web creators can fairly easily avoid the use of keywords employed by the filters, by using synonyms, strategic misspellings, innuendo and so on. On the other hand, many keywords are as likely to show up in innocent contexts as in problematic ones. In one well-known example, the word "breast" was employed as a keyword in a filtering program designed to block access to sites containing pornographic material. In addition to blocking access to some such sites, however, the program blocked access to sites dealing with breast cancer, and even sites containing recipes for chicken breasts.

83. Perhaps more fundamentally, many filtering products can simply be disabled. Peacefire, for example, makes available at its Web site a free program that disables filtering products like *CyberPatrol*, *Net Nanny* and *CyberSitter* with a flick of a button. Moreover, while this program does not work with ISP-level blocking devices such as AOL Parental Controls, Peacefire provides information about how to "get around" such filtering efforts by these ISPs.

84. One last problem with filtering programs that deserves mention is that they tend to be exclusively text-based. As such, they will not identify the problematic material they are designed to find when the material is, as it increasingly tends to be, in audio or visual form.

85. Finally, content-labelling systems, like that proposed by ICRA, also have their flaws. In the first place, they depend to some degree on the voluntary rating of content by the content creator. It is to be expected that many creators of racist material will simply refuse to rate their material; others will agree to rate it, but will not do so honestly.[65] In addition, despite the attempts by ICRA and others to produce a truly "objective" rating system, it has been suggested by many commentators that there is an inescapable subjective and cultural component to the rating of any content, and thus that any such rating system is subject to inconsistency.[66]

C. Free speech concerns

86. Each of the responses to Internet-based racism described in this report has been criticized by a wide variety of NGOs and other private organizations on the basis that it interferes with free speech protections contained in national laws and constitutions, as well as in international instruments. Some groups, like the American Civil Liberties Union and the Center for Democracy and Technology, have argued that racist speech itself should be protected, as long as it does not incite to violence, and thus that efforts to eliminate such speech from the Internet are misguided. Even if, however, it is believed that such content may be eliminated without violating free speech principles, many have criticized the particular methods employed to eliminate such speech. Filtering programs, as noted, may be over-inclusive, and may thus block access to content that falls within free speech protections. Hotline operations are subject to the individual judgements of the hotline operators, judgements that may not necessarily be informed by free speech concerns in the first instance. And content labelling systems, especially those developed by industry or other private entities, may not have the degree of democratic input that would strike the appropriate balance between free speech interests and the interests of minimizing harm.[67]

VI. COMBATING INTERNET-BASED RACIST SPEECH THROUGH EDUCATION AND OUTREACH

87. In view of the shortcomings just detailed, many commentators have concluded that education about racist content on the Internet, about how it is mistaken, and about how to foster tolerance, is the single most effective way of combating Internet-based racism. A great many organizations are involved in such educational efforts.

A. International efforts

88. Many different international organizations maintain extensive information online about racism and efforts to combat it.

89. Some prominent examples are: OHCHR, which has published on its Web site information about the seminars mentioned above, dealing in part specifically with problems posed by Internet-based racist speech.[68] The UNESCO Web site contains reports and discussions on the general question of content regulation on the Internet, including the problematic occurrence of racist content.[69] The Web site of the European Commission against Racism and Intolerance (ECRI) contains various documents concerning Internet racist content, including reports made to the European Conference against Racism (2000), relevant international legal instruments concerning racism, and country-by-country breakdowns of anti-racist legislation and initiatives.[70] The ILO Web site contains reports on many aspects of racism and discrimination in work settings.[71]

B. Efforts by other organizations

90. Interesting efforts by private organizations in this area include the following.

91. The Southern Poverty Law Center in the United States is about to launch its “tolerance” Web site.[72] The site contains news about racist episodes and about efforts by individuals and groups to combat racism and intolerance. There are sites for children, with stories and a site where children can submit their own artwork and stories about tolerance for display. There are also sites for guiding parents and teachers in ways to help their children to navigate the children’s site. Elsewhere on the site, the Center has provided thumbnail sketches of some American-based hate sites. Visitors can click on certain highlighted areas in the sketches; “truth balloons” appear which debunk the myths and misrepresentations that occur at the hate sites. In addition, the main site contains links to pages containing interactive maps of hate groups in the United States, and of human rights groups (with links to the home pages of such groups).

