

GOVERNING RACIST CONTENT ON THE INTERNET: NATIONAL AND INTERNATIONAL RESPONSES

Dr. Yaman Akdeniz*

INTRODUCTION

Racism and the dissemination of ideas based on racial superiority or hatred was a pressing social problem long before the emergence of the digital age. The advancement of communication technologies such as the Internet has, however, added a new dimension to this pressing problem by providing individuals and organizations “with modern and powerful means to support racism and xenophobia”.¹ Long before the Internet entered our homes, racist groups made use of other communication tools including the telephone networks from as far back as the 1970s. For example, the Western Guard Party, a white-supremacist Neo-Nazi group based in Toronto, Canada, had a telephone answering machine which was used to propagate hatred,² and was the subject matter of a long legal dispute.³

Concerns about “digital hate” date back to the mid-1980s along with the documented use of computers, computer bulletin boards and networks to disseminate racist views and content.⁴ New methods of dissemination of anti-Semitic and

* Senior lecturer at the School of Law, University of Leeds. He is also the director of the LL.M. in CyberLaw programme, and the co-ordinator of the CyberLaw Research Unit. His forthcoming publications include *Internet Child Pornography and the Law: National and International Responses* (London: Ashgate) [forthcoming in 2007]. For further information about his work see <<http://www.cyber-rights.org/yamancv.htm>>. He would like to thank Dr. Louise Ellison, School of Law at the University of Leeds for her invaluable comments and assistance with this article. An earlier, shorter version of this article was published as a background report for the High Level Seminar on Racism and the Internet, presented to the Intergovernmental Working Group on the Effective Implementation of the Durban Declaration and Programme of Action in 2006, UN Doc. E/CN.4/2006/WG.21/BP.1, online: <http://www.cyber-rights.org/reports/ya_un_paper_int_06.pdf>.

¹ Council of Europe, Committee of Ministers, *Explanatory Report of the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, (2002) at para. 3, online: Council of Europe <<http://conventions.coe.int/Treaty/en/Reports/Html/189.htm>>.

² Canadian Human Rights Commission, *Hate on the Net* (Ottawa: Association for Canadian Studies, Spring 2006) at 4, online: Canadian Human Rights Commission <http://www.chrc-ccdp.ca/pdf/hateoninternet_bil.pdf>.

³ *Canada (Human Rights Commission) v. Taylor*, [1990] 3 S.C.R. 892 [*Taylor*] (Prohibition on telephone hate messages in section 13(1) of the *Canadian Human Rights Act*, S.C. 1976-77, c. 33 was justifiable). See also *Canada (Human Rights Commission) v. Canadian Liberty Net*, [1998] 1 S.C.R. 626 [*Liberty Net*] and *Canada (Human Rights Commission) v. Heritage Front*, [1994] F.C.J. No. 2010 (T.D.) (QL).

⁴ See “Neo-Nazis’ Inspire White Supremacists” *The Washington Post* (26 December 1984) (dissemination of racist comments through computer bulletin boards in North America). See also Anti-Defamation League, *Computerized Networks of Hate* (January 1985).

revisionist propaganda about the Holocaust (including video games, computer programs and the Minitel system in France) were noted by a United Nations (UN) Secretary-General report in 1994,⁵ and the growing use of modern electronic media in international communications between right-wing radical groups (computer disks, databanks, etc.) was recorded in 1995.⁶ But officially the use of electronic mail and the Internet was first observed as a growing trend amongst racist organizations to spread racist or xenophobic propaganda in 1996.⁷ The United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, in his 1997 report declared that:

The Internet has become the new battleground in the fight to influence public opinion. While it is still far behind newspapers, magazines, radio and television in the size of its audience, the Internet has already captured the imagination of people with a message, including purveyors of hate, racists and anti-Semites.⁸

It was predicted that the dissemination of racist content would increase with the rapid growth of Internet use around the globe. Easy and inexpensive access to the Internet, as well as the development of the World Wide Web, provided new and ready opportunities for publishing and this extended to material of a racist nature.⁹ Flyers and pamphlets that had traditionally been distributed locally by hand and had limited visibility could now be distributed and accessed globally through the Internet. The “slow, insidious effect of a relatively isolated bigoted commentary...has now changed to a form of communication having a widespread circulation.”¹⁰ In time, this type of content would be presented in more attractive

⁵ Secretary-General, *Elimination Of Racism And Racial Discrimination*, UN GA, 49th Sess., UN Doc. A/49/677 (1994).

⁶ Maurice Glélé-Ahanhanzo, *Implementation Of The Programme Of Action For The Second Decade To Combat Racism And Racial Discrimination - Report of the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, CHR Res. 1994/64, UN ESCOR, 51st Sess., UN Doc. E/CN.4/1995/78 (1995).

⁷ Secretary-General, *Elimination Of Racism And Racial Discrimination: Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, UN GA, 51st Sess., UN Doc. A/51/301 (1996).

⁸ Maurice Glélé-Ahanhanzo, *Implementation Of The Programme Of Action For The Second Decade To Combat Racism And Racial Discrimination - Report of the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, CHR Res. 1996/21, UN ESCOR, 53d Sess., UN Doc. E/CN.4/1997/71 (1997).

⁹ See generally Kenneth S. Stern, *Hate and the Internet* (2004), online: American Jewish Committee <<http://www.ajc.org/site/apps/nl/content3.asp?c=ijITI2PHKoG&b=846637&ct=1363047>>.

¹⁰ *Warman v. Harrison*, 2006 CHRT 30 at para. 46. See further *Liberty Net*, *supra* note 3.

high quality formats including that of online racist videos,¹¹ games¹² and cartoons; as well as music,¹³ radio, and audio-visual transmissions.

The use of the Internet as an instrument for the widespread dissemination of racist content can be traced to the mid-1990s. The Simon Wiesenthal Center identified a single website in 1995,¹⁴ and approximately 70 websites disseminating racist content in 1996.¹⁵ Ten years later, it has been estimated that there are more than 5,000 websites in a variety of languages which promote racial hatred, anti-Semitism, violence and xenophobia around the world.¹⁶ A 2005 study by the Simon Wiesenthal Center entitled *Digital Terrorism & Hate 2005* reported a 25% increase in such websites compared to 2004 which indicated that the problem of racism and xenophobia was growing over the Internet.¹⁷ A similar estimate was made by Gabriel Weimann, whose research revealed more than 4,300 websites related to terrorist organizations and purposes in 2004.¹⁸ The estimated number of websites which promote racial hatred and violence reached over 6,000 in May 2006 according to the *Digital Terrorism & Hate 2006* report.¹⁹

¹¹ See e.g. "Videos of hate flout curbs on Islamists" *The [London] Sunday Times* (16 July 2006). The story covers the hate videos published on the website of Ahlus Sunnah wal Jamaah (ASWJ), a splinter of Al-Muhajiroun.

¹² For example, the racist game *ZOG's Nightmare*, in which ethnical cleansing is the main theme, was released by the U.S. National Socialist Movement in June 2006. A considerable number of such games were documented in the Simon Wiesenthal Center report *Digital Terrorism & Hate 2006* which is available online at <<http://www.wiesenthal.com/>>.

¹³ Note that more than 600 CDs containing racist music are available for purchase through the U.S. National Socialist Movement's website: <<http://nsm88records.com/>>.

¹⁴ Secretary-General, The fight against racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, UN GA, 59th Sess., UN Doc. A/59/329 (2004) at para. 29.

¹⁵ Secretary-General, *supra* note 7 at para. 45.

¹⁶ "Digital Terrorism & Hate 2005 Report Shows 25 Per Cent Increase In Hate Sites" *Canada NewsWire* (7 October 2005).

¹⁷ See also International Network Against Cyber Hate, *Hate on the Net: Virtual Nursery for In Real Life Crime* (June 2004), online: <<http://www.inach.net/content/inach-hateonthenet.pdf>>.

¹⁸ Gabriel Weimann, *www.terror.net: How Modern Terrorism Uses the Internet* (March 2004), online: United States Institute of Peace <<http://www.usip.org/pubs/specialreports/sr116.pdf>>; Gabriel Weimann, "Terrorists and Their Tools: Using the Internet" *YaleGlobal* (26 April 2004), online: YaleGlobal <<http://yaleglobal.yale.edu/display.article?id=3768>>. See further Clive Walker, "Cyber-Terrorism: Legal Principle and Law in the United Kingdom" (2006) 110 Penn St. L. Rev. 625.

¹⁹ Simon Wiesenthal Center, *supra* note 12.

These types of websites are largely used for propaganda, disseminating hatred,²⁰ recruitment,²¹ training,²² fundraising,²³ and for communication purposes.²⁴ In terms of content and typology, racist websites on the Internet could be categorized into transnational hate, religious hatred, and those denying historical events such as the Holocaust.²⁵ Some of them are regionally based, for instance the Nazi supremacy and skinhead pages in the United States; and the extreme nationalistic, anti-immigrant and anti-Semitic web pages based in Europe.²⁶ There is a greater

²⁰ See the study conducted by Jack Glaser *et al.*, "Studying Hate Crime with the Internet: What Makes Racists Advocate Racial Violence?" (2002) 58(1) *Journal of Social Issues* 177.

²¹ Hilary Hylton, "How Hizballah Hijacks the Internet" *Time Magazine* (8 August 2006), online: Time.com <<http://www.time.com/time/world/article/0,8599,1224273,00.html>>.

²² Publications such as *Mujahideen Explosive Handbook* and the *Encyclopaedia of the Afghan Jihad* are examples of some of the publications disseminated and distributed through the Internet. See also "Terror law vague, accused to argue" *The Globe and Mail* (30 August 2006); "Abu Hamza trial: Islamic cleric had terror handbook, court told" *The Guardian* (12 January 2006).

²³ The European Union for example is concerned about the use of the Internet by terrorist organizations for recruitment purposes. See EC, Commission, *Communication from the European Commission to the European Parliament and the Council concerning Terrorist recruitment: addressing the factors contributing to violent radicalisation* (Brussels EC, 2005) COM(2005) 313 final. Note also the largely classified *EU Presidency note on Preventing Radicalisation and Recruitment to Terrorist Groups* (July 2005) 10916/05 classified RESTREINT UE, which sets out in detail possible measures to be taken, at both the national and EU levels, in order to prevent radicalisation and recruitment to terrorist groups, taking into account structural, motivational and logistical factors. The EU Presidency note focuses on countering the methods, propaganda and conditions through which people are drawn into terrorism. It also contains suggestions for operating procedures with a view to preventing, spotting and disrupting possible causes of radicalisation and social instability as raising factors to terrorism, and aims at promoting the development of best practices for a successfully coordinated community approach in this field.

²⁴ In July 2006, U.S. authorities arrested three suspects accused of plotting to damage transit tunnels under New York's Hudson River. The plot was broken up in the early planning stages when the FBI, through routine monitoring of Islamic terrorist recruiting websites, discovered suspicious e-mail and chat-room postings. See "Foiled plots" *The Globe and Mail* (11 August 2006). Note also that the 17 terror suspects arrested and charged in June 2006 under s. 83 of the Canadian *Criminal Code* in relation to alleged plots in Toronto, Miami and New York City, used chat-rooms to discuss their activities. See generally "Counterterrorism's new battleground: As terrorism investigators stalk the Internet, they tread a fine line between overreacting to 'jihadi bravado' and missing the next 9/11" *Ottawa Citizen* (13 July 2006); "Generation jihad: terror at the touch of a key; Tech-savvy terrorist groups are going on-line to spread their extremist message" *The Globe and Mail* (15 June 2006); and "Plot began in chat room" *The Toronto Star* (5 June 2006).

²⁵ See generally Deborah E. Lipstadt, *Denying the Holocaust: The Growing Assault on Truth and Memory* (New York: Plume, 1994); Deborah E. Lipstadt, *History on Trial: My Day in Court with David Irving* (New York: HarperCollins World, 2005); Michael Shermer & Alex Grobman, *Denying History: Who Says the Holocaust Never Happened and Why do they Say it?* (Berkeley: University of California Press, 2002); Richard J. Evans, *Lying About Hitler: History, Holocaust and the David Irving Trial* (New York: Basic Books, 2001).

²⁶ An assessment of the nature of hate on the Internet was also made in 2003 by Phyllis B. Gerstenfeld *et al.*, "Hate Online: A Content Analysis of Extremist Internet Sites" (2003) 3(1) *Analyses of Social Issues & Public Policy* 29.

concern for the resurgence of Nazi ideology within the Council of Europe region²⁷ and there are several neo-Nazi websites associated with that movement. There is also a growing number of radical Islamic websites under the umbrella of E-jihad²⁸ in the post-September 11th world, “particularly in relation to the conflict in Palestine and Israel.”²⁹ A considerable number of websites still disseminate anti-Semitic materials³⁰ including the fraudulent document known as the *Protocols of the Elders of Zion*³¹ “which purports to be the actual blueprint by Jewish leaders to take over the world.”³² Although several other controversial publications of a racist nature or that encourage violence³³ are available over the Internet, none are as widely available as this anti-Semitic forgery which “refuses to die”.³⁴ The *Protocols of the Elders of Zion* was first published in Russia in 1905 and is available through a number of websites including Hamas Online (website of the Palestinian Sunni Islamist militant organization) and is still a bestseller in print format in many Muslim countries, including Turkey.³⁵

²⁷ See Council of Europe, P.A., 2006 Ordinary Sess. (Second Part) *Combating the resurgence of Nazi ideology*, Texts Adopted, Res. 1495 (2006) online: CoE <<http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta06/ERES1495.htm>>. Paragraph 14 of the Resolution states that the Assembly “believes that it is urgent to step up co-ordinated action in order to resist efforts aiming at revitalising Nazi ideology, to fight xenophobia, intolerance and hatred based on racial and ethnic grounds, political and religious extremism, and all forms of totalitarian action. The Council of Europe must play a leading role in this process”. See further Council of Europe, P.A., *Combating the resurgence of nazi ideology*, Documents, Doc. 10766 (19 December 2005), online: CoE <<http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc05/EDOC10766.htm>>.

²⁸ See generally Hanna Rogan, “Jihadism Online - A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes” Norwegian Defence Research Establishment, FFI/REPORT-2006/00915, online: FFI <<http://rapporteur.ffi.no/rapporteur/2006/00915.pdf>>; and Hanna Rogan, “The London Bombings.Com: An Analysis of Jihadist Website Discussion about the Attacks”, Norwegian Defence Research Establishment, FFI/NOTAT-2005/02970, online: FFI <http://www.mil.no/multimedia/archive/00066/Rogan-N-2005-02970_66657a.pdf>.

²⁹ Gary R. Bunt, *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments* (London: Pluto Press, 2003) at 25-26.

³⁰ See U.K., Parliamentary Committee Against Antisemitism, *Report of the All-Party Parliamentary Inquiry into Antisemitism*, (London: The Stationery Office Limited, 2006), online: <<http://thepcaa.org/Report.pdf>>.

³¹ Sergius Nilus, *The Protocols of the Meetings of the Learned Elders of Zion With Preface and Explanatory Notes* (Honolulu: University Press of the Pacific, 2003).

³² Will Eisner, *The Plot: The Secret Story of the Protocols of the Elders of Zion* (New York: W.W. Norton & Company, 2005). See further Norman Cohn, *Warrant for Genocide: The Myth of the Jewish World Conspiracy and the Protocols of the Elders of Zion* (Serif Publishing, 2005); and Hadassa Ben-Itto, *The Lie That Wouldn't Die: The Protocols of the Elders of Zion* (Mitchell Vallentine & Company, 2005).

³³ See for example Andrew MacDonald, *The Turner Diaries: A Novel* (Fort Lee, N.J.: Barricade Books, 1996) (which has been considered by the U.S. Justice Department and FBI as the bible of right-wing militia groups). This book is available over the Internet and is believed to have provided the blueprint for the Oklahoma City bombing.

³⁴ Edward Rothstein, “The Anti-Semitic Hoax That Refuses to Die” *The New York Times* (21 April 2006).

³⁵ Phillip Adams, “Mel Gibson’s affliction seems hereditary” *The Australian* (08 August 2006).

As will be discussed in this article, these disturbing developments have naturally informed the global fight against racism. A significant number of international instruments acknowledge and attempt to address the problem of racism. The Universal Declaration of Human Rights, the International Convention on the Elimination of All Forms of Racial Discrimination (1963) (ICERD),³⁶ the International Convention on Civil and Political Rights (ICCPR),³⁷ the International Convention on Economic, Social and Cultural Rights (ICESCR),³⁸ the International Convention on the Elimination of All Forms of Discrimination against Women (CEDAW),³⁹ the International Convention on the Suppression and Punishment of the Crime of Apartheid (“Apartheid Convention”),⁴⁰ and the Convention on the Rights of the Child (CRC)⁴¹ are some of the more important international instruments to note.

In addition to the adoption of normative standards, the international community has responded to the persistence of racism since the entry into force of the ICERD, by proclaiming three consecutive Decades to Combat Racism and Racial Discrimination (1973-1983; 1983-1993; 1993-2003), and by organizing three World Conferences at the United Nations level to Combat Racism and Racial Discrimination in 1978, 1983 and 2001.

Apart from these noteworthy initiatives, the growing problem of racist content on the Internet has also prompted vigorous responses from a variety of agents, including governments, supranational and international organizations as well as from the private sector.⁴² This multi-tiered and multi-agency pluralistic approach to governing racist Internet content will be the focus of this article.

³⁶ The ICERD was adopted in 1965 and entered into force on 4 January 1969. As of 6 December 2006, the total number of Member States to this treaty reached 173, making it one of the most widely-ratified human rights treaties.

³⁷ The ICCPR was adopted in 1966 and entered into force in 1976. As of 6 December 2006, 160 States had ratified the ICCPR.

³⁸ The ICESCR was adopted in 1976 and entered into force in 1976. As of 6 December 2006, 155 States were parties to the ICESCR.

³⁹ CEDAW was adopted in 1979 and entered into force in 1981. As of 6 December 2006, its membership stood at 185 State parties.

⁴⁰ The 1973 Apartheid Convention entered into force in 1976, and as of 6 December 2006, 107 States have become party thereto.

⁴¹ The CRC was adopted in 1989 and entered into force in 1990; with 193 State parties as of 6 December 2006, it is the UN human rights instrument enjoying most universal ratification.

⁴² See *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*, UN GAOR, UN Doc. A/CONF.189/PC.2/12 (2001).

1. Identifying Key Issues

The global, decentralized and borderless nature of the Internet creates a potentially infinite and unbreakable communications complex which cannot be readily bounded by one national government or even several or many acting in concert; there is simply no unique solution for effective regulation at the national level. Harmonization efforts to combat illegal content have been protracted and are ongoing, even for universally condemned content such as child pornography.⁴³ Efforts to harmonize laws to combat racist Internet content have proved to be even more problematic. For example, while child pornography is often regarded as a clear cut example of “illegal content”, racist content has been much more difficult to categorize.⁴⁴ Content regarded by some as harmful or offensive is not always considered illegal in all States. The differing views on the limits to freedom of expression have resulted in different legal responses to racist discourse in North America (especially in the United States) and in Europe. There are also varied approaches within Europe in terms of what constitutes illegal content, with individual States having differing approaches to “harm”.⁴⁵ Unfortunately, content regarded as harmful or offensive do not fall within the boundaries of illegality in all States.

Achieving a proper balance between the desire to control racist content and to protect freedom of expression has inevitably proved challenging on the Internet. Despite an attempt at regional harmonization at the Council of Europe level with an Additional Protocol to the 2001 Convention on cybercrime,⁴⁶ there is no uniformed approach to the dissemination and availability of racist content on the Internet.

The European Commission Against Racism and Intolerance (ECRI) has noted, “the obligation incumbent upon all States to prevent and prohibit discrimination on the basis of race is enshrined in articles 55(c) and 56 of the Charter of the United

⁴³ See Juan Miguel Petit, *Rights of the Child - Report of the UN Special Rapporteur on the sale of children, child prostitution and child pornography*, Commission on Human Rights, 61st Sess., UN Doc. E/CN.4/2005/78 (2004). See also the Addendum to this report: UN Doc. E/CN.4/2005/78/Add.3 (2005). See further Yaman Akdeniz, “Child Pornography” in Yaman Akdeniz *et al.*, eds., *The Internet, Law and Society* (Essex: Longman, 2000) at 231-249; Yaman Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (London: Ashgate) [forthcoming in 2007].

⁴⁴ Racist content is commonly portrayed in written form, but is often presented together with images, unlike child pornography which is generally presented only in image and video format.

⁴⁵ See generally Yaman Akdeniz, “Controlling Illegal and Harmful Content on the Internet” in David S. Wall, ed., *Crime and the Internet* (London: Routledge, 2001) at 113-40.

⁴⁶ *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, 28 January 2003, C.E.T.S. No: 189. See further the related *Explanatory Report*, *supra* note 1. See also Yaman Akdeniz, *An Advocacy Handbook for the Non Governmental Organizations: The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems* (Leeds: Cyber-Rights & Cyber-Liberties, 2003), online: Cyber-Rights <http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf>.

Nations and has been subsequently reiterated in numerous multilateral conventions."⁴⁷ The most significant instrument in this context is the ICERD, article 4 of which states that the signing and ratifying States agree to:

condemn all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form, and undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination and, to this end, with due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5 of this Convention, *inter alia*:

- (a) Shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof;
- (b) Shall declare illegal and prohibit organizations, and also organized and all other propaganda activities, which promote and incite racial discrimination, and shall recognize participation in such organizations or activities as an offence punishable by law;
- (c) Shall not permit public authorities or public institutions, national or local, to promote or incite racial discrimination.⁴⁸

With 173 ratifications by Member States as of this writing,⁴⁹ the ICERD provisions remain the most important normative basis upon which international efforts to eliminate racial discrimination can be built.⁵⁰ The Committee on the

⁴⁷ Council of Europe, *Report of the European Commission against Racism and Intolerance - Legal Instruments to Combat Racism on the Internet*, CRI (2000) 27 at 65, online: ECRI <http://youth-against-racism.net/files/youth/ECRI_Combat_Racism_Internet.pdf>.

⁴⁸ *International Convention on the Elimination of All Forms of Racial Discrimination*, 7 March 1966, 9464 U.N.T.S. 660, art. 4.

⁴⁹ Note that 24 States have yet to become parties to the Convention. Five States have signed but not yet ratified the Convention: Bhutan (26 March 1973), Grenada (17 December 1981), Guinea Bissau (12 September 2000), Nauru (12 November 2001) and Sao Tome and Principe (6 September 2000). Eighteen States have neither signed nor ratified the Convention: Angola, Brunei Darussalam, Cook Islands, Democratic People's Republic of Korea, Djibouti, Dominica, Kiribati, Malaysia, Marshall Islands, Federated States of Micronesia, Myanmar, Niue, Palau, Saint Kitts and Nevis, Samoa, Singapore, Tuvalu and Vanuatu. See further *Efforts by the Office of the United Nations High Commissioner for Human Rights for universal ratification of the International Convention on the Elimination of All Forms of Racial Discrimination - Note by the Secretariat*, UN ESCOR, 62 Sess., UN Doc. E/CN.4/2006/13 (2006).

⁵⁰ See *Report of the Committee on the Elimination of Racial Discrimination*, UN GAOR, 64th Sess. & 65th Sess., UN Doc. A/59/18 (2004).

Elimination of Racial Discrimination (CERD) in its General Recommendations⁵¹ explained that the provisions of article 4 are of a mandatory character. According to CERD, to satisfy these obligations, States parties need to enact appropriate legislation and ensure that such legislation is effectively enforced. CERD believes that:

the prohibition of the dissemination of all ideas based upon racial superiority or hatred is compatible with the right to freedom of opinion and expression. This right is embodied in article 19 of the Universal Declaration of Human Rights and is recalled in article 5 (d) (viii) of the International Convention on the Elimination of All Forms of Racial Discrimination. Its relevance to article 4 is noted in the article itself. The citizen's exercise of this right carries special duties and responsibilities, specified in article 29, paragraph 2, of the Universal Declaration, among which the obligation not to disseminate racist ideas is of particular importance. The Committee wishes, furthermore, to draw to the attention of States parties article 20 of the International Covenant on Civil and Political Rights, according to which any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.⁵²

Nonetheless, harmonization has not been established and there remain different interpretations as well as applications of article 4. For example, nineteen States have entered reservations and/or interpretative declarations with respect to article 4. Furthermore, a number of States have not fulfilled the requirements of article 4; most notably, the U.S. Government declared that:

the Constitution and laws of the United States contain extensive protections of individual freedom of speech, expression and association. Accordingly, the United States does not accept any obligation under this Convention, in particular under articles 4 and 7, to restrict those rights, through the adoption of legislation or any other measures, to the extent that they are protected by the Constitution and laws of the United States.⁵³

As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in his 1998 Report, "the ambivalence surrounding points related to the principle of the need to balance rights and

⁵¹ CERD, *General Rec. No. 07: Legislation to eradicate racial discrimination (Art. 4)*, UN CERD, 32d Sess., UN Doc. A/40/18 (1985); CERD, *General Rec. No. 15: Organized violence based on ethnic origin (Art. 4)*, UN CERD, 42d Sess., UN Doc. A/48/18 (1993).

⁵² *Supra* note 50.

⁵³ *Ratifications and Reservations of the International Convention on the Elimination of All Forms of Racial Discrimination New York, 7 March 1966*, online: UN High Commissioner for Human Rights <<http://www.ohchr.org/english/countries/ratification/2.htm>>.

protections is evident in the positions taken by Governments through the declarations and reservations they have entered to article 4 of the [ICERD].”⁵⁴

It could be argued that ICERD provisions are rather limited and fall short of tackling various manifestations of racism and discrimination despite the progressive interpretation of the various provisions of the instrument. Within this context the question arises, for example, as to whether there is a need for complementary international standards to combat racism on the Internet.⁵⁵ While there is an urgent need to review the functioning of ICERD and consider whether it should be updated, “great care must be taken to achieve an appropriate balance between the rights to freedom of opinion and expression and to receive and impart information and the prohibition on speech and/or activities promoting racist views and inciting violence”,⁵⁶ as noted by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in his 1998 Report. That balance has yet to be reached and agreed upon.

2. Governance of Racist Content on the Internet

Clearly, there is need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different...⁵⁷

Typically, the stance taken by governments is that what is illegal and punishable in an offline format must also be treated as illegal and punishable online. There are, however, several features of the Internet which fundamentally affect approaches to its governance. As stated above, the Internet’s decentralized nature creates barriers to effective regulation at the national level. The legal and investigative possibilities at the national level are restricted by the global, distributed and decentralized architecture of the Internet. According to the Commission on Global Governance Reforming the United Nations:

Global governance is about a varied cast of actors: people acting together in formal and informal ways, in communities and countries,

⁵⁴ Abid Hussain, *Question of the Human Rights of All Persons Subjected to any Form of Detention or Imprisonment - Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, CHR Res. 1997/26, UN ESCOR, 54th Sess., UN Doc. E/CN.4/1998/40 (1998).

⁵⁵ This issue was considered without conclusion during the Fourth session of the UN Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action in Geneva from 16 to 27 January 2006: See *Report of the Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action on its fourth session*, UN ESCOR, 62d Sess., UN Doc. E/CN.4/2006/18 (2006), online: United Nations <[http://daccessdds.un.org/doc/UNDOC/GEN/G06/119/23/PDF/G0611923.pdf](http://daccessdds.un.org/doc/UNDOC/GEN/G06/119/23/PDF/G0611923.pdf?)>.

⁵⁶ Hussain, *supra* note 54.

⁵⁷ Kofi Annan (Opening Statement at the Global Forum on Internet Governance, 24 March 2004) in Don MacLean, *Internet Governance: A Grand Collaboration* (New York: United Nations ICT Task Force, 2004).

within sectors and across them, in non-governmental bodies and citizens' movements, and both nationally and internationally, as a global civil society. And it is through people that other actors play their roles: states and governments of states, regions and alliances in formal or informal garb. But we also noted that a vital and central role in global governance falls to people coming together in the United Nations, aspiring to fulfil some of their highest goals through its potential for common action.⁵⁸

This pluralistic Internet governance approach, as it is currently emerging, may include several layers including the national (and the local), supranational (e.g. European Union) or regional (Council of Europe or OSCE) and international (United Nations). The effect of supranational/regional and international developments on nation-state governance cannot be underestimated, and the aligning of strategies and policies may be necessary to find common solutions for Internet related problems. Internet governance may comprise not only regulatory action by governments but also social norms, self-regulation (ISPs), co-regulation (Hotlines), co-operation with the ISPs (notice and takedown provisions), regulation through code and technical means (such as rating and filtering tools), as well as education and awareness campaigns. The development of international agreements and conventions may also be part of this emerging pluralistic Internet governance model.

The following sections of this article provide a critical overview of key developments at national, regional international, and international levels of Internet governance.

3. The National Approaches to Internet Governance and its Limitations

For obvious reasons, States have been keen to apply national laws to the Internet. It has become quickly apparent, however, that enforcement is problematic and the application of national laws to control the flow of information on the global Internet can often prove ineffectual due to the multi-national nature of the Internet. A number of court cases have targeted the creators of racist content, as well as those hosting it or providing access to such content, in a number of jurisdictions. The most significant of these cases will be highlighted here to illustrate the difficulties encountered at a national level when fighting racist Internet content.

(A) *Yahoo Case (France/USA)*

In May 2000, the League Against Racism and Anti-Semitism (la Ligue Contre Le Racisme et L'Antisemitisme - LICRA) and the Union of French Jewish Students (UEJF) brought an action against Yahoo! Inc. and Yahoo France. The plaintiffs alleged that Yahoo! Inc. hosted an auction website which contained for sale thousands of items of Nazi paraphernalia and that Yahoo France provided a link and access to this content through the Yahoo.com website. The French Court in its

⁵⁸ Commission on Global Governance, *Our Global Neighbourhood: Reforming the United Nations*, online: < <http://www.libertymatters.org/globalgovernance.htm>>; see especially chapter 5.

initial judgment⁵⁹ held that access by French Internet users to the auction website containing Nazi objects constituted a contravention of French law, as an offence to the “collective memory” of the country, and that the simple act of displaying such objects (e.g. exhibition of uniforms, insignia or emblems resembling those worn or displayed by the Nazis) in France constitutes a violation of the *Penal Code* and is therefore considered a threat to internal public order. On 22 May 2000 the Tribunal de grande instance de Paris ordered Yahoo! Inc. to take all necessary measures to dissuade and make impossible any access via Yahoo.com to the auction service for Nazi memorabilia as well as to any other site or service that may be construed as an apology for Nazism or contesting the reality of Nazi crimes. In November 2000, the Paris Court ordered Yahoo! Inc. to comply in three months with the injunctions contained in its order of 22 May 2000.⁶⁰

Yahoo! Inc. announced in January 2001 that it would no longer allow Nazi and Ku Klux Klan memorabilia to be displayed on its Yahoo France website and that it would take a proactive approach to the problem by implementing a monitoring or filtering system. The new policy, which also included a ban on other forms of hate material, took effect on 10 January 2001. However, Yahoo! Inc. also asked the U.S. District Court in San Jose to declare the French ruling in violation of the First Amendment⁶¹ and to rule that the French court did not have jurisdiction over content produced by a U.S. company. This was followed by LICRA filing a motion with the San Jose Court to dismiss Yahoo! Inc.’s case. LICRA’s motion was denied by the U.S. District Court for the Northern District of California in San Jose and a motion for summary judgment was granted, with the Court stating:

this case is not about the moral acceptability of promoting the symbols or propaganda of Nazism. Most would agree that such acts are profoundly offensive. By any reasonable standard of morality, the Nazis were responsible for one of the worst displays of inhumanity in recorded history. This Court is acutely mindful of the emotional pain reminders of the Nazi era cause to Holocaust survivors and deeply respectful of the motivations of the French Republic in enacting the underlying statutes and of the defendant organizations in seeking relief under those statutes. Vigilance is the key to preventing atrocities such as the Holocaust from occurring again.⁶²

The Court also questioned “whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States

⁵⁹ Trib. gr. inst. Paris, 20 November 2000, *League Against Racism and Antisemitism (LICRA), French Union of Jewish Students v. Yahoo! Inc. (USA), Yahoo France* (Interim Court Order), online: CDT <<http://www.cdt.org/speech/international/20001120yahoofrance.pdf>>.

⁶⁰ *Ibid.* See further Yaman Akdeniz, “Case Analysis of *League Against Racism and Antisemitism (LICRA), French Union of Jewish Students v. Yahoo! Inc. (USA), Yahoo France*” (2001) 1(3) *Electronic Business Law Reports* 110.

⁶¹ U.S. Const. amend. I.

⁶² *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'antisemitisme*, 169 F.Supp.2d 1181 (N.D. Cal. 2001).

resident within the United States on the basis that such speech can be accessed by Internet users in that nation.”⁶³ This was a crucial point in granting summary judgment in favour of Yahoo! However, LICRA’s subsequent appeal to the U.S. Court of Appeals for the Ninth Circuit (i.e. that the District Court did not properly exercise personal jurisdiction over the French organizations) was successful, and the Court held that Yahoo! had made no allegation which could lead a court to conclude that the conduct of LICRA and UEJF was wrongful.⁶⁴ Although the Ninth Circuit Court of Appeals granted a petition from Yahoo! for the Court to reconsider its decision,⁶⁵ before a decision was reached, an appeals court in Paris upheld a decision absolving Yahoo! from legal responsibility for the sale of Nazi paraphernalia auctioned through its website.⁶⁶ According to the French Appeals Court, Yahoo! did not seek to “justify war crimes and crimes against humanity” by allowing such sales on its site.⁶⁷

Ultimately, in January 2006, a 6-5 majority of the U.S. Court of Appeals for the Ninth Circuit dismissed Yahoo!’s case,⁶⁸ reversing a lower court ruling that had rejected the French plaintiffs’ attempts to enforce French laws against U.S. companies in U.S. courts. The U.S. Appeals Court concluded that “First Amendment issues arising out of international Internet use are new, important and difficult [and they] should not rush to decide such issues based on an inadequate, incomplete or unclear record.”⁶⁹ The Court argued that without knowing “whether further restrictions on access by French, and possibly American users are required, [it] cannot decide whether or to what degree the First Amendment might be violated by enforcement of the French court’s orders”.⁷⁰

⁶³ *Ibid.* at 1186.

⁶⁴ *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'antisemitisme*, 379 F.3d 1120 (9th Cir. 2004).

⁶⁵ *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 399 F.3d 1010 (9th Cir. 2005). See further: “Yahoo Sees Small Victory in Nazi Dispute” *Bizreport* (11 February 2005), online: Bizreport <<http://www.bizreport.com/news/8669/>>; and “Yahoo Lawyers Ask Court for Protection” *Associated Press Financial Wire* (March 28 2005).