92. Chichester University in the United Kingdom has created and operates a Web site for children and youth.[73] The visitor to the site is invited to provide information about him- or herself, including age, race and religion. The site introduces the visitor to other children of about the same age, who describe their own lives and cultures, including problems they have faced involving racism. In addition to the games, the site contains statistics and other information relevant to the occurrence of and the fight against racism; and it contains links to other public service and information sites.

93. The Media Awareness Network (Mnet) is a Canadian not-for-profit organization that, among other things, operates an educational Web site called the Web Awareness Canada site.[74] This site provides information and interactive activities for parents, teachers, librarians and students (age 9 to18) designed to help young persons learn how to use the Internet wisely and safely. The information on the site focuses on online marketing efforts directed at children, safety issues and how to deal with offensive, including racist, content. One animated computer game that students can access at the site, for example, is specifically designed to help young persons to "detect bias and harmful stereotyping in online content".

94. The Movement against Racism and for Friendship amongst Peoples) operates a Web site that contains information-testing games for adults and children on important persons and events in the fight against racism.[75] It also contains articles and information about legislation, reform efforts and significant legal cases involving racist issues.[76]

VII. CONCLUSION

95. This report has summarized various approaches for combating the use of the Internet for purposes of incitement to racial hatred, racist propaganda and xenophobia, including the principal initiatives taken to date to promote international cooperation. The approaches described include measures taken at the international and national levels, as well as initiatives undertaken by industry, private organizations and individuals. Some of these measures are of a legal character, while many are of a non-legal nature.

96. Most initiatives of a legal character have taken place at the national level, either through court cases, the adoption of new legislation or the amendment of existing legislation. However, there have been only a small number of court cases to date: most have been decided only in the past two or three years and some are still subject to appeal. Similarly, national legislation specifically drafted to address Internet content is also in an initial stage of application. Questions of jurisdiction, the technical feasibility of regulation, and differing legal standards from one State to another will continue to strongly influence the effectiveness of legal approaches to Internet-based racism.

97. Although industry, private organizations and individuals have taken various steps to address racist content on the Internet, this report has indicated that there are questions concerning the methodology of some of these approaches as well as limitations with respect to their effectiveness.

98. At the international level, it is encouraging to note that a significant number of initiatives have taken place to date and that international meetings on this subject are occurring with a certain degree of regularity. However, these efforts also appear to be in an initial phase and it is difficult at this time to draw conclusions about the effectiveness of the few concrete measures that have been adopted.

99. In conclusion, approaches to combating Internet-based racism are in a state of flux. As States, industry, private organizations and individuals gain experience and perspective in dealing with this issue, it is likely there will be a considerable evolution in their approaches in the coming years. As these approaches develop, however, it is worth bearing in mind what many

commentators have noted: the Internet itself has enormous potential for educational purposes. This potential has already been tapped to address racism: as this report has indicated, there exist at present a number of Web sites aimed at combating racism, racial discrimination, xenophobia and related intolerance. It is likely that there will be further development of such educational sites in the future.

Notes

[1] See ITU Telecommunication Indicators Update, available at www.itu.int

[2] Ibid.

[3] See Global Internet Statistics, available at www.glreach.com/globstats/index.php3

[4] Ibid.

[5] The typical end-user initially dials into a computer, called an access provider, that serves as a gateway into the rest of the Internet system.

[6] An Internet service provider (ISP) provides access to the Internet for its customers. In addition to providing such access, it may also provide space for the posting of (i.e., it may "host") content, often in the form of web pages. Generally, but not always, access providers, such as America Online, both serve as gateways for their customers to access the Internet and as hosts for content provided by their customers.

[7] See *Poisoning the Web: Hatred Online*, Report of the Anti-Defamation League (1999), available at www.adl.org.