⁶⁶ Note that Yahoo! was acquitted by a Paris criminal court in February 2003, but the Association of Auschwitz Survivors and the French Movement Against Racism (MRAP) pursued a civil action against Yahoo! as the public prosecutor declined to appeal the Court’s decision on the criminal charges. See generally: “Auschwitz survivors continue challenge of internet sale of Nazi memorabilia” *Agence France Presse* (January 19 2005); “Appeals court says former Yahoo exec not liable” *Associated Press* (April 6 2005); “French Court Says Yahoo Not Responsible For Nazi Sales” *National Journal’s Technology Daily [Washington]* (April 7 2005); and “Can the Internet Have Borders?” *The Washington Post* (April 7 2005).

⁶⁷ “Appeals court says former Yahoo exec not liable” *Associated Press* (April 6 2005).

⁶⁸ *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'antisemitisme*, 433 F.3d 1199 (9th Cir. 2006) [*Yahoo*]. See also “Court rules against Yahoo in Nazi speech case” *Reuters* (12 January 2006).

⁶⁹ *Yahoo, ibid.* at 1223.

⁷⁰ *Ibid.* at 1224.

The dissenting judgment recognized the “horrors of the Holocaust and the scourge of anti-Semitism, and France’s understandable interest in protecting *its* citizens from those who would defend or glorify either”,⁷¹ but did not question the validity of the French orders on French soil. However, in strong words, the dissenting judgment stated that the majority, after properly opening the door to the federal courthouse by upholding personal jurisdiction, nonetheless turns a blind eye to the constitutional free speech interests of Yahoo!, throwing the case out of court because those interests are “not ripe for adjudication”.⁷² According to the dissenting judgment:

[the majority’s decision] leaves in place a foreign country’s vague and overbroad judgment mandating a U.S. company to bar access to prohibited content by Internet users from that country. This astonishing result is itself the strongest argument for finding Yahoo!’s claims ripe for adjudication.⁷³

The dissenting members of the court further questioned whether it should be assumed that “U.S.-based Internet service providers are now the policing agencies for whatever content another country wants to keep from those within its territorial borders – such as, for example, controversial views on democracy, religion or the status of women?”⁷⁴ The dissent concluded by stating that U.S. courts “should not allow a foreign court order to be used as leverage to quash constitutionally protected speech by denying the United States-based target an adjudication of its constitutional rights in federal court.”⁷⁵

In May 2006, the U.S. Supreme Court decided not to consider the Yahoo! case following an appeal by the two French associations arguing that the ruling leaves the door open for Yahoo! to try to use U.S. courts to avoid judgments from courts in other countries.⁷⁶

The Yahoo! case is an example of nation-states’ desire to enforce and apply national laws to a global and multi-national medium. With the advancement of new technologies such as the Internet, cultural, moral, religious, historical and legal differences become more pronounced. While such differences are legitimate and acceptable, enforcement of such local and national standards to a company based in another country remains inherently problematic.

⁷¹ *Ibid.* at 1234 [emphasis in original]. See also EUMC working paper, *Antisemitism: Summary overview of the situation in the European Union 2001-2005* (May 2006), online EUMC <http://eumc.europa.eu/eumc/material/pub/AS/AntisemitismOverview_May.pdf>.

⁷² *Ibid.* at 1252.

⁷³ *Ibid.*

⁷⁴ *Ibid.*

⁷⁵ *Ibid.*

⁷⁶ *Yahoo*, *supra* note 68, *certiorari* denied, 126 S. Ct. 2332 (2006); see also “Supreme Court won’t consider Yahoo case” *Associated Press* (12 May 2006).

(B) Toben Case (Australia/Germany)

Dr. Frederick Toben, a German-born Australian Holocaust revisionist who denies the existence of the Holocaust,⁷⁷ maintains the Adelaide Institute website⁷⁸ in Australia. A complaint lodged by the Executive Council of Australian Jewry (ECAJ) about the Adelaide Institute's website was heard by the Australian Human Rights and Equal Opportunity Commission (HREOC) in November 1998.⁷⁹ The material on the Adelaide Institute website was deemed to be in breach of section 18(c) of the Australian *Racial Discrimination Act 1975*⁸⁰ by the Human Rights and Equal Opportunity Commission in October 2000 because its content denied the existence of the Holocaust and vilified Jewish people.⁸¹ The material posted on the Adelaide Institute website by Toben cast doubt on the Holocaust, and "suggested that homicidal gas chambers at Auschwitz were unlikely and that some Jewish people, for improper purposes including financial gain, had exaggerated the number of Jews killed during World War II."⁸² The Commission's decision was never enforced, but in 2002, an Australian Federal Court agreed with that decision and ordered Toben to remove the content in question from his website.⁸³ The Court was satisfied that Toben had published material on the World Wide Web which was reasonably likely, in all of the circumstances, to offend, insult, humiliate and intimidate Jewish Australians or a group of Jewish Australians. As Branson J. stated, it was "more probable than not that the material would engender in Jewish Australians a sense of being treated contemptuously, disrespectfully and offensively."⁸⁴ The Court deliberated for some 14 months before making this ruling, and Toben did not file any defence. The Federal Court made orders requiring Toben to remove the offending material, as well as any other material substantially similar to the offending material, from all websites controlled by him or the Adelaide Institute, and not to publish or republish such material again. Toben appealed and in June 2003 the Full Court of the Federal Court of Australia held that Part IIA of the

⁷⁷ For a detailed history of the Holocaust denial movement see Kenneth S. Stern, *Holocaust Denial* (1993), online: American Jewish Committee <<http://www.ajc.org/site/apps/nl/content3.asp?c=ijlTI2PHKoG&b=846637&ct=1102259>>.

⁷⁸ See online: <<http://www.adelaideinstitute.org>>.

⁷⁹ "Jewish group seeking apology over website material" *AAP Newsfeed* (2 November 1998).

⁸⁰ *Racial Discrimination Act 1975* (Cth.).

⁸¹ *Jones v. Toben* (5 October 2000), Australian Human Rights and Equal Opportunity Commission, Case No. H97/120.

⁸² See Australian Race Discrimination Commissioner, *Racism and the Internet: Review of the operation of Schedule 5, Broadcasting Services Act 1992* (November 2002), online Australian Department of Communications, Information Technology and the Arts <http://www.dcita.gov.au/_data/assets/word_doc/10892/Racism_and_the_Internet.doc>.

⁸³ *Jones v. Toben*, [2002] FCA 1150, online: AustLII <http://www.austlii.edu.au/au/cases/cth/federal_ct/2002/1150.html>.

⁸⁴ *Ibid.* at para. 93.

Racial Discrimination Act 1975 which deals with prohibiting offensive behaviour based on racial hatred was constitutionally valid as an exercise of the external affairs power:

In my opinion it is clearly consistent with the provisions of the [International Convention on the Elimination of all forms of Racial Discrimination] and the ICCPR that a State party should legislate to 'nip in the bud' the doing of offensive, insulting, humiliating or intimidating public acts which are done because of race, colour or national or ethnic origin before such acts can go into incitement or promotion of racial hatred or discrimination. The authorities show that, subject to the requisite connection [with the external affairs power], it is for the legislature to choose the means by which it carries into or gives effect to a treaty.⁸⁵

It is worth noting that Toben was previously prosecuted and imprisoned in Germany in December 2000 by the German *Bundesgerichtshof* (Federal High Court) for publishing the same material on the Adelaide Institute website.⁸⁶ To accomplish this, the German Federal High Court had to reverse a lower court decision which held that Toben could not be convicted under the law against inciting racial hatred because the inciting material existed on a foreign website. Toben was arrested in Germany⁸⁷ while attending a conference, and neither his Australian citizenship nor the fact that his web server was located in Australia served as a defence. 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 website.⁸⁸ Toben commented that Germany was "trying to rule the world again by saying that the people who access the Internet have no choice. If someone is offended by the material, they can switch off."⁸⁹ Toben was sentenced to 10

⁸⁵ *Toben v. Jones* [2003] FCAFC 137, online: AustLII <<http://www.austlii.edu.au/au/cases/cth/FCAFC/2003/137.html>>. See further Australian Human Rights and Equal Opportunity Commission, *Change and Continuity: Review of the Federal Unlawful Discrimination Jurisdiction: Supplement September 2002 – August 2003* (Sydney, 2003), Carr J. at 2.

⁸⁶ See Steve Gold, "German Landmark Nazi Ruling" *Newsbytes News Network* (December 12 2000). Note also that in another similar case American neo-Nazi Gary Lauck was jailed for four years in Hamburg after a court convicted him in 1996 of inciting racial hatred for sending anti-Semitic literature to Germany for many years; see "History's rewriter faces German jail" *The Australian* (8 July 1999).

⁸⁷ An English copy of the Arrest Warrant for Dr. Frederick Töben is available at <<http://www.ihr.org/other/990409warrant.html>>. See further "Australian historian arrested in Germany for disputing Holocaust" *Agence France Presse* (09 April 1999).

⁸⁸ See *Report of the High Commissioner for Human Rights, supra* note 42.

⁸⁹ See "Neo-Nazis Sheltering Web Sites In the U.S.; German Courts Begin International Pursuit" *The Washington Post* (21 December 2000).

months imprisonment “for the offences of criminal defamation, several counts of disparaging the memory of the dead and of inciting the populace.”⁹⁰

(C) *Zündel Case (Canada/Germany)*

Ernst Zündel, a German citizen who lived in Canada until his deportation in February 2005, is one of the “world’s most prominent distributors of revisionist neo-Nazi propaganda through the use of facsimiles, courier, telephone, mail, media, shortwave radio transmissions, satellite videos and the Internet, through his website the *Zundelsite*”.⁹¹ In 1997, the Canadian Human Rights Tribunal⁹² heard a complaint brought against Zündel and his website *Zundelsite*,⁹³ which was located on a server in the United States at the time.

Among the principal issues that the Tribunal was called upon to decide was whether the website, in denying the Holocaust,⁹⁴ promoted hatred, and whether Zündel could be said to control the site given that it was physically located outside of Canada.⁹⁵ It was alleged that by posting material to the *Zundelsite*, Zündel caused repeated telephonic communication that was likely to expose Jews to hatred or contempt. The Tribunal was asked to determine whether it was a discriminatory practice to post material on a website if the material was likely to expose a person to hatred or contempt. Further, the Tribunal was asked to consider what limits, if any, were to be applied to repeated communication of hate messages via the Internet. Finally, if these limits applied to the Internet, whether this would be a permissible restriction on freedom of speech under the *Canadian Charter of Rights and Freedoms*.⁹⁶ The original complaints were made in 1996 but the case proceeded very slowly and it took almost six years for the Tribunal to bring this case to an end. A decision was finally published in January 2002.⁹⁷

⁹⁰ See Greg Taylor, “Casting the Net Too Widely: Racial Hatred on the Internet” (2001) *Criminal Law Journal* 262. See further *German Criminal Code*, StGB, ss. 130(1),(3). For the German decision see Bundesgerichtshof, Urteil vom 12. December 2000 - 1 StR 184/00.

⁹¹ *Re Zündel* (2005), 251 D.L.R. (4th) 511 at para. 23, 2005 FC 295 (T.D.).

⁹² For an overview of Canadian issues see Human Rights Commission, *supra* note 2.

⁹³ See <<http://www.zundelsite.org/>>.

⁹⁴ See generally Robert A. Kahn, *Holocaust Denial and the Law: A Comparative Study* (New York: Palgrave MacMillian, 2004). See also *R. v. Zundel*, [1992] 2 S.C.R. 731; and Robert A. Kahn, “Rebuttal versus Unmasking: Legal Strategy in *R v. Zundel*” (2000) 34(3) *Institute for Jewish Policy Research* 3.

⁹⁵ See *Report of the High Commissioner for Human Rights*, *supra* note 42.

⁹⁶ *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.

⁹⁷ *Citron v. Zündel* (18 January 2002), T.D. 1/02, Canadian Human Rights Tribunal, online: CHRT <http://www.chrt-tcdp.gc.ca/search/view_html.asp?doid=252&lg=e&isruling=0> [*Citron*]. See also: *Citron v. Zundel* (2000), 189 D.L.R. (4th) 131 (F.C.A.); and 195 D.L.R. (4th) 399 (F.C.A.); both involved administrative appeals during the course of the Tribunal’s consideration of the case. Similarly note also *Zundel v. Canada (Attorney General)* (T.D.), [1999] 4 F.C. 289 (T.D.).

The Tribunal referred to a number of previous cases and studies which found that hate propaganda poses a “serious threat to society”.⁹⁸ The Tribunal ordered that Zündel, and any other individuals who act in his name or in concert with him, cease to communicate telephonically content of the type contained on the *Zundelsite*, contrary to section 13(1) of the *Canadian Human Rights Act*.⁹⁹ In the view of the Tribunal, the use of section 13(1) of the *Act* to deal with hateful telephonic messages on the Internet remains a restriction on the Respondent's freedom of speech which is reasonable and justified in a free and democratic society.¹⁰⁰ In terms of the effect of the Internet to disseminate hatred, the Tribunal stated that it was difficult “to see why the Internet, with its pervasive influence and accessibility, should be available to spread messages that are likely to expose persons to hatred or contempt. One can conceive that this new medium of the Internet is a much more effective and well-suited vehicle for the dissemination of hate propaganda.”¹⁰¹ The Tribunal sent a clear message that hate could not be tolerated on the Internet or elsewhere. However, the *Zundelsite* continued to transmit through a server in the United States and continues to do so today.

In the later case of *Warman v. Kyburz*, the Canadian Human Rights Tribunal rightly assessed that “the unique nature of Internet technology, including the jurisdictional challenges arising from the borderless world of cyberspace, as well as the ‘moving targets’ created by the use of mirror sites raise real concerns as to the efficacy of cease and desist orders in relation to hate messages disseminated on the Internet.”¹⁰² Despite these difficulties and technical challenges, a “cease and desist

⁹⁸ See for example *Taylor*, *supra* note 3; see also *Report to the Minister of Justice of the Special Committee on Hate Propaganda in Canada* (Ottawa: Queen's Printer, 1966); See generally Philip Rosen, *Hate Propaganda* in Current Issue Review 85-6E (Ottawa: Canadian Parliamentary Research Branch, 2000), online: Government of Canada <<http://www.parl.gc.ca/information/library/PRBpubs/856-e.pdf>>.

⁹⁹ *Canadian Human Rights Act*, R.S.C. 1985, c. H-6, s. 13(1):

It is a discriminatory practice for a person or a group of persons acting in concert to communicate telephonically or to cause to be so communicated, repeatedly, in whole or in part by means of the facilities of a telecommunication undertaking within the legislative authority of Parliament, any matter that is likely to expose a person or persons to hatred or contempt by reason of the fact that that person or those persons are identifiable on the basis of a prohibited ground of discrimination.

¹⁰⁰ See further Monette Maillet, “Hate Message Complaints and Human Rights Tribunal Hearings” in *Hate on the Net*, (Ottawa: Association for Canadian Studies, Spring 2006) 78, online: Canadian Human Rights Commission <http://www.chrc-ccdp.ca/pdf/hateoninternet_bil.pdf>.

¹⁰¹ *Citron*, *supra* note 97 at para. 240. See also: *Schnell v. Machiavelli and Associates Emprize Inc.* (20 August 2002) T.D. 11/02 (CHRT) [*Schnell*]; *Warman v. Kyburz* (9 May 2003) 2003 CHRT 18 [*Kyburz*]; and *Warman v. Warman* (23 September 2005) 2005 CHRT 36 [*Warman*].

¹⁰² *Kyburz*, *ibid.* at para. 81. For Canadian Human Rights Tribunal decisions in Internet related cases see further: *Warman v. Harrison* (15 August 2006) 2006 CHRT 30 [*Harrison*]; *Warman v. Kulbashian* (10 March 2006) 2006 CHRT 11; *Warman v. Winnicki* (13 April 2006) 2006 CHRT 20; *Schnell*, *ibid.*; and *Warman*, *ibid.*

order can have both a practical and symbolic effect.”¹⁰³ Such a decision prevents (albeit not always successfully) the individuals or organizations concerned from continuing to publish material of a racist nature. Apart from trying to prevent and eliminate discriminatory practices, such a decision also has a significant symbolic value in the public denunciation of such actions, as well as enabling the open discussion of the principles enunciated therein.

As for Ernst Zündel, he moved to the United States in 2000, but was deported back to Canada in 2003 for alleged immigration violations. He was declared a national security threat by a Canadian Federal Court and was deported to Germany in February 2005. Zündel was charged with inciting racial hatred, libel and disparaging the dead before the State Court in the Southwestern city of Mannheim,¹⁰⁴ and was sentenced to a five-year prison term in February 2007.¹⁰⁵ In a parallel development, David Irving, a well known British Holocaust denier who also publishes his thoughts on this subject, was arrested in November 2005 in Austria on a warrant issued in 1989 under Austrian laws that make it a crime to deny the Holocaust.¹⁰⁶ Irving was sentenced to three years imprisonment in February 2006.¹⁰⁷

The limitations of the legal system are also evidenced in Britain in respect to a website hosted outside Britain that started publishing hit lists around 2003.¹⁰⁸ *Redwatch*, produced by “Combat 18”, started publishing the names and addresses of anti-racist campaigners in Britain in print format in 1993, almost 10 years before they set up the website.¹⁰⁹ As the printed publication encouraged violence, several

¹⁰³ Harrison, *ibid.* at para. 72.

¹⁰⁴ Anthony Long, “Forgetting the Fuhrer: The recent history of the Holocaust denial movement in Germany” (2002) 48(1) *Australian Journal of Politics & History* 72.

¹⁰⁵ See “5-year prison term urged for Holocaust denier” *Associated Press* (26 January 2007).

¹⁰⁶ See “Irving faces week in Austria cell” *BBC News* (18 November 2005); and “Austria Arrests David Irving, Writer Known as a Holocaust Denier” *The New York Times* (18 November 2005).

¹⁰⁷ See “Irving jailed for 3 years after denying Holocaust” *The Daily Telegraph* (21 February 2006); “Irving jailed for denying Holocaust: Three years for British historian who described Auschwitz as a fairytale” *The Guardian* (21 February 2006); and “Irving gets three years' jail in Austria for Holocaust denial” *The Independent* (21 February 2006). Note that David Irving was also convicted in Germany in 1993 of insulting the memory of the dead, for describing the Auschwitz I gas chamber as an “Attrappe” (“fake”) at a rally on 21 April 1990, in the *Löwenbräukeller* in Munich. See Long, *supra* note 104 at 83.

¹⁰⁸ See “Pictures of children on fascist site” *Evening Chronicle [Newcastle]* (17 January 2003); “Student is target on hate website” *UK Newsquest Regional Press - This is Lancashire* (09 April 2003); “Extreme-right Website Targets Lecturer” *Times Educational Supplement* (25 April 2003); “Race Hate Website Targeting Activists” *The [Sheffield] Star* (23 October 2003); “Neo-Nazi's target MEP” *UK Newsquest Regional Press - This is Lancashire* (23 December 2003); “Anti-racism councillor caught in far right web” *The [Stoke] Sentinel* (4 January 2004); and “Web outing won't stop my battle to beat racism” *The [Stoke] Sentinel* (5 January 2004).

¹⁰⁹ See “RACE magazines publish names and addresses of 'Red' Activists” *The Guardian* (20 February 1993); and “Rapid increase in racial attacks ‘Widely Ignored’” *The Guardian* (20 February 1993).

warnings were issued by the Special Branch to the targets named by *Redwatch* during the late 1990s.¹¹⁰ In late 2003, the Home Office and the former Home Secretary, David Blunkett, were put under pressure to shut down the website.¹¹¹ There were further calls for action from the House of Lords in January 2004.¹¹² After Lord Greaves brought this issue to the attention of Parliament, his picture and details were also posted on the *Redwatch* website.¹¹³ The Home Office launched an investigation in March 2004,¹¹⁴ but this did not develop into anything. There were further calls for action within the British Parliament in June 2006 following an incident involving an attack on an anti-fascist campaigner whose details were listed on the website.¹¹⁵ Angela Eagle, MP, stated that “what is certain is that both the incitement to violence and the attacks are continuing, despite the fact that the existence of this website was exposed and caused widespread concern several years ago.”¹¹⁶ Obviously, concerns were raised about the U.S. hosting of the website, and the government “initiated inquiries with the U.S. Department of Justice to establish whether hosting such a website constitutes a breach of U.S. law, regulations or industry good practice.”¹¹⁷ Whether any action will be taken in the U.S. remains to be seen. Websites like *Redwatch* are designed to encourage violence, but freedom of speech should not include the freedom to conspire to attack people. As Hari rightly questions: what possible other purpose is there but to encourage attacks or, at the very least, intimidation?¹¹⁸

These examples reflect the complex nature of the Internet as well as the limitations of the application of existing laws to the Internet. New communication technologies challenge the territoriality notion of nation-states¹¹⁹ as the Internet does

¹¹⁰ See “Warning to VIPs on Nazi list of targets” *Evening Standard [London]* (23 February 1996); and “Yard alerts targets on Nazi hit list” *Mail on Sunday [London]* (2 April 1995).

¹¹¹ See “Special report: Website linked to far right hit list: Home secretary under pressure to clamp down on fascist” *The Guardian* (17 December 2003).

¹¹² See “Lords demand action to shut racist websites” *Yorkshire Evening Post* (10 January 2004).

¹¹³ See “Call to close hard right website” *The Guardian* (15 January 2004).

¹¹⁴ See “Home Office begins inquiry into far-right hate website” *Morning Star [London]* (16 March 2004).

¹¹⁵ See “MPs in move to close far-right website” *The Guardian* (20 July 2006).

¹¹⁶ U.K., H.C., *Parliamentary Debates*, vol. 447, col. 1436 at 1437 (21 June 2006).

¹¹⁷ *Ibid.* at col. 1442.

¹¹⁸ Johann Hari, “Violence, Hatred and Freedom of Speech” *The Independent [London]* (5 December 2003).

¹¹⁹ See generally Christo Pierson, *The Modern State* (London: Routledge, 1996) at 5-35; Francis Harry Hinsley, *Sovereignty*, 2d ed. (Cambridge: Cambridge University Press, 1986) at 1-26; Max Weber, “Politics as vocation” in Hans Heinrich Gerth & Charles Wright Mills, eds., *From Max Weber* (London: Routledge, 1970) at 78; and David Held, *Democracy and the Global Order* (Cambridge: Polity, 1995) at 66.

not respect boundaries¹²⁰ to the effect that no single nation-state can effectively dominate or control the Internet by means of unilateral state regulation.¹²¹ According to Castells, nation-states are losing their capacity to govern due to the “globalisation of core economic activities, globalisation of media and electronic communication, and globalisation of crime.”¹²² This is also true for the governance of the Internet by individual nation-states.

It should be noted that the Zündel case took nearly five years to be finalized in Canada, and even after that, various Zündel-related trials continued in Germany until February 2007. Even now, Zündel’s website is still running and regularly updated with his “letters from prison” despite his incarceration. The Toben case was a similarly drawn-out affair and Toben’s carefully drafted website is also still active and regularly updated. On the same note, various cases related to the Yahoo! case both in France and the U.S. were initiated over five years ago and only came to a conclusion in May 2006. Today *Redwatch*, which came to the attention of the British Home Office in 2003, still publishes the above mentioned lists. The legal system, which is more adapted to deal with traditional one-off publications (such as newspapers and magazines) has been extremely slow in dealing with web-based publications. Above all else, these cases illustrate that the emergence of Internet governance entails a more diverse and fragmented regulatory network with no presumption that these will be anchored primarily in nation-states. A shift from unilateral state regulation into various forms and models of governance will almost inevitably be witnessed, in which alternatives to state regulation such as self-regulation, co-regulation, or a mixture of these will be considered by states and international organizations. These alternative and additional forms of regulation are addressed later in this article.

4. Regional International Initiatives

There is no doubt that the future development of the international legal system will not only rest on the activities of states, but also increasingly on the international organizations they have created themselves to overcome the limits of the capacity of national governments to deal effectively with transnational problems.¹²³

There have been a number of developments at the international level in relation to the availability of racist content on the Internet and related policy matters. This section of the article provides an overview of the initiatives at the Council of Europe

¹²⁰ See generally Brian Kahin & Charles Nesson, eds., *Borders in Cyberspace: Information Policy and Global Information Infrastructure* (Cambridge, Mass.: MIT Press, 1997).

¹²¹ See e.g. Jack Goldsmith, “Unilateral Regulation of the Internet: A Modest Defence” (2000) 11 E.J.I.L. 135.

¹²² See Manuel Castells, *The Power of Identity (Volume II of The Information Age: Economy, Society and Culture)* (Oxford: Blackwell Publishers, 1997) at 244-62.

¹²³ See Peter Malanczuk, *Akehurst's Modern Introduction to International Law*, 7th ed. (London: Routledge, 1997) at 96.

(CoE), the Organization for Security and Co-operation in Europe (OSCE) and the European Union (EU) levels before addressing the larger international initiatives at the UN level.

(A) Initiatives by the Council of Europe

The Council of Europe (CoE)¹²⁴ was the first international organization to be founded in Europe after the Second World War and its main role is to strengthen democracy, human rights and the rule of law throughout its Member States. The CoE's Cyber-Crime Convention 2001¹²⁵ is the first international treaty to address criminal law and procedural aspects of various types of offensive behaviour directed against computer systems, networks or data, in addition to content related crimes such as child pornography. In general, the Convention aims to harmonize national legislation in this field, facilitate investigations, and allow efficient levels of co-operation between the authorities of different Member States of the CoE and other third party states who would be party to the Convention following a ratification process at the national level.

A Committee of Experts on Crime in Cyberspace (PC-CY) was established within the CoE in 1997 to draw up the Cyber-Crime Convention to fight *inter alia* substantive offences committed through the use of the Internet.¹²⁶ A number of non-Member States such as the U.S., Canada, Japan, and South Africa also contributed to the development of the Convention through the PC-CY.¹²⁷ Since then, several versions have been developed and a final version was published in June 2001¹²⁸ following the approval of the European Committee on Crime Problems (CDPC).¹²⁹ The Council of Europe Ministers' Deputies approved the Convention in September 2001.¹³⁰ This was followed by a formal adoption at the Foreign Affairs Ministers meeting and an opening up of the Convention to signatures in November 2001.

¹²⁴ See <<http://www.coe.int>>.

¹²⁵ The text of the Cyber-Crime Convention can be found at <<http://conventions.coe.int/treaty/en/projects/cybercrime.htm>>. See further Akdeniz, *supra* note 46.

¹²⁶ See European Commission, *Interim report on Initiatives in EU Member States with respect to Combating Illegal and Harmful Content on the Internet*, Version 7 (4 June 1997).

¹²⁷ The United States was invited to participate as an "observer" for the development of the 1989 and 1995 Recommendations, as well as in the development of the Convention on Cyber-Crime. See Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice, *Council of Europe Convention on Cybercrime - Frequently Asked Questions and Answers* (November 2003), online: U.S. Department of Justice <<http://www.justice.gov/criminal/cybercrime/COEFAQs.htm>>.

¹²⁸ Council of Europe, European Committee on Crime Problems (CDPC), *Final Draft Convention on Cyber-crime* CDPC (2001) 17. See also the related *Explanatory Memorandum to the Cyber-Crime Convention*, online: <<http://www.privacyinternational.org/issues/cybercrime/coe/cybercrimememo-final.html>>.

¹²⁹ An intergovernmental body of experts reporting to the Council of Europe's Committee of Ministers.

¹³⁰ Council of Europe, Press Release, 646a(2001), "First international treaty to combat crime in cyberspace approved by Ministers' Deputies" (19 September 2001).

As of this writing, the signing and ratification process for the main Cyber-Crime Convention has resulted in 38 Member States (as well as the external supporters)¹³¹ signing and 19 of the potential 50 countries ratifying the main convention.¹³² Following the first five ratifications, the Cyber-Crime Convention came into force on 1 July 2004.

(B) Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems

Although action against racism is viewed by the CoE as an integral part of the protection and promotion of human rights, the CoE did not develop a specific convention addressing racism. In 1997, a CoE Recommendation on Hate Speech called upon Member States “to take appropriate steps to combat hate speech by ensuring that such steps form part of a comprehensive approach to the phenomenon which also targets its social, economic, political, cultural, and other root causes”.¹³³ Parallel to this political call, the Committee drafting the Cyber-Crime Convention discussed the possibility of including content-related offences other than child pornography (article 9) within the Convention, such as the distribution of racist propaganda through computer systems. However, provisions involving the criminalisation of acts of a racist and xenophobic nature committed through computer systems were left out of the Cyber-Crime Convention 2001 as there was no consensus on the inclusion of such provisions. While European states such as France and Germany strongly supported inclusion, the United States of America, which has been influential in the development of the main Convention, opposed the inclusion of speech related provisions apart from child pornography.

Noting the complexity of the issue, the Committee drafting the cybercrime Convention decided that the Committee would refer to the CDPC the issue of drafting an Additional Protocol to the Convention.¹³⁴ In its Opinion No. 226 (2001) concerning the Convention, the Parliamentary Assembly recommended the immediate development of an additional protocol to the Convention under the title “Broadening the scope of the convention to include new forms of offence”, with the purpose of defining and criminalising, *inter alia*, the dissemination of racist propaganda.¹³⁵

¹³¹ The United States, Canada, South Africa, Japan and Montenegro.

¹³² Of the 45 CoE States and 5 external supporters, the Convention has been ratified by: Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, France, Hungary, Iceland, Lithuania, Netherlands, Norway, Romania, Slovenia, the former Yugoslav Republic of Macedonia, Ukraine, and the United States. The U.S. Senate approved the ratification of the CyberCrime Convention on 3 August 2006. See Declan McCullagh & Anne Broache, “Senate ratifies controversial cybercrime treaty” *CNET News* (05 August 2006), online: News.com <http://news.com.com/Senate+ratifies+controversial+cybercrime+treaty/2100-7348_3-6102354.html>.

¹³³ Council of Europe, Committee of Ministers, *Recommendation R (97)20* (1997).

¹³⁴ See *Explanatory Report*, *supra* note 1 at para. 4.

¹³⁵ *Ibid.* at para. 5.

The CDPC and its Committee of Experts on the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems (PC-RX) were handed the task of preparing the additional protocol, dealing in particular with the following issues:

(i) the definition and scope of elements for the criminalisation of acts of a racist and xenophobic nature committed through computer networks, including the production, offering, dissemination or other forms of distribution of materials or messages with such content through computer networks;

(ii) the extent of the application of substantive, procedural and international co-operation provisions in the Convention on Cyber-Crime to the investigation and prosecution of the offences to be defined under the additional Protocol.¹³⁶

The Parliamentary Assembly viewed racism “not as an opinion but as a crime” in its Recommendation 1543 (2001) on Racism and Xenophobia in Cyberspace.¹³⁷ The Parliamentary Assembly also noted that the protocol will “have no effect unless every state hosting racist sites or messages is a party to it”.¹³⁸

The Additional Protocol aims to harmonize substantive criminal law in the fight against racism and xenophobia on the Internet and to improve international cooperation in this area.¹³⁹ The CoE believes that a harmonized approach in domestic laws may prevent misuse of computer systems for a racist purpose. The Explanatory Memorandum to the Additional Protocol states that “[t]his kind of harmonisation alleviates the fight against such crimes on the national and on the international level. Corresponding offences in domestic laws may prevent misuse of computer systems for a racist purpose by Parties whose laws in this area are less well defined.”¹⁴⁰ Further:

[The Additional] Protocol entails an extension of the [Cyber-Crime] Convention’s scope, including its substantive, procedural and international cooperation provisions, so as to cover also offences of racist and xenophobic propaganda. Thus, apart from harmonizing the substantive law elements of such behaviour, the Protocol aims at improving the ability of the Parties to make use of the means and avenues of international cooperation set out in the Convention in this area.¹⁴¹

¹³⁶ *Ibid.* at para. 6.

¹³⁷ Council of Europe, P.A., *Recommendation 1543 (2001)* at para. 1, as adopted by the Standing Committee, acting on behalf of the Parliamentary Assembly.

¹³⁸ *Ibid.* at para. 4.

¹³⁹ See *Explanatory Report*, *supra* note 1 at para. 10.

¹⁴⁰ *Ibid.* at para. 3.

¹⁴¹ *Ibid.* at para. 7.

The definition of “racist and xenophobic material” contained in article 2 of the Additional Protocol refers to written material (e.g. texts, books, magazines, statements, messages, etc.), images (e.g. pictures, photos, drawings, etc.) or any other representation of thoughts or theories:

which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors in such a format that it can be stored, processed and transmitted by means of a computer system.¹⁴²

Measures to be taken at the national level are explained in chapter II of the Additional Protocol. Article 3 (“Dissemination of racist and xenophobic material through computer systems”) requires parties to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the distribution of, or otherwise making available, racist and xenophobic material to the public through a computer system.¹⁴³ Such conduct needs to be committed intentionally and without right.¹⁴⁴ The “intention” requirement would limit the liability of Internet Service Providers (ISPs) if they acted solely as a conduit, but this would not exclude “notice based liability” as introduced by the EU Directive on Electronic Commerce and discussed below.

Article 4 requires parties to criminalise racist and xenophobic motivated threats through computer systems and, as with article 3, such conduct needs to be committed intentionally and without right.¹⁴⁵ Article 5 requires parties to criminalise racist and xenophobic motivated insults made in public¹⁴⁶ through computer systems.¹⁴⁷ Article 6 requires the criminalisation of expressions which deny, grossly minimize, approve or justify acts constituting genocide or crimes against humanity, as defined by international law and as recognized by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 April

¹⁴² *Ibid.* at para. 12.

¹⁴³ Note that article 7 requires parties to criminalise the intentional aiding or abetting of the commission of any of the offences established in accordance with the Additional Protocol.

¹⁴⁴ But note that article 3(2) states that Parties may reserve the right not to attach criminal liability to such conduct “where the material, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available”. Notwithstanding this, article 3(3) further allows a Party to reserve the right not to attach criminal liability to “those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to [above]”.

¹⁴⁵ Note that unlike in article 3, no exceptions are provided for this offence and parties may not reserve the right not to attach criminal liability to such conduct.

¹⁴⁶ Unlike the case of threat, an insult expressed in private communications is not covered by this provision.

¹⁴⁷ Note, however, that article 5(2) permits Parties to reserve the right not to apply this provision, or to require that an “insult” be defined as exposure to “hatred, contempt or ridicule”.