[8] See www.wiesenthal.org.

[9] The majority of racist sites do physically reside on United States soil. For example, Otto Schily, the Minister of the Interior of Germany, recently estimated that about 90 per cent of neo-Nazi materials posted on the Internet by German citizens exist on ISPs in the United States. See "Neo-Nazi web sites moving to U.S.", at www.steptoe.com

[10] Interim court order, 22 May 2000 (interim order), p. 2 (French language version and English translation available at www.juriscom.net).

[11] As mentioned, the court's order was provisional. The court continued the proceedings for two months to enable Yahoo to present the measures it intended to take to prevent access to the site by persons located in France.

An expert's report submitted to the court in the interim concluded that approximately 30 per cent of the IP addresses "assigned to French surfers can[not] be matched with certainty to a service provider located in France" (Interim order of 20 November 2000, No. RG: 00/05308, p. 8; available at www.legalis.net; English translation available at www.cdt.org). The panel

(less one dissenter) explained that these persons could not be identified by Yahoo as being located in France at the time they would visit the auction site. However, the report concluded that Yahoo could institute a policy of requiring any such "anonymous" visitor to make a sworn declaration of nationality as a condition of entering the site. In this way, Yahoo could be apprised of every person attempting to connect to the auction site from France. Finally, the experts concluded that Yahoo could institute filtering methods that would assure that, generally, French visitors would not be able to view, or purchase, the offending Nazi material from the auction site.

The court accepted these findings and concluded that Yahoo was in fact able to comply with the 22 May 2000 order. It therefore ordered Yahoo to block access by Internet users located in France to the auction site; and instituted a fine of 100,000 francs per day until Yahoo complied with the order.

This dispute is ongoing. Yahoo has filed suit in California, requesting a United States federal court to declare that the order of the French court is neither recognizable nor enforceable in the United States, in part because the French court's order violates Yahoo's free speech rights under the United States Constitution, and in part because the expert report was mistaken in concluding that compliance with the French court's order was technically possible. See "Complaint for declaratory relief" in *Yahoo! Inc. v. La Ligue Contre le Racism et L'Antisemitisme, et al.*, Case No. C00-21275PVTADR, filed in the Northern District of California, San José Division, on 21 December 2000.

[12] See Amy Knoll, "Any which way but loose: nations regulate the Internet", 4 *Tulane Journal of International and Comparative Law* 275, pp. 287-88 (1996).

[13] Ibid., p. 288.

[14] See "Combating extremism in cyberspace", Report by the Anti-Defamation League (2000) (ADL Report), available at www.adl.org.

[15] See ADL Report, pp. 21-22.

[16] See Court Judgment, English translation available at www.cyber-rights.org.

[17] See "German hate law: no denying it", available at www.wired.com.

[18] See ABA Annual Report 1999-2000, available at www.aba.gov.au/about/information/an99-00/chapter_3.htm.

[19] Bills Digest 179 1998-99, available at www.aph.gov.au/library/pubs/bd/1998-99/99bd179.htm.

The approach just described is similar to the hotline approach described below. A significant difference between the two approaches, however, is that the latter is a voluntary

system, sometimes involving governmental cooperation and sometimes not. Recommendations by such hotlines typically are not binding on the ISPs involved; orders by the ABA in Australia, by contrast, are binding.

[20] B'nai B'rith Anti-Defamation Commission Breakfast Keynote Address, available at www.law.gov.au/ministers/attorney-general/articles/censorship.html.

[21] See "Australian publisher ordered to remove 'racist' material", available at www.newsbytes.com.

[22] See "Legal test on Holocaust Internet site" at www.theage.com.au/news/20001110/A38273-2000Nov9.html.

[23] See English translation of Act, available at www.dsv.su.se/jpalme/society/swedish-bbs-act.html.

[24] See "Hate on the Internet", by Karen R. Mock, in *Human Rights and the Internet* (2000).

[25] See *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

[26] Ibid., p. 877.