1945.¹⁴⁸ This is supported by the European Court of Human Rights which made it clear in its judgment in *Lehideux and Isorni v. France* that the denial or revision of “clearly established historical facts – such as the Holocaust – whose negation or revision would be removed from the protection of article 10 by article 17 [of the European Convention on Human Rights].”¹⁴⁹ According to the Court, “there is no doubt that, like any other remark directed against the Convention’s underlying values, the justification of a pro-Nazi policy could not be allowed to enjoy the protection afforded by Article 10.”¹⁵⁰

The Additional Protocol was opened for signature in Strasbourg on 28 January 2003 and has since been signed by 31 Member States.¹⁵¹ Out of the 31 signing States, only 10 Member States¹⁵² have ratified the Additional Protocol as of this writing. The Protocol entered into force on 1 March 2006, following the initial five ratifications. More recently, a Recommendation of the Parliamentary Assembly of the Council of Europe on Media and Terrorism¹⁵³ recommended that the Committee of Ministers ask member and observer States to apply the Additional Protocol to terrorist content insofar as such content advocates, promotes or incites hatred or violence against any individual or group of individuals based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

¹⁴⁸ Note, however, that article 6(2) permits Parties to reserve the right not to apply this provision, or to require that the denial or gross minimization referred to be committed with the intent to incite hatred, discrimination or violence against an individual or group.

¹⁴⁹ *Lehideux and Isorni v. France*, judgment of 23 September 1998, p. 2864, ECHR 1998-VII [*Lehideux*]. See also Shermer & Grobman, *supra* note 25.

¹⁵⁰ *Lehideux, ibid.* at para. 53. See, *mutatis mutandis*, *Jersild v. Denmark*, judgment of 23 September 1994, Series A no. 298, ECHR, p. 25, § 35. Note also that a recent United Nations Resolution rejected any denial of the Holocaust as an historical event, either in full or part in October 2005: *Holocaust remembrance*, GA Res. 60/7, UN GAOR, 60th Sess., UN Doc. A/60/L.12 (2005).. See further the UN General Assembly resolution condemning any denial of Holocaust, GA Res. 61/255, UN GAOR, 61st Sess., UN Doc. A/61/L.53 (2007).

¹⁵¹ Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Poland, Portugal, Romania, Serbia and Montenegro, Slovenia, Sweden, Switzerland, Ukraine. Note that Canada also signed the Additional Protocol.

¹⁵² Of the 45 CoE States and five external supporters, the convention has been ratified by: Albania, Bosnia and Herzegovina, Cyprus, Denmark, France, Lithuania, Slovenia, Ukraine, and the former Yugoslav Republic of Macedonia.

¹⁵³ Council of Europe, P.A., 2005 Ordinary Session (Third Part) *Media and Terrorism*, Texts Adopted, Rec. 1706 (2005), online: CoE <<http://assembly.coe.int/Documents/AdoptedText/ta05/EREC1706.htm>>. See also Josef Jarab, *Report for the Parliamentary Assembly on Media and Terrorism*, Doc. 10557 (2005), online: CoE <<http://assembly.coe.int/Documents/WorkingDocs/Doc05/EDOC10557.htm>>.

(C) Initiatives by the Organization for Security and Co-operation in Europe

During the past few years there have been increasing demands within the Organization for Security and Co-operation in Europe (OSCE) to enhance the work of the Organization in the area of action against racism, xenophobia, discrimination, and anti-Semitism.¹⁵⁴ The 11th Ministerial Council meeting in December 2003 in Maastricht encouraged the participating States to collect and keep records and statistics on hate crimes, including forms of violent manifestations of racism, xenophobia, discrimination and anti-Semitism. The Ministerial Council also gave concrete responsibilities to the OSCE institutions, including the Office for Democratic Institutions and Human Rights which was tasked with serving as a collection point for information and statistics collected by participating States, in full cooperation with, *inter alia*, the UN Committee on the Elimination of Racial Discrimination (CERD), the European Commission against Racism and Intolerance (ECRI), and the European Monitoring Centre on Racism and Xenophobia (EUMC), as well as relevant Non-Governmental Organizations (NGOs).

The OSCE has organized a number of high-level conferences and meetings in recent years to address the problems of racism, xenophobia, discrimination, and anti-Semitism.¹⁵⁵ The need to combat hate crimes, which can be fuelled by racist, xenophobic and anti-Semitic propaganda on the Internet, was explicitly recognized by a decision during the 2003 Maastricht Ministerial Council.¹⁵⁶ This was reinforced by the OSCE Permanent Council Decision on Combating anti-Semitism (PC.DEC/607)¹⁵⁷ and its Decision on Tolerance and the Fight against Racism, Xenophobia and Discrimination (PC.DEC/621)¹⁵⁸ in 2004. In November 2004, the

¹⁵⁴ See generally OSCE Office for Democratic Institutions and Human Rights (ODIHR), *International Action Against Racism, Xenophobia, Anti-Semitism and Tolerance in the OSCE Region: A Comparative Study* (September 2004), online: OSCE <http://www.osce.org/publications/odihr/2004/09/12362_143_en.pdf>. See also: ODIHR, *Combating Hate Crimes in the OSCE Region: An Overview of statistics, legislation, and national initiatives* (June 2005), online: OSCE <http://www.osce.org/publications/odihr/2005/09/16251_452_en.pdf>; and ODIHR, *Challenges and Responses to Hate-Motivated Incidents in the OSCE Region*, (October 2006), online: OSCE <http://www.osce.org/documents/odihr/2006/10/21496_en.pdf>.

¹⁵⁵ Conference on Anti-Semitism, Vienna (19 June 2003); Conference on Racism, Xenophobia and Discrimination, Vienna (4 September 2003); Conference on Anti-Semitism, Berlin (28 April 2004); Meeting on the Relationship between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes, Paris (16 June 2004); Conference on Tolerance and the Fight Against Racism, Xenophobia and Discrimination, Brussels (13 September 2004); and Conference on Anti-Semitism, and other forms of Intolerance, Cordoba (8 June 2005).

¹⁵⁶ See Maastricht Ministerial Council, *Decision No. 4/03 on Tolerance and Non-Discrimination* (2003) at para. 8.

¹⁵⁷ See <http://www.osce.org/documents/pc/2004/04/2771_en.pdf>.

¹⁵⁸ See <http://www.osce.org/documents/pc/2004/07/3374_en.pdf>.

OSCE also published a Permanent Council Decision on Promoting Tolerance and Media Freedom on the Internet (PC.DEC/633).¹⁵⁹

The November 2004 Council Decision stated that participating States should investigate and, where applicable, fully prosecute violence as well as criminal threats of violence motivated by racist, xenophobic, anti-Semitic or other related bias on the Internet.¹⁶⁰ Alongside the decision, the OSCE Representative on Freedom of the Media was given the task of actively promoting both freedom of expression and access to the Internet, and will continue to observe relevant developments in all participating States. This will involve monitoring and issuing early warnings when laws or other measures prohibiting speech motivated by racist, or other related bias are enforced in a discriminatory or selective manner for political purposes which can lead to impeding of the expression of alternative opinions and views.¹⁶¹ The Council also decided that participating States should study the effectiveness of laws and other measures regulating Internet content, specifically with regard to their effect on the rate of racist crimes,¹⁶² as well as encourage and support analytically rigorous studies on the possible relationship between racist speech on the Internet and the commission of crimes motivated by such speech.¹⁶³

(D) Initiatives by the European Union

European developments with respect to the governance of hate speech on the Internet are of particular interest. On the one hand, there is the diversity of European societies and their varying experiences with racial hatred. On the other hand, the Internet is said to engender the "Network Society",¹⁶⁴ where there is far greater social and political interconnectivity, which regionally builds upon the integrative efforts of the EU. In addition to being concerned with: telecommunications

¹⁵⁹ See <http://www.osce.org/documents/pc/2004/11/3805_en.pdf>. Note also the Ministerial Council Decision No. 12/04 on Tolerance and Non-Discrimination, December 2004, at <http://www.osce.org/documents/mcs/2004/12/3915_en.pdf>, as well as the Cordoba Declaration, CIO.GAL/76/05/Rev.2, 9 June 2005, at <http://www.osce.org/documents/cio/2005/06/15109_en.pdf>.

¹⁶⁰ See Maastricht Ministerial Council, *Decision No. 633: Promoting Tolerance and Media Freedom on the Internet* (2004), at decision no. 2, online: OSCE <http://www.osce.org/documents/mcs/2004/12/3915_en.pdf>.

¹⁶¹ *Ibid.* at decision no. 4.

¹⁶² *Ibid.* at decision no. 5.

¹⁶³ *Ibid.* at decision no. 6.

¹⁶⁴ See Manuel Castells, *The Rise of the Network Society (Volume 1 of The Information Age: Economy, Society and Culture)* (Oxford: Blackwell Publishers, 1997).

liberalization; the creation of a European Information Society;¹⁶⁵ the development of electronic commerce; and data protection and privacy, the EU is also committed to steering cooperation in fighting crime within the Member States in relation to the exploitation of women, the sexual exploitation of children, and high-tech crime.¹⁶⁶ The concepts of tolerance, anti-discrimination and the fight against racism are strongly embedded in the institutional framework of the EU.¹⁶⁷ The EU has always been very active in the field of racism and xenophobia as well as in relation to safer use of the Internet.¹⁶⁸

In November 2001, the European Commission proposed a Framework Decision on combating racism and xenophobia designed to ensure that both are punishable in all member States by effective, proportionate and dissuasive criminal penalties.¹⁶⁹ The draft Framework Decision addresses every form of racism and xenophobia irrespective of its motivation or grounds, and intends to improve judicial cooperation between the Member States. However, the Framework Decision has not been finalized; discussions in the Council of the EU on the proposed Framework Decision continued under the Luxembourg Presidency in 2005, but were not concluded, again largely due to differing approaches between Member States to limitations in the exercise of freedom of expression.¹⁷⁰ Even if an agreement had been reached in 2005, the implementation of the Framework Decision would not have taken place before June 2007.

More specifically, in relation to safer use of the Internet, the EU developed an Action Plan through the European Commission¹⁷¹ in 1998 which encouraged self-

¹⁶⁵ See EC, *eEurope - An Information Society for all - Progress report for the Special European Council on Employment, Economic reforms and social cohesion towards a Europe based on innovation and knowledge* (March 2000); EC, *eEurope 2002 - An Information society for all - Draft Action Plan* (June 2000); EC, *The eEurope 2002 update* (December 2000); EC, *eEurope 2002: Impact and Priorities A communication to the Spring European Council in Stockholm* (March 2001); and EC, *Opinion of the Economic and Social Committee on 'eEurope 2002 - An information society for all - Draft Action Plan'* [2001] O.J. C 123/36.

¹⁶⁶ At its Tampere meeting in October 1999, the Council of the European Union stated that the fight against cybercrime is a priority in developing the Union as an area of freedom, security and justice (article 2 of the EU Treaty); see EC, *Presidency Conclusions* (October 1999) at para. 48, online: <http://www.europarl.europa.eu/summits/tam_en.htm>. See further EC, *Joint Action 97/154/JHA concerning action to combat trafficking in human beings and sexual exploitation of children* [1997] O.J. L 63/2.

¹⁶⁷ See EU, *Annual Report on Human Rights – 2005* (Brussels, 2005).

¹⁶⁸ See EC, *Joint Declaration by the Council and the Representatives of the Governments of the Member States, meeting within the Council of 8 June 2001 on combating racism and xenophobia on the Internet by intensifying work with young people* [2001] O.J. C 196/01.

¹⁶⁹ EC, *Proposal for a Council framework decision on combating racism and xenophobia*, [2002] O.J. C 75E/269.

¹⁷⁰ See *Annual Report*, *supra* note 167.

¹⁷¹ Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, December 1998.

regulatory initiatives to deal with illegal and harmful Internet content including: the creation of a European network of hotlines for Internet users to report illegal content such as child pornography; the development of self-regulatory and content-monitoring schemes by access and content providers; and the development of internationally compatible and interoperable rating and filtering schemes to protect users. Furthermore, the EU Action Plan advocated measures to increase awareness among parents, teachers, children and other consumers of available options to help these groups use the networks safely by choosing the right control tools. Although originally established as a three year Action Plan, in 2002¹⁷² the European Commission prolonged the work in this field for another two years, expanding the Action Plan related work and projects to cover the EU candidate countries.¹⁷³ One of the main reasons for this expansion was the fact that illegal and harmful content on the Internet remained as a continuing concern for lawmakers, the private sector, and parents. The coverage of the Action Plan was extended to new online technologies:

including mobile and broadband content, online games, peer-to-peer file transfer, and all forms of real-time communications such as chat rooms and instant messages. Action will be taken to ensure that a broader range of areas of illegal and harmful content and conduct of concern are covered, including racism and violence.¹⁷⁴

In May 2005, the EU extended the Action Plan work for the period of 2005-2008 to continue to promote safer use of the Internet and new online technologies, by strengthening the fight against illegal content such as child pornography and racist material, content that is potentially harmful to children and content unwanted by the end-user. It is suggested by the extended "Safer Internet Plus Action Plan" that:

practical measures are still needed to encourage reporting of illegal content to those in a position to deal with it, to encourage assessment of the performance of filter technologies and the benchmarking of those technologies, to spread best practice for codes of conduct embodying generally agreed canons of behaviour, and to inform and educate parents and children on the best way to benefit from the potential of new online technologies in a safe way.¹⁷⁵

¹⁷² See EC, *Follow-up to the Multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks: Proposal for a decision of the European Parliament and of the Council amending Decision No 276/1999/EC adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks*, COM (2002) 152, Brussels.

¹⁷³ *Ibid.* at para. 3.1.2. (Interface to candidate countries).

¹⁷⁴ See *Safer Internet Action Plan: Work Programme 2003-2004* at 3, online: EC <http://ec.europa.eu/information_society/activities/sip/docs/pdf/programmes/workprgm/work_programme_2003_04_en.pdf>.

¹⁷⁵ EC, *Decision No 854/2005/EC of the European Parliament and of the Council establishing a Multiannual Community Programme on promoting safer use of the internet and new online technologies*, [2005] O.J. L 149/1 at para. 7.

The four year program will have a budget of EUR 45 million and it will focus more closely on end-users; namely parents, educators and children. The indicated budget breakdown suggests that almost half of the available budget will be spent on raising awareness (47-51%). Fighting against illegal content will receive 25-30%, tackling unwanted and harmful content 10-17%, and promoting a safer environment 8-12% of the budget.¹⁷⁶

In 2005, the European Commission also published the draft Television Without Frontiers Directive¹⁷⁷ with the aim of making all audiovisual media services (both linear¹⁷⁸ and non-linear¹⁷⁹) subject to the same minimum regulatory requirements. With the proposed Directive, the European Commission aims to ensure compliance with policy objectives relating to the protection of minors against harmful audiovisual content and the protection of human dignity, including a ban on incitement to racial hatred.

One of the proposed provisions¹⁸⁰ would make non-linear services and linear services subject to the same minimum requirements of the prohibition of incitement to hatred. However, the draft Directive proposes minimum standards which are not subject to derogation by EU Member States, who will no longer be able to derogate from the country of origin principle¹⁸¹ unless it is necessary for the protection of minors or the fight against incitement to hatred on grounds of race, sex, religion or nationality, and violation of human dignity concerning individual persons or protection of consumers as provided in article 3(4) of the E-Commerce Directive.¹⁸²

Despite these significant policy initiatives, developing common approaches remains problematic in the face of cultural, moral and legal diversity at the EU level, which has been shaped by historical, political and social experiences of wartime conflict. The individual Member States are in a much better position to decide how best to protect minors within their own society based upon the values, morality and

¹⁷⁶ See also in this context the EU Proposal for a Recommendation of the European Parliament and of the Council on the protection of minors and human dignity and the right of reply in relation to the competitiveness of the European audiovisual and information services industry, currently under consideration by the European Parliament.

¹⁷⁷ EC, *Commission, Proposal for a Directive of the European Parliament and of the Council amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities* COM(2005) 646 final.

¹⁷⁸ Scheduled broadcasts, the order of which the viewer cannot change.

¹⁷⁹ Audiovisual programmes available to the viewer on-demand (not scheduled by the broadcaster).

¹⁸⁰ *Supra* note 177, Articles 3c to 3h.

¹⁸¹ See EC, *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, [2000] O. J. L 178/1.

¹⁸² *Ibid.* See further *supra* note 177 at para. 10.

religion to which that particular society subscribes. If there is a “pressing social need”¹⁸³ to protect minors from harmful content, it should fall to the national authorities to make the initial assessment of whether that protection is best achieved through state regulation or if other alternatives should be considered. A fragmented approach to protection from harmful Internet content is unavoidable, though it has been suggested that “states within Western Europe should especially avoid pandering to the lowest common denominator where the least tolerant [such as in respect of racist expression in France¹⁸⁴ and in Germany¹⁸⁵] can set the pace.”¹⁸⁶ An agreement on these proposed provisions of the draft Television Without Frontiers Directive will be difficult to reach at the EU level, as the process faces many of the same drawbacks as the discussions around the draft Framework Decision on combating racism and xenophobia, resulting from different approaches to limitations on freedom of expression.

5. International Initiatives through the United Nations

A call for a study of the use of new technologies (including video games and computer networks) for the propagation of racial hatred and the urgent proposal of a set of internal and international measures to end such abuses were issued following the first European meeting of National Institutions for the Promotion and Protection of Human Rights in November 1994 and were to be considered by both the UN and the CoE Member States.¹⁸⁷ Further calls for research to consider whether international measures should be taken to control information transmitted over the Internet were made during 1996¹⁸⁸ with the recognition that “no national legislation has any power over this worldwide network”.¹⁸⁹

The availability of racist and xenophobic propaganda through electronic networks and the responsive measures to be taken at the national and international levels were considered during a UN seminar to assess the implementation of the

¹⁸³ See especially *Handyside v. United Kingdom*, judgment of 12 July 1976, App. No 5493/72, Series A no. 24, ECHR.

¹⁸⁴ *League Against Racism and Antisemitism*, *supra* note 59; Akdeniz, *supra* note 60.

¹⁸⁵ Criminal case of Somm, Felix Bruno, File No: 8340 Ds 465 JS 173158/95, Local Court (Amtsgericht) Munich. An English version of the case is available at <<http://www.cyber-rights.org/isps/somm-dec.htm>>.

¹⁸⁶ Clive Walker & Yaman Akdeniz, “The governance of the Internet in Europe with special reference to illegal and harmful content” (1998) Spec. Ed. (December) *Crim. L. Rev.* 5 at 14.

¹⁸⁷ See Glélé-Ahanhanzo, *supra* note 6.

¹⁸⁸ Secretary-General, *supra* note 7.

¹⁸⁹ *Ibid.* at para. 46.

ICERD in Geneva during September 1996.¹⁹⁰ In the course of the seminar, Rabbi Abraham Cooper stated that “online discussion or chat groups provided an opportunity to denigrate minorities, promote xenophobia and identify potential recruits for the racist groups”.¹⁹¹ The seminar participants felt that the UN is responsible for ensuring that modern communications technologies are not used to spread racism. The consensus was that an international approach would help overcome the problem created by legislative differences making it possible for racist material produced in countries with no legal sanctions against incitement of racial hatred to be made available in countries where those legal restrictions exist by means of the Internet. Cooperation with the Internet industry, especially with ISPs, was also encouraged. In addition, the participants recalled that article 4, paragraphs (a) and (b) of the ICERD contains the provisions on the basis of which States Parties can take legal measures to ban organizations involved in spreading racist propaganda over the Internet. The recommendations adopted by the seminar called on the UN, in particular its Legal Office, and other international and regional organizations to undertake a systematic review of existing international instruments with the view to assessing their applicability and adaptability to parallel forms of communication on the Internet.

The Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance noted in his 1997 report that “emphasis should be placed on the use of modern communications technology, including the Internet, as a vehicle for incitement to racial hatred and xenophobia”.¹⁹² The Special Rapporteur recommended joint action, research, and studies at an international level on the use of the Internet as a vehicle for racist propaganda.¹⁹³ The Special Rapporteur also welcomed the initiative taken by the General Assembly in its resolution 51/81,¹⁹⁴ whereby the Assembly recommended that a seminar be organized by the UN Centre for Human Rights (now the UN Office of the High Commissioner for Human Rights), in cooperation with the CERD, the UN Educational, Scientific and Cultural Organization (UNESCO), the International Telecommunication Union (ITU) and other relevant UN bodies, NGOs and ISPs, with a view to assessing the role of the Internet in light of the provisions of the ICERD.¹⁹⁵

¹⁹⁰ *Implementation of the Programme of Action for the Third Decade to Combat Racism and Racial Discrimination, Report of the United Nations seminar to assess the implementation of the International Convention on the Elimination of All Forms of Racial Discrimination with particular reference to articles 4 and 6, Commission on Human Rights, 53d Sess., UN Doc. E/CN.4/1997/68/Add.1 (1996).*

¹⁹¹ *Ibid.* at para. 60.

¹⁹² Glélé-Ahanhanzo, *supra* note 8 at para. 8.

¹⁹³ *Ibid.* at para. 132.

¹⁹⁴ *Third Decade to Combat Racism and Racial Discrimination*, GA Res. 51/81, UN GAOR, 51st Sess., UN Doc. A/RES/51/81 (1997) at para. 10.

¹⁹⁵ See generally Secretary-General, *Elimination Of Racism And Racial Discrimination: Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, UN GA, 52nd Sess., UN Doc. A/52/471 (1997).

The Office of the High Commissioner for Human Rights organized a seminar on “the role of the Internet in the light of the provisions of the International Convention on the Elimination of All Forms of Racial Discrimination” in Geneva, in November 1997.¹⁹⁶ The seminar concluded by strongly condemning the Internet’s use by some groups and persons to promote racism and hate speech in violation of international law.¹⁹⁷ The seminar further recommended that the Internet be used as an educative tool to combat racist propaganda, prevent the spread of racist doctrines and practices, and promote mutual understanding. The seminar also recommended that UN Member States continue their cooperation and establish international juridical measures in compliance with the ICERD to prohibit racism on the Internet while respecting individual rights, especially freedom of expression.

In his 1998 report, the Special Rapporteur noted that “although the States have now become aware of the dangers these acts represent, very few efforts have been made to combat the phenomenon,”¹⁹⁸ and that “only globally concerted action will be effective enough to halt the tendency to use the Internet for racist and xenophobic purposes, in view of the global, cross-frontier nature of that type of activity.”¹⁹⁹ The Special Rapporteur questioned whether it would be possible to adopt appropriate legislation, on a country-by-country basis, against incitement to hatred and racial discrimination, which would conform with articles 4 and 5 of the ICERD. In addition to taking possible legislative action, he also called upon the international community to undertake positive action to combat the abusive exploitation of the Internet on its own ground; that is, “by using the Internet itself to broadcast anti-racist and anti-xenophobic messages, and even to spread human rights education against racism.”²⁰⁰ In this respect, the CoE’s efforts were displayed in the launch of the European Commission against Racism and Intolerance website. In that same report, the Special Rapporteur once again recommended a consideration of possible action at the international level by immediately beginning studies, research and consultations on the use of the Internet for purposes of incitement of hatred, racist propaganda and xenophobia, as well as the creation of a program of human rights education and exchanges over the Internet on experiences in the struggle against racism, xenophobia and anti-Semitism.

¹⁹⁶ Maurice Glélé-Ahanhanzo, *Racism, Racial discrimination, xenophobia and related intolerance: Report of the UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance*, CHR Res. 1997/73, Commission on Human Rights, 54th Sess., UN Doc. E/CN.4/1998/79 (1998) at para. 23.

¹⁹⁷ *Racism, Racial Discrimination, Xenophobia and Related Intolerance: Report of the expert seminar on the role of the Internet in the light of the provisions of the International Convention on the Elimination of All Forms of Racial Discrimination*, Commission on Human Rights, 54th Sess., UN Doc. E/CN.4/1998/77/Add.2 (1998).

¹⁹⁸ *Supra* note 196 at para. 50.

¹⁹⁹ *Ibid.*

²⁰⁰ *Ibid.* at para. 51.

In 1999, the Commission on Human Rights, noting with concern the increase in the use of new communication technologies (in particular the Internet) to disseminate racist ideas and incite racial hatred, stated that the use of Internet technologies could contribute to combating racial discrimination and related intolerance through initiatives such as websites used to disseminate anti-racist and anti-xenophobic messages.²⁰¹ The Special Rapporteur suggested that the issue of Internet use in the dissemination of racism and xenophobia should be included in the agenda of the World Conference on Racism and Racial Discrimination, Xenophobia and Related Intolerance. In his 2000 report, the Special Rapporteur strongly recommended the holding of further consultations at the international level with a view to regulating the use of the Internet and harmonizing criminal legislation on use of the Internet for racist purposes.²⁰²

The work conducted by the UN High Commissioner for Human Rights led to the UN General Assembly, at the request of the UN Commission on Human Rights, to convene the third World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance which took place in Durban in 2001. The States participating in the World Conference adopted a Declaration and Programme of Action (Durban Declaration), containing recommendations intended to strengthen the international human rights framework for combating racism and related intolerance.

The Durban Declaration²⁰³ recognized “the positive contribution that the exercise of the right to freedom of expression, particularly by the media and new technologies, including the Internet, and full respect for the freedom to seek, receive and impart information can make to the fight against racism, racial discrimination, xenophobia and related intolerance”.²⁰⁴ However, the document also expressed deep concern with the use of new information technologies “for purposes contrary to respect for human values, equality, non-discrimination, respect for others and tolerance, including to propagate racism, racial hatred, xenophobia, racial discrimination and related intolerance, and that, in particular, children and youth having access to this material could be negatively influenced by it”.²⁰⁵ The Declaration explicitly recognized “the need to promote the use of new information and communication technologies, including the Internet, to contribute to the fight

²⁰¹ See Secretary-General, *Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, UN GA, 54th Sess., UN Doc. A/54/347 (1999).

²⁰² See Secretary-General, *Report of the Special Rapporteur of the Commission on Human Rights on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, UN GA, 55th Sess., UN Doc. A/55/304 (2000).

²⁰³ See generally *Report of the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance*, Durban, 31 August - 8 September 2001, UN Doc. A/CONF.189/12 (2002), online: United Nations <http://www.un.org/WCAR/aconf189_12.pdf> [Durban Declaration].

²⁰⁴ *Ibid.* at para. 90.

²⁰⁵ *Ibid.* at para. 91.

against racism, racial discrimination, xenophobia and related intolerance”²⁰⁶ and declared that “new technologies can assist the promotion of tolerance and respect for human dignity, and the principles of equality and non-discrimination”.²⁰⁷ Among other significant recommendations, the Durban Declaration urged States to:

implement legal sanctions, in accordance with relevant international human rights law, in respect of incitement to racial hatred through new information and communications technologies, including the Internet, and further urge[d] them to apply all relevant human rights instruments to which they are parties, in particular the International Convention on the Elimination of All Forms of Racial Discrimination, to racism on the Internet...²⁰⁸

The Durban Declaration also called upon the States to consider the following, while taking all necessary measures to guarantee the right to freedom of opinion and expression:

- (a) Encouraging Internet service providers to establish and disseminate specific voluntary codes of conduct and self-regulatory measures against the dissemination of racist messages and those that result in racial discrimination, xenophobia or any form of intolerance and discrimination; to that end, Internet providers are encouraged to set up mediating bodies at national and international levels, involving relevant civil society institutions;
- (b) Adopting and applying, to the extent possible, appropriate legislation for prosecuting those responsible for incitement to racial hatred or violence through the new information and communications technologies, including the Internet;
- (c) Addressing the problem of dissemination of racist material through the new information and communications technologies, including the Internet, *inter alia* by imparting training to law enforcement authorities;
- (d) Denouncing and actively discouraging the transmission of racist and xenophobic messages through all communications media, including new information and communications technologies, such as the Internet;
- (e) Considering a prompt and co-ordinated international response to the rapidly evolving phenomenon of the dissemination of hate speech and racist material through the new information and communications technologies, including the Internet; and in this context strengthening international co-operation.

²⁰⁶ *Ibid.* at para. 92.

²⁰⁷ *Ibid.*

²⁰⁸ *Ibid.* at para. 145.

(f) Encouraging access and use by all people of the Internet as an international and equal forum, aware that there are disparities in use of and access to the Internet;

(g) Examining ways in which the positive contribution made by the new information and communications technologies, such as the Internet, can be enhanced through replication of good practices in combating racism, racial discrimination, xenophobia and related intolerance;

(h) Encouraging the reflection of the diversity of societies among the personnel of media organizations and the new information and communications technologies, such as the Internet, by promoting adequate representation of different segments within societies at all levels of their organizational structure.²⁰⁹

In his 2002 report,²¹⁰ the Special Rapporteur expressed his hope that the concerned States and the international community will succeed in developing measures to nip this increasingly alarming phenomenon in the bud pursuant to the provisions of the Durban Declaration.²¹¹

In 2003 the UN General Assembly continued its condemnation of the misuse of print, audiovisual, electronic media, and the new communication technologies, to incite violence motivated by racial hatred, with a call for States to take all necessary measures to combat this form of racism in accordance with their commitments under the Durban Declaration,²¹² in accordance with existing international and regional standards of freedom of expression and taking all necessary measures to guarantee the right to freedom of opinion and expression.

In his 2003 report, the Special Rapporteur²¹³ commended the November 2002 CoE Council of Ministers on its adoption of the Additional Protocol to the Convention on Cyber-Crime concerning the Criminalisation of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems.²¹⁴ The Special Rapporteur expressed his hope for the emergence of a similar document at the international level in the form of an additional protocol to the ICERD, so that more States can adopt legal measures to combat the use of the Internet for racist or

²⁰⁹ *Ibid.* at para. 147.

²¹⁰ Secretary-General, *Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, UN GA, 57th Sess., UN Doc. A/57/204 (2002).

²¹¹ See Durban Declaration, *supra* note 203 at c. I, paras. 143-147.

²¹² Secretary-General, *The fight against racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action*, UN GA, 58th Sess., UN Doc. A/58/313 (2003).

²¹³ Note the change in Special Rapporteur: Mr. Doudou Diène (Senegal) replaced Mr. Maurice Glèlè-Ahanhanzo (Benin) (1993-2002) as of August 2002 (E/CN.4/RES/2002/68).

²¹⁴ See Secretary-General, *supra* note 212.

xenophobic purposes.²¹⁵ There was support for such a consideration from the UN General Assembly in 2004.²¹⁶ However, as mentioned previously, disagreements (especially between the United States and certain European countries) on the most appropriate strategy for preventing the dissemination of racist content on the Internet, including the need to adopt regulatory measures to that end, remains and these differences were highlighted by the Secretary-General report in September 2004.²¹⁷ These differences were also evident during the fourth session meetings of the UN Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action in Geneva in January 2006.²¹⁸ In the absence of global consensus and agreement on the limits of interference with freedom of expression, such an international instrument will be difficult to develop and implement.

6. Effectiveness of Regional and International Regulatory Efforts & Alternatives to State Legislation

Substantial international efforts such as the CoE's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems carry political significance; but will such legislative initiatives have an impact on reducing the problem of racist content on the Internet? Although State legislation is still a strong option and may be preferred in most instances, problems associated with the Internet may require the careful consideration of alternatives to State regulation. Due to the global and decentralized nature of the Internet, government regulation and even prosecutions may have limited effect and application especially if the racist content is transmitted from outside the jurisdiction in which it is considered illegal. As shown above, the reaction of the courts to prosecutions for racist content has been slow and problematic, hence the need to consider alternative and/or additional forms of regulation in this fight.

The steps taken by a number of governments at the national level have shown their limitations, and a regional international regulatory initiative such as the CoE Additional Protocol aimed at punishing racism on the Internet will have no effect unless every state hosting racist sites or messages is a party to the Additional Protocol.²¹⁹ The ratification process is a drawn out affair and it took over three years to bring the Protocol into force in March 2006 with only 10 States ratifying it so far. A considerable amount of time will be required to reach a substantial number of ratifications, though this is not unusual as the ratification of such instruments is a very long process at the Member States level. Even Germany, one of the main supporters of the Additional Protocol, has yet to ratify, and France only ratified the Protocol in early 2006.

²¹⁵ *Ibid.*

²¹⁶ See Secretary-General, *supra* note 14.

²¹⁷ *Ibid.* at para. 31.

²¹⁸ *Report of the Intergovernmental Working Group, supra* note 55.

²¹⁹ See *Explanatory Report, supra* note 1.

States such as the United Kingdom, Spain, Russia, Norway, Italy, Ireland, and Hungary have not yet signed the Additional Protocol and this only impedes the success of such a regional instrument. Member States may be reluctant to sign and/or ratify the Additional Protocol as such an action may require substantial changes to national laws. Speech restrictions may not be allowed by certain State constitutions, and the definition provided for “racist and xenophobic material” may conflict with the laws and constitutions of certain States. The offences included within the Additional Protocol, *inter alia*, dissemination of racist and xenophobic material, racist and xenophobic motivated threats, racist and xenophobic motivated insults, and the criminalisation of expressions which deny, grossly minimize, approve or justify acts constituting genocide or crimes against humanity, may not all be supported by the non-signing and non-ratifying Member States.

The reservations present in articles 3, 5, and 6 could also result in disparities between the parties to the Additional Protocol and harmonization may never take place in relation to both “racist and xenophobic motivated insults” (article 5), and “denial, gross minimisation, approval or justification of genocide or crimes against humanity” (article 6) as these two articles allow parties to the Protocol to reserve the right not to apply, in whole or in part, the offences provided therein. For example, within the CoE region, only Austria, Belgium, the Czech Republic, France, Germany, Lithuania, the Netherlands, Poland, Romania, Slovakia, Spain, and Switzerland, have laws criminalising the denial of genocide committed by the Nazis.²²⁰ Yet, “the proliferation of Holocaust Denial websites dramatically underscores the limitations of any national laws, or even international conventions, to eliminate or punish any form of hate speech”.²²¹ A similar reservation is also provided in relation to the “dissemination of racist and xenophobic material through computer systems” (article 3) but only so far as the dissemination is related to material which advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. It is also provided that a party may reserve the right not to apply the dissemination offence in article 3 to those cases of discrimination for which it cannot provide an effective remedy as a result of established principles in its national legal system concerning freedom of expression.

It is difficult to speculate how effective a regional international effort such as the CoE Additional Protocol will be. Even if all Member States of the CoE sign and ratify the Additional Protocol, the problems associated with racist Internet content will not disappear. Certain websites will continue to be hosted in the United States and other countries where the transmission of racist content is not criminalised.

²²⁰ See Council of Europe, *supra* note 47.

²²¹ Abraham Cooper & Harold Brackman, “Punishing Religious Defamation and Holocaust Denial: Is There a Double Standard?” *Equal Voices* Issue 18 (July 2006), online: EUMC <http://www.eumc.europa.eu/eumc/index.php?fuseaction=content.dsp_cat_content&catid=4498115372af1&contentid=44bb8bd0bd09f>.

This, in a sense, reflects the inherent risks of the Internet. The key question is how to manage these risks.