[27] Ibid., p. 885. In its decision, the Court acknowledged that it has permitted relatively more government regulation in the context of broadcast media like radio and television than it has in the case of other media, such as print media, because of the relatively "invasive" nature of the former. However, the Court characterized the Internet as "not as 'invasive' as radio or television", (for example, unlike in the case of radio or television, an Internet user is not likely merely to "happen" upon objectionable content by accident), and it thus declined to employ its broadcast media precedents to control its analysis. Ibid., p. 867.

The Court left intact section 230 of the Act, which states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". This section protects ISPs that carry, but do not create or host, illegal content, from liability.

[28] See *R.A.V. v. City of St. Paul*, 505 United States 377 (1992). There are exceptions: racist speech intended to provoke, and with a high probability of provoking, violence, for example, is not protected.

[29] See Singapore Broadcasting Authority (Class License) Notification 1996 (in chapter 297 of the Singapore Broadcasting Authority Act), available at www.sba.gov.sg.

[30] See Ari Staiman, "Shielding Internet users from undesirable content: the advantages of a PICS based rating system", 20 *Fordham International Law Journal* 866 (1977) ("Shielding users").

[31] See A. Lin Neumann, "The Great Firewall" (translating these regulations at n.2), available at www.cpj.org/Briefings/2001/China_jan01/China_jan01.html.

[32] Ibid.

[33] "Shielding users", p. 901.

[34] See "Bulgarian Government tries to control Internet access", at www.fitug.de/debate/9910/msg00003.html.

[35] Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999, available at http://158.169.50.95:10080/iap/decision.

[36] Some of these hotlines are described below.

[37] INCORE (Internet Content Rating for Europe), a group of European organizations, was recently funded by the European Commission, under the auspices of the Action Plan, to develop such a generic rating and filtering system for European users. INCORE issued its final report on this work in June 2000. The report is available at www.incore.org.

[38] See also *General Conclusions of the European Conference Against Racism* (2000), available at www.ecri.coe.int.

[39] See E/CN.4/1998/77/Add.2, 6 January 1998.

[40] See A/CONF.189/PC.1/8, 26 April 2000.

[41] Agenda, summary record and proceedings available at www.oecd.org.

[42] Some details available at www.stiftung.bertelsmann.de.

[43] Details available at www.stockholmforum.gov.se.

[44] See www.isoc.org.

[45] Netherlands laws potentially applicable to Internet-based racism include the Constitution of the Netherlands, article 1, prohibiting "discrimination on the ground of … race", and various criminal statutes.

[46] See "Fighting on-line racism, anti-Semitism and revisionism - The Complaints Bureau for Discrimination on the Internet in the Netherlands", by Ronald Eissens, Director of MDI, in *The Stockholm International Forum Combating Intolerance* (29-30 January 2001), Plenary and Seminar speaker's abstracts.

[47] See "British ISPs crack down on hate", available at www.wired.com.

[48] See www.inhope.org.

Finally, note should be taken of the CyberTipline, a United States-based hotline, launched by the National Center for Missing and Exploited Children in 1998. The mission of this hotline is to assist in the location of missing children and to field complaints about possible child exploitation. The hotline takes "tips", analyses them and passes them on to law enforcement officials when appropriate. While it does not handle complaints about racist content, its existence is significant for the fight against Internet-based racism simply because it represents the advent of the hotline strategy in the United States, which is the home of the greatest number of end-users and also the home of many of the racist Web sites on the Internet. Groups in the United States may well expand the CyberTipline strategy in the future to problematic racist content.

[49] See www.euroispa.org.

[50] See 1998 Standards and Practices, available at www.afa-france.com/html/accueil/mend2.htm.

[51] See www.telesa.or.jp/e_guide/e_guid01.html.

[52] See Code, available at www.iia.net.au.

[53] See Code of Conduct, available at www.caip.ca.

[54] See ADL Report.

[55] Ibid.

[56] See www.icra.org.

[57] See "ICRA launches new system to make the Internet safer for children", available at http://biz.yahoo.com/bw/001213/internet_c.html.

[58] See www.w3c.org.