It is not suggested that nothing can be done to tackle the problem of racist content on the Internet; there are other options available to tackle such risks and problems in a global society than the development of international conventions and adoption of corresponding laws. The development of international agreements and their subsequent implementation at a national level is an incredibly slow and problematic process as witnessed by the implementation of the International Convention on the Elimination of All Forms of Racial Discrimination, the CoE's Cyber-Crime Convention, the limited implementation of the Additional Protocol to the Cyber-Crime Convention, and the UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

Regulation is often designed to reduce risk but alternative methods can be less costly, more flexible, adopted quicker and more effective than prescriptive government legislation. Such alternatives include: doing nothing; reliance on social norms; and support for self-regulation, co-regulation, or regulation through technical means, information, education and awareness campaigns.

In response to the issue of racism and xenophobia on the Internet, "doing nothing" is not a viable option given the extent and expanding nature of the problem. At the same time relying on social norms, customs and netiquette (essentially Internet customs) is also not a viable option as these are neither enforceable nor effective in a borderless, multi-national and multi-cultural environment.²²²

The Declaration on Freedom of Communication on the Internet adopted by the Committee of Ministers of the CoE on 28 May 2003 encouraged self-regulation and co-regulatory initiatives regarding Internet content. Similar recommendations were also made in a CoE Recommendation (2001)8 on self-regulation with respect to cyber-content.²²³ Within this context, the self-regulatory approaches adopted by the European Commission with its Action Plan on promoting safer use of the Internet should also be noted.

With self- and co-regulatory initiatives, States and international organizations can and should cooperate with NGOs and the private sector, as a "socially responsible private sector can help realize an Information Society that respects

²²² During the early days of the Internet, such norms and netiquette were observed by the Internet community through peer pressure, but with the growth of the Internet such rules have become largely inefficient. See Eduardo Gelbstein & Jovan Kurbalija, *Internet Governance: Issues, Actors, and Divides* (Malta: DiploFoundation, 2005) at 71, online: DiploFoundation <<http://www.diplomacy.edu/isl/ig/>>.

²²³ Council of Europe, *Recommendation* (2001) 8.

human rights.”²²⁴ This multi-actor approach²²⁵ is supported by the Durban Declaration which encouraged the private sector to promote the development of voluntary ethical codes of conduct, self-regulatory measures, policies, and practices aimed at combating racism and related intolerance.²²⁶

The proceeding section provides a critical analysis of alternative means of combating racist Internet content including self-regulation by ISPs, co-regulatory initiatives of Internet Hotlines, and regulation through code, and technical means.

7. Self and Co-Regulatory Initiatives

(A) *The Role of Internet Service Providers*

Close cooperation and interaction with the industry, and in particular, internet service providers is absolutely necessary in order to find solutions that are not only juridically sound but also technically achievable.²²⁷

Illegal content must be dealt with at its source by law enforcement agencies, and their activities are covered by the rules of national law and agreements of judicial cooperation. Nevertheless, ISPs can help in reducing circulation of illegal content through properly-functioning systems of self-regulation (such as codes of conduct and the establishment of hotlines) in compliance with and supported by the legal system.

Technically, Internet access is not possible without the services of an ISP, making the role of the ISP a pivotal one. Content regulation is the most politically prominent aspect of Internet regulation in relation to ISPs; although no ISP controls third party content, their crucial role in providing Internet access makes them visible targets for those seeking content control.

In broad terms, ISPs are neither guardians nor guarantors of Internet content, and are therefore not liable to assess, classify or filter any third party content before its transmission. Moreover, “consideration should be given to the fact that ISPs are

²²⁴ Office of the High Commissioner for Human Rights, *Background Note on the Information Society and Human Rights*, UN Doc. WSIS/PC-3/CONTR/178-E (2003).

²²⁵ See Jane Bailey, “Strategic Alliances: The Inter-related Roles of Citizens, Industry and Government in Combating Internet Hate” in *Hate on the Net* (Ottawa: Association for Canadian Studies, Spring 2006) 56, online: Canadian Human Rights Commission <http://www.chrc-ccdp.ca/pdf/hateoninternet_bil.pdf>; see also Jane Bailey, “Private Regulation and Public Policy: Toward Effective Restriction of Internet Hate Propaganda” (2004) 49 McGill L.J. 59.

²²⁶ Durban Declaration, *supra* note 203 at para. 144.

²²⁷ Council of the European Union, *Conclusions of the first High Level Political Dialogue on Counter-Terrorism between the Council, the Commission, and the European Parliament*, JAI 240, 9246/06, Brussels, (18 May 2006).

technical in nature and lack the capacities to determine whether material on the Internet is illegal or harmful.”²²⁸ Several technical factors also prevent an ISP from blocking the free flow of information on the Internet. First, an ISP cannot easily stop the incoming flow of material to its servers; no one can monitor the enormous quantity of network traffic, which may consist of hundreds of thousands of e-mails, newsgroup messages, files, and web pages that pass through in dozens of text and binary formats, some of them readable only by particular proprietary tools. ISPs do have a limited technical ability to detect and control content, but in most cases it would be impossible for a single ISP to judge whether this enormous amount of material contains content that is illegal under the laws of the country of service. In fact, article 15 of the EU Directive on Electronic Commerce²²⁹ prevents Member States from imposing a general monitoring obligation on service providers for actively seeking facts or circumstances indicating illegal activity on their servers.²³⁰

While a general monitoring obligation cannot be imposed upon ISPs, this does not prevent states from issuing blocking orders. In early 1996, Deutsche Telekom blocked users of its subsidiary T-Online computer network from accessing Internet sites used to spread anti-Semitic propaganda. Deutsche Telekom was responding to demands by Mannheim prosecutors who were investigating Ernst Zündel and his Toronto-based *ZundelSite*.²³¹ This initial attempt to block access to Zündel’s website resulted in the controversial material being copied and mirrored all over the Internet.²³² In 2002, North Rhine Westphalia, Germany’s most populous state, issued a blocking order to prevent German-based ISPs from providing access to websites based outside of Germany (mainly in the U.S.) that host racist and neo-Nazi content.²³³ Prior to the issuing of the blocking order, the Dusseldorf District Authority President Jurgen Bussow wrote to four U.S. ISPs in August 2000 requesting that they prevent access to four websites containing racist neo-Nazi

²²⁸ Report of the Intergovernmental Working Group, *supra* note 55 at para. 47.

²²⁹ Directive 2000/31/EC, *supra* note 181. See also EC, *Common Position (EC) No 22/2000 of 28 February 2000 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a Directive of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce)* [2000] O.J. C 128/32. Member States had until January 2002 to implement the Directive into national law. See generally EC, *Commission, First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)*, COM(2003) 702 final.

²³⁰ However, article 15 does not prevent public authorities from imposing a monitoring obligation in a specific and clearly defined individual case.

²³¹ See “German Service Cuts Net Access” *San Jose Mercury News* (January 27, 1996).

²³² See further Yaman Akdeniz, “To Link or Not to Link: Problems with World Wide Web Links on the Internet” (1997) 11:2 *Int’l Rev. L. Comp. & Tech* 281. See further Institute for Jewish Policy Research and American Jewish Committee, *Antisemitism World Report 1997*.

²³³ See “Ban On Neo-nazi Web Content In German State Upheld” *National Journal’s Technology Daily [Washington]* (22 December 2004).

material. As this action was unsuccessful, Bussow issued the blocking order²³⁴ which affected approximately 76 ISPs within that region.²³⁵ Despite numerous legal cases and appeals surrounding the blocking orders, a number of administrative courts have ruled that German authorities can continue to ask ISPs to block such pages.

A similar attempt in France to block access to the <Front14.org> portal²³⁶ and the racist sites it hosted for free was unsuccessful in 2001. *J'accuse!*, an association aimed at eradicating racism on the Internet, sued 14 major French ISPs²³⁷ and although the court agreed that the racist portal violated French law, it did not require ISPs to block access to the portal.²³⁸ But in June 2005, a Paris court ordered French ISPs to block access of French viewers to the website of the French revisionist organization Association of Former Connoisseurs of War and Holocaust Stories (AAARGH).²³⁹ Two U.S.-based ISPs have since also agreed to stop hosting AAARGH's website.

²³⁴ See generally Eric T. Eberwine, "Sound and Fury Signifying Nothing?: Jurgen Bussow's Battle Against Hate-Speech on the Internet" (2004) 49 N.Y.L. Sch. L. Rev. 353; and Christopher D. Van Blarcum, "Internet Hate Speech: The European Framework and the Emerging American Haven" (2005) 62 Wash & Lee L. Rev. 781.

²³⁵ Between 2002 and 2004 the Duesseldorf District Administration issued 90 ordinances against Internet providers in North Rhine-Westphalia, forcing them to block access to certain websites with rightwing extremist content. See U.S. Bureau of Democracy, Human Rights, and Labor, *Report on Global Anti-Semitism* (January 2005) online: <<http://www.state.gov/g/drl/rls/40258.htm>>. See also Secretary-General, *Combating racism, racial discrimination, xenophobia and related intolerance and comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action*, UN GA, 59th Sess., UN Doc. A/59/330 (2004).

²³⁶ The <Front14.org> website had the following disclaimer:

Only front 14 offers free web hosting and e mail exclusively to racialsists. Join today. Many White people don't have the time and energy to put into hosting their own domain, so they join Geocities, Angelfire, etc, in an attempt to get their voices heard. But these "free" services (who bombard you with ads) have adopted an aggressive anti-White policy. We decided to provide an alternative to proud White men and women, one that would be for our White interests only. Join.

²³⁷ In the course of 1996, the four principal network providers in France (Imagnet, Calvacon, Internetway and Internet France) blocked access to fourteen discussion forums of French antisemitic and Holocaust-denying propaganda, advertisements for Nazi memorabilia and banned literature. In March 1997, the UEJF took out a court injunction against nine network providers guilty of transmitting Holocaust-denial material. It was the country's first Internet trial. No penalty has been announced, but the network providers have been ordered to revise contracts to ensure that racist and Holocaust-denial propaganda is removed from the sites on which they appear. See Institute for Jewish Policy Research and American Jewish Committee, *Antisemitism World Report 1997*.

²³⁸ Trib. gr. inst. Paris, ordonnance de référé, 30 October 2001, online : <<http://www.foruminternet.org/telechargement/documents/tgi-par20011030.pdf>>. See generally Benoit Frydman & Isabelle Rorive, "Regulating Internet Content through Intermediaries in Europe and the USA" (2002) 23 *Zeitschrift für Rechtssoziologie* Heft 1, S. 41-59, online: Max Planck Institute <http://www.isys.ucl.ac.be/etudes/cours/linf2202/Frydman_&_Rorive_2002.pdf>.

²³⁹ See U.S. Bureau of Democracy, *Human Rights, and Labor, International Religious Freedom Report 2005 - France*, online: U.S. Department of State <<http://www.state.gov/g/drl/rls/irfi/2005/51552.htm>>.

Interestingly, in March 2006, the Pakistan Supreme Court ordered the government to block Internet sites displaying blasphemous cartoons depicting the Prophet Mohammad that were originally published in the Danish daily newspaper *Jyllands-Posten* on 30 September 2005.²⁴⁰ In the Court's notice to the Pakistan Telecommunication Authority, Chief Justice Iftikhar Muhammad Chaudhry said that they "will not accept any excuse or technical objection on this issue because it relates to the sentiments of the entire Muslim world."²⁴¹ The blocking involved all websites that carried the controversial cartoons including the popular weblog domain <blogger.com>.²⁴² Some governments and state regulators may not always agree with blocking, and in August 2006, the Canadian Radio-Television and Telecommunications Commission (CRTC) refused to authorize the blocking by Canadian ISPs of two U.S. neo-Nazi websites that published the personal contact information of Canadian lawyer and human rights activist Richard Warman.²⁴³ The publication of Warman's personal details resulted in death threats which in turn lead him to ask the Canadian ISPs to block access to the websites; they refused to do so in the absence of an order from the CRTC. The Commission published its decision in a letter stating that it would be inappropriate to order blockage of the particular websites without affording Canadian ISPs and all other interested parties an opportunity for comment.²⁴⁴

As racist websites and organizations seem to find refuge in the United States, where they benefit from the protection offered by the First Amendment, the utility and effectiveness of various blocking or removal orders around the globe remains to be seen. However, in the case of <Redwatch.info>, the website of the Polish wing of the neo-fascist Blood and Honour organization, the Federal Bureau of Investigation (FBI) contacted the hosting company in Arizona which decided to remove the website from its server.²⁴⁵ <Redwatch.info> published blacklists of Polish gays, feminists and left-wing sympathizers, including personal information such as their names, photos, and in some cases their addresses, phone numbers, and

²⁴⁰ See "Supreme Court directs strict steps for banning blasphemous web-sites" *The Pakistan Newswire* (2 March 2006); "Pakistan Blocks Anti-President, 'Blasphemous' Blogs" *BBC Monitoring International Newswire* (6 March 2006).

²⁴¹ *Ibid.*

²⁴² See "Web Sites Carrying Blasphemous Images Blocked, Supreme Court Told" *Pakistan Press International* (20 March 2006); and "SC orders case against cartoon publishers" *Daily [Pakistan] Times* (18 April 2006).

²⁴³ See "Ottawa lawyer loses CRTC bid to block access to U.S. website: Neo-Nazis calling for man's death" *Ottawa Citizen* (27 August 2006). The websites in question were <<http://www.overthrow.com>> and <<http://dossiernoir.blogspot.com>>.

²⁴⁴ Letter from Canadian Radio-television and Telecommunications Commission to J. Edward Antecol (24 August 2006), CRTC File No: 8622-P49-200610510, online: CRTC <<http://www.crtc.gc.ca/archive/ENG/Letters/2006/lt060824.htm>>. See further Michael Geist, "Content blocking a can of worms that must be opened" *The Toronto Star* (28 August 2006).

²⁴⁵ See "Polish police, US FBI block neo-Nazi website" *Agence France Presse* (06 July 2006).

car registration numbers. Polish police asked the FBI for assistance in May 2006, following a knife attack in Warsaw on a Jewish human rights activist who was named on the website. Several journalists with left-leaning political affiliations who were named on the website were also threatened.

Nevertheless, even when responsible U.S. hosting companies agree to remove racist websites from their servers, hosting for those sites is still available through specialized companies such as NSM88 Network, a design network initiated and maintained by America's Nazi Party. In fact, when *nukeisrael.com* was removed from the servers of a Toronto-based Canadian ISP called *<Canaca.com>* in May 2005, the site was simply moved to the NSM88 Network.²⁴⁶

(B) Notice and Takedown Procedures

While ISPs ought to provide reasonable assistance to authorities investigating criminal activity, it is incumbent on law enforcement bodies, and not ISPs, to initiate and pursue policing action. ISPs should also ensure that proper authorization (such as by judicial warrant) is obtained for policing interventions. The above mentioned EU Directive on Electronic Commerce provides a notice-based liability for ISPs for hosting illegal content. According to the Directive, "upon obtaining actual knowledge...of illegal activities [service providers] ha[ve] to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level".²⁴⁷ Under the Directive, "notice" has to be specific and may be given by an individual complainant or by a self-regulatory hotline. In some States the notice may be given by law enforcement agencies or provided through court orders.

The concept of notice-based liability is emerging in relation to other types of content including terrorism related materials over the Internet.²⁴⁸ An example is the British government's proposed criminalisation of the encouragement of terrorism and the dissemination of terrorist material through the Internet following the July 2005 terrorist attacks in London.²⁴⁹ The *Terrorism Act 2006*, which came into force

²⁴⁶ See League for Human Rights of B'nai Brith Canada, *2005 Audit of Antisemitic Incidents 2005* (2006), online: B'nai Brith Canada <<http://www.bnaibrith.ca/audit2005.html>>.

²⁴⁷ *Directive 2000/31/EC*, *supra* note 181 at para. 46.

²⁴⁸ See for example Brynjar Lia, "Al-Qaeda online: understanding jihadist internet infrastructure" in *Jane's Intelligence Review* (1 January 2006), online: <http://www.mil.no/multimedia/archive/00075/Al-Qaeda_online__und_75416a.pdf>.

²⁴⁹ But note the human rights considerations, especially in relation to freedom of expression: ODIHR, *Background Paper on Human Rights Considerations in Combating Incitement to Terrorism and Related Offences* (2006), online: OSCE <http://www.osce.org/documents/odihr/2006/10/21814_en.pdf>.

in March 2006, contains provisions criminalizing the encouragement of terrorism²⁵⁰ and the dissemination of terrorist publications.²⁵¹ The *Act* also includes notice and takedown provisions if the encouragement or dissemination takes place over the Internet.²⁵² Hazel Blears, the Minister of State for the Home Office, explained that the intention behind section 3 is “to provide a method by which webmasters could be made aware of content on their websites; thus ensuring that they could not claim not to have known about it if they were subsequently prosecuted.”²⁵³

It is important to note the different approach adopted in the United States to ISP liability. While a notice-based liability policy seems to be preferred in Europe, American ISPs have more protection from liability for third party content regardless of their “knowledge” of it. In the United States, section 230(c)(1) of the *Communications Decency Act* provides 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.”²⁵⁴ Section 230 was considered and tested by the Fourth Circuit Court of Appeals in *Zeran v. America Online Inc.*, a defamation case where the Court held that “by its plain language, section 230 created a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.”²⁵⁵ Nor did the fact that the provider had notice of the transmission of wrongful material prevent the operation of this immunity in *Zeran*. However, it should be noted that the *Zeran*

²⁵⁰ *Terrorism Act 2006* (U.K.), 2006, c. 11, s. 1: “This section applies to a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism...”

²⁵¹ *Ibid.* s. 2(2): dissemination of terrorist publications includes: distributing or circulating a terrorist publication; giving, selling, or lending such a publication; offering such a publication for sale or loan; providing a service to others that enables them to obtain, read, listen to or look at such a publication, or to acquire it by means of a gift, sale or loan; transmitting the contents of such a publication electronically.