[59] While the ICRA system itself contemplates self-rating by content creators, other parties that may be interested in the content at sites - from religious groups to groups fighting child pornography to anti-racist organizations - may employ PICS to rate sites based on the ICRA categories. By employing lists prepared by parties with interests in common with their own, end-users will not be completely dependent on self-labelling by content creators for determining which sites are desirable for them and which are not.

[60] Lists are being prepared by various groups. To take just one example, a whitelist of "family friendly" sites ("CyberMoms-Approved sites") is available at www.getnetwise.org. One criterion employed to determine if a site should be on this list is whether there is any evidence of bigotry or racism on it.

[61] The ICRA system gained momentum when it was presented at the Internet Content Summit, hosted and funded by the Bertelsmann Foundation, in cooperation with INCORE, in Munich in September 1999. At that Summit, the Foundation released a Memorandum, drafted by an expert panel including law school professors and international law enforcement and government officials, which recommended the establishment of "an improved architecture for the rating and filtering of Internet content" on a global basis, along the lines of the ICRA system. See "AOL, others plan global Net content rating system", available at http://news.cnet.com.

Other recommendations of the Memorandum include the further development of voluntary codes of conduct by ISP organizations, the further establishment of hotlines and the removal of illegal content by ISPs upon notification.

[62] Some ISPs, particularly in the United States, have refused to prohibit racist content on their servers. For example, EarthLink, a United States ISP, has taken the position that it "supports the free flow of information and ideas over the Internet" and does not "actively monitor [or] exercise control over …. the content of any Web site … created or accessible over or through EarthLink services". GTE.NET has a similar policy. See ADL Report. Both of these ISPs host Web sites with racist material or contain links to such sites. In view of the legality of most such content in the United States, persons wishing to create and post such content may do so in relative safety while within the United States.

[63] See *Regulation of the Internet: A Technological Perspective*, p. 34, available at www.strategis.ic.gc.ca.

[64] An Anonymizer-type strategy, however, is not necessarily effective for end-users who, for example, have to identify themselves in order to get on to the Internet in the first place.

[65] The ICRA terms and conditions provide that ICRA "may" monitor labelling performed by content creators for accuracy and may revoke the licence to use a label in the event that ICRA concludes that the label misrepresents the content at a site. However, there is no guarantee, and there cannot be (in the light of the sheer number of Web sites), that ICRA will check every labelled site for label accuracy.

[66] This problem is mitigated to some degree by the fact that the end-user himself has ultimate control over the lists he employs to block access to sites; presumably, he will construct or accept lists containing sites he personally finds objectionable. Nevertheless, the typical end-user simply cannot independently visit each of the sites on these lists to determine if the content there is accurately reflected, in his judgement, by the content label generated by the labelling system. Thus, the end-user is still, to some degree, subject to the content rating of content creators and of third parties - sources that may be making quite subjective and potentially inconsistent (from the end-user's point of view) rating judgements.

[67] See OHCHR report on its 1997 seminar referred to below, for discussion of many of the criticisms outlined in this section.

[68] See www.unhchr.ch.

[69] See www.unesco.org.

[70] See www.ecri.coe.int.

[71] See www.ilo.org.

[72] The site, which may be in operation by the time of the publication of this report, will be located at www.tolerance.org.

[73] See www.britkid.org.

[74] See www.media-awareness.ca.

[75] See www.mrap.asso.fr.

[76] Other prominent sites include the one operated by the Simon Wiesenthal Center at www.wiesenthal.org and the one operated by the Anti-Defamation League ("ADL") at www.adl.org. The Wiesenthal Center, in addition to lobbying ISPs not to host or to provide access to racist sites, also monitors racist Web sites and publishes a list of such sites on its Web site. This Web site also contains an interactive multimedia centre, virtual exhibits in its Museum of Tolerance, and teacher's resources, all centering on Holocaust themes. The ADL Web site contains, among many other things, reports on aspects of Internet-based racism (including the two ADL reports cited below), as well as a hate symbols database and materials on the Holocaust.