²⁵² *Ibid.* ss. 3, 4.

²⁵³ U.K., H.C., *Parliamentary Debates*, vol. 442, col. 1471 (15 February 2006).

²⁵⁴ *Communications Decency Act*, 47 U.S.C. (1996). Section 230(e)(2) defines “interactive computer service” as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions”. Section 230(e)(3) defines “information content provider” as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service”. See however, the different policy established for copyright infringement with the passage of the *Digital Millenium Copyright Act of 1998*, Pub. L. No. 105-304, 112 Stat. 2860.

²⁵⁵ *Zeran v. America Online Inc.*, 129 F.3d 327 at 330 (4th Cir. 1997), *certiorari* denied, 48 S. Ct. 2341 (1998). The plaintiff’s claim, which arose out of a false bulletin board posting that the plaintiff was selling t-shirts with offensive messages about the Oklahoma City bombing, was framed as one for negligence in failing to remove the posting, but the court said that the allegations were in substance indistinguishable from a “garden variety defamation action”: 129 F.3d 327 at 332.

decision is often criticized²⁵⁶ and in his dissent in *Doe v. America Online, Inc.* Lewis J. wrote that “the so-called ‘Decency Act’ has, contrary to well-established legal principles, been transformed from an appropriate shield into a sword of harm and extreme danger which places technology buzz words and economic considerations above the safety and general welfare of our people.”²⁵⁷ Yet, in *Batzel v. Smith*,²⁵⁸ the U.S. Court of Appeals for the Ninth Circuit re-emphasized that “in insulating Internet service providers from liability for certain content published on their sites, [Congress] recognised the importance of protecting the unfettered and unregulated development of free speech on the Internet.”²⁵⁹ Although the *Zeran* decision remains the authority on ISP liability, “whether or not that is a desirable state of affairs is of course a matter for debate”.²⁶⁰ Section 230 and the protection it offers to U.S. ISPs remains the current law in the United States.

(C) Hotlines for Reporting Illegal Activity

Some ISPs and/or their trade associations, especially in the Western world, have developed hotlines to report illegal Internet content. Most of the current Internet hotlines are run privately by industry-based organizations and in many countries they are funded by ISPs. They may constitute centres of expertise providing guidance to ISPs as to what content might be illegal.²⁶¹

Internet hotlines usually allow members of the public to report illegal Internet content that often takes the form of child pornography but some hotlines deal with other forms of illegality including racist material.²⁶² In most cases, the hotline will assess the report and if the reported content is deemed illegal by the hotline operator, it is then reported to the ISPs, the police and to a corresponding hotline (if one exists) when the content is hosted in a different jurisdiction. Upon receipt of the notice, ISPs will generally remove the reported illegal content from their servers.

There is international cooperation between various hotlines, and the Internet Hotline Providers in Europe Association (INHOPE) has been set up to facilitate and

²⁵⁶ See for example *Doe v. GTE Corp.*, 347 F.3d. 655 (7th Cir. 2003) (held *Zeran* was flawed). See also *Barrett v. Rosenthal*, 9 Cal. Rptr. 3d 142 at 154 (C.A. 2004). See further David A. Myers, “Defamation and the Quiescent Anarchy of the Internet: A Case Study of Cyber Targeting” (2006) 110 Penn St. L. Rev. 667.

²⁵⁷ *Doe v. America Online Inc.*, 783 So. 2d 1010 (Fla. Sup. Ct. 2001), Lewis J., dissenting.

²⁵⁸ *Batzel v. Smith*, 333 F.3d 1018 at 1027 (9th Cir. 2003) quoted in *Yahoo*, *supra* note 68.

²⁵⁹ *Ibid.*

²⁶⁰ See generally Yaman Akdeniz & Horton Rogers, “Defamation on the Internet” in Yaman Akdeniz *et al.*, eds., *The Internet, Law and Society* (Essex: Longman, 2000) at 294-317.

²⁶¹ See *Decision No 854/2005/EC*, *supra* note 175.

²⁶² During 2004, the Austrian Ministry of the Interior’s Internet hotline for reporting National Socialist activity received 140 reports of right-wing extremist activity, particularly in connection with the Internet. See U.S. Bureau of Democracy, Human Rights, and Labor, *Report on Global Anti-Semitism*, online: U.S. Department of State, at <<http://www.state.gov/g/drl/rls/40258.htm>>.

co-ordinate the work of internet hotlines in responding to illegal Internet content.²⁶³ INHOPE currently has 18 full members,²⁶⁴ and 7 provisional members.²⁶⁵

While most hotlines do have expertise in dealing with child pornography, the same may not be said for racist content; this type of content is predominantly text-based and in most cases assessing the racist nature of a publication may not be as straightforward as identifying child pornography. However, expertise and specialized hotlines do exist in Europe, and it is worth mentioning the International Network Against Cyber Hate (INACH)²⁶⁶ which acts as an umbrella organization for hotlines specializing in racist content.²⁶⁷ INACH was set up in 2002 by the Magenta Foundation, the Dutch Complaints Bureau for Discrimination on the Internet and by <Jugendschutz.net> in Germany.²⁶⁸ The work of both the Dutch and the German hotlines is noteworthy in this field and the Dutch hotline received a total of 5,825 complaints about racist content between 1997 and 2003.²⁶⁹ In 2002, of the 1,798 reported expressions, 1,619 originated in the Netherlands, and 1,238 were deemed illegal following the hotline's own assessment. In 881 cases, the Dutch hotline asked that the content in question be removed, and was successful in 557 instances.²⁷⁰ In 2003 alone, the hotline dealt with 1,496 reported expressions; 797 of these were deemed illegal and the hotline was successful in the removal of 624 expressions of the 655 instances reported to the authorities.²⁷¹ Jugendschutz.net's activities resulted in action against 184 illegal extreme right-wing websites in 2003.²⁷² In 154 instances, websites were blocked or illegal portions were removed

²⁶³ INHOPE is a project under the EC Daphne Programme to encourage co-operation between European Internet Hotline providers to reduce the level of child pornography on the Internet. For details see <<http://www.inhope.org/>>. Some but not all of the members of INHOPE deal with racist Internet content, namely members from Austria, France, Germany, Greece, Ireland, UK, and Spain.

²⁶⁴ From Australia, Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Netherlands, South Korea, Spain, Taiwan, United Kingdom and the United States.

²⁶⁵ From Brazil, Canada, Cyprus, Greece, Hungary, Lithuania, and Poland.

²⁶⁶ See <<http://www.inach.net/>>. See also INACH, *Antisemitism on the Internet* ed. by Suzette Bronkhorst & Ronald Eissens (2004), online: <<http://www.inach.net/content/INACH - Antisemitism on the Internet.pdf>>; and INACH, *Hate on the Net – Virtual nursery for in Real Life crime* (2004), online: <<http://www.inach.net/content/inach-hateonthenet.pdf>>.

²⁶⁷ INACH members are based in Canada, Denmark, France, Germany, Latvia, Moldova, The Netherlands, Poland, Russia, Slovakia, Spain, Sweden, the United Kingdom and the United States.

²⁶⁸ See the *INACH 2005 Annual Report*, online: <<http://www.inach.net/content/INACH-annual-report-2005.pdf>>.

²⁶⁹ *Ibid.*

²⁷⁰ Magenta Foundation, Complaints Bureau for Discrimination on the Internet, *Meldpunt Discriminatie Internet, Annual Report 2002* (Amsterdam: Stichting Magenta, 2003), online: INACH <<http://www.inach.net/content/MDI-annual-report-2002.pdf>>.

²⁷¹ Magenta Foundation, Complaints Bureau for Discrimination on the Internet, *Meldpunt Discriminatie Internet, Annual Report 2003* (Amsterdam: Stichting Magenta, 2004), online: INACH <<http://www.inach.net/content/MDI-annual-report-2003.pdf>>.

²⁷² Jugendschutz.Net, *Annual Report 2003: Right-Wing Extremism on the Internet*, online: INACH <<http://www.inach.net/content/annual-report-jugendschutznet-2003.pdf>>.

from the Internet; 107 of those sites were German, while 47 were foreign.²⁷³ In 2004, a further 131 websites were either blocked or removed by the German hotline.²⁷⁴

Hotlines may not always be in a position to judge the suitability or illegality of this type of Internet content, and they are in fact often criticized as serious concerns remain about the policing role that such organizations inevitably play. Many maintain that decisions involving illegality should be decided by courts of law rather than hotline operators. It has been argued that “these hotlines violate due process concepts that are also enshrined in international, regional, and national guarantees around the world”.²⁷⁵

While it may be tempting to identify and attempt to block content posted to particular newsgroups, websites, or other Internet forums, that seems devoted to illegality, such measures could set dangerous precedents if hotlines assume the role of the courts. Over time, such an approach could result in a form of privatized censorship with no limit on its application. Although hotlines could play an important role in regulating illegal Internet content, there remain significant questions about their operation. As the Martabit report to the UN stated “while encouraging these initiatives, States should ensure that the due process of law is respected and effective remedies remain available in relation to measures enforced.”²⁷⁶

(D) Self-Regulation Through Code: Rating and Filtering Systems

The development of rating and filtering systems has been encouraged since the mid-1990s to deal with harmful Internet content as a means of user empowerment. Such tools are “promoted in order to enable users to make their own decisions on how to deal with unwanted and harmful content”.²⁷⁷ Rating systems, such as the Platform for Internet Content Selections (PICS),²⁷⁸ work by embedding electronic labels into

²⁷³ Jugendschutz.Net, *Chart of illegal and blocked websites containing right-wing extremism 2003*, online: INACH <http://www.inach.net/content/jugendschutz_figures_2003.pdf>.

²⁷⁴ Jugendschutz.Net, *'Right-wing Extremism on the Internet' - successful strategies against Online-Hate: 2004 Annual Report*, online: INACH <<http://www.inach.net/content/jgs-annual-report2004.pdf>>.

²⁷⁵ American Civil Liberties Union, Press Release, “ACLU Joins International Protest Against Global Internet Censorship Plans” (9 September 1999), quoting ACLU President Nadine Strossen, online: ACLU <<http://www.aclu.org/intlhumanrights/gen/13778prs19990909.html>>.

²⁷⁶ *Report of the Intergovernmental Working Group*, *supra* note 55 at para. 47.

²⁷⁷ The EU Safer Internet *plus* Programme, from *Decision No 854/2005/EC*, *supra* note 175; online: Safer Internet <http://europa.eu.int/information_society/activities/sip/programme/index_en.htm>.

²⁷⁸ Note also the ICRA (Internet Content Rating Association) system which follows from the RSACi system; see <<http://www.icra.org/>>.

web documents to vet their content before a computer displays them.²⁷⁹ The vetting system could include political, religious, advertising or commercial topics that can be added either by the publisher of the material or by a third party (e.g. an ISP or an independent vetting body). In addition to the rating systems, several filtering software packages are also available in response to the wishes of parents making decisions about what their children can access at home. The type of harmful, offensive, disturbing, shocking, unwanted or undesirable content that is blocked by various filtering software usually includes: sexually explicit material; graphically violent material; content advocating hate; and content advocating illegal activity such as drug use, bomb-making, or underage drinking and gambling.

There are approximately 50 filtering products (mainly U.S.-based) currently available, and roughly 40 of these block content that advocates or promotes hatred and discrimination.²⁸⁰ For a long time, filtering software was seen as a preferable alternative to government legislation, including by the U.S. Supreme Court,²⁸¹ and it has been stated that "promoting filter use does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished."²⁸² It was argued that filters might well be more effective than certain legislation and imposing selective restrictions on speech at the receiving end would prevent universal restrictions at the source level. It was, however, acknowledged by the Supreme Court that "filtering software is not a perfect solution because it may block some materials not harmful to minors and fail to catch some that are".²⁸³

It is important to note the limitations and criticisms related to rating and filtering systems. Neither system offers total protection to citizens or addresses content-related problems in full. The key limitations are highlighted below.

i. Limited Functionality of Rating Systems

Although various governments have welcomed the use and development of rating systems, the capacity of these tools is limited to certain parts of the Internet. Rating systems are designed for World Wide Web sites while excluding other Internet-related communication forums such as chat environments,²⁸⁴ file transfer protocol

²⁷⁹ See Computer Professionals for Social Responsibility, *Filtering FAQ*, online: <<http://quark.cpsr.org/~harryh/faq.html>>. Note that most filtering systems based on third-party rating, such as CyberPatrol, are compliant with the PICS labelling system.

²⁸⁰ For a partial list, see <<http://kids.getnetwise.org/tools/index.php>>.

²⁸¹ *Reno v. ACLU*, 117 S. Ct. 2329 (1997).

²⁸² *Ashcroft v. ACLU*, 542 U.S. 656 (2004) at 696.

²⁸³ *Ibid.*

²⁸⁴ Interactive environments, like chat channels, cannot be rated as the exchange and transmission of information takes place live and spontaneously.

servers (ftp),²⁸⁵ peer-to-peer networks (p2p), Usenet discussion groups, real-audio and real-video systems (which can include live sound and image transmissions), and finally the ubiquitous e-mail communication. These cannot be rated with the systems that are currently available and therefore the assumption that rating systems would make the Internet a “safer environment” is false as World Wide Web content represents only a fraction of the whole of the Internet; it may be argued that it is the most fanciful and rapidly growing fraction, but problems such as racism are not unique to the World Wide Web. The development of rating systems has been gradual and it does not seem realistic to expect that they will ever be widely used.

ii. Third Party Systems and Problems with Accountability

If the duty of rating is handed to third parties, this could cause problems for freedom of speech and with few third-party rating products currently available, the potential for arbitrary censorship increases. This would leave no scope for argument and dissent because the ratings would be done by private bodies without any “direct” government involvement. So far this has not been the case, but as self-rating is not booming, from time to time third party rating systems are considered.

iii. Defective Systems

Another downside of relying on such technologies is that these systems can lead to restrictions on access to socially useful websites and information.²⁸⁶ It has been reported many times that filtering systems and software can be over-inclusive, limiting access to and censoring inconvenient websites,²⁸⁷ as well as filtering potentially educational materials regarding AIDS, drug abuse prevention and teenage pregnancy. According to the report on Internet Filters by the National Coalition Against Censorship:

- I-Gear blocked an essay on “Indecency on the Internet: Lessons from the Art World”, the United Nations report “HIV/AIDS: The Global Epidemic”, and the home pages of four photography galleries.
- Net Nanny, SurfWatch, Cybersitter, and Bess, among other products, blocked House Majority Leader Richard “Dick” Armey’s official website upon detecting the word “dick”.

²⁸⁵ It is estimated there are nearly a million ftp servers accessible via the Internet; some of these online libraries may have offensive content or legal content that may be considered harmful for children.

²⁸⁶ See Electronic Privacy Information Center, *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet* (Washington, 1997), online: EPIC <<http://www2.epic.org/reports/filter-report.html>>. See generally <<http://www.peacefire.org>> as well as Seth Finkelstein, *Anticensorware Investigations – Censorware Exposed*, online: Seth Finkelstein <<http://sethf.com/anticensorware/>>.

²⁸⁷ Gay & Lesbian Alliance Against Defamation, *Access Denied: The Impact of Internet Filtering Software on the Lesbian and Gay Community* (New York, 1997), online: GLAAD <http://www.glaad.org/glaad/access_denied/index.html>.

- SmartFilter blocked the Declaration of Independence, Shakespeare's complete plays, *Moby Dick*, and *Marijuana: Facts for Teens*, a brochure published by the National Institute on Drug Abuse (a division of the National Institute of Health).
- SurfWatch blocked human rights sites like the Commissioner of the Council of the Baltic Sea States and Algeria Watch, as well as the University of Kansas' Archie R. Dykes Medical Library (upon detecting the word "dykes").
- X-Stop blocked the National Journal of Sexual Orientation Law, Carnegie Mellon University's Banned Books page, "Let's Have an Affair" catering company, and, through its "foul word" function, searches for *Bastard Out of Carolina* and "The Owl and the Pussy Cat".²⁸⁸

At the same time some filtering software has been criticized for under-blocking.²⁸⁹ In general, there is too much reliance on mindless mechanical blocking through identification of key words and phrases. Moreover, this is usually based on the morality to which a particular company or organization is committed to in developing their filtering criteria and databases. Broad and varying concepts of offensiveness, inappropriateness, or disagreement with the political viewpoint of the manufacturer are seen in the use of such tools. Most of the companies creating this kind of software provide no appeal mechanism²⁹⁰ to content providers who are banned or blocked, thereby "subverting the self-regulating exchange of information that has been a hallmark of the Internet community".²⁹¹

iv. Circumvention is Possible

Apart from the worrying defects explained above, circumvention of such tools is also relatively easy. There is not only the often-cited example of children uninstalling or removing such software from their computers, but also a piece of software known as *Circumventor*, developed by Peacefire.org which bypasses any

²⁸⁸ Marjorie Heins & Christina Cho, *Internet Filters: A Public Policy Research* (2001), online: National Coalition Against Censorship <<http://www.ncaac.org/issues/internetfilters.html>>.

²⁸⁹ At one time, WebSense published a daily list of sexually explicit websites to show which websites its competitors did not block. Anybody - including students from schools that were using SmartFilter and SurfControl - could access the list, however, simply by clicking a button on the WebSense site agreeing that they were over the age of 18. See Peacefire's report on Websense at <<http://peacefire.org/censorware/WebSENSE/>>.

²⁹⁰ Some companies provide a review mechanism and others let their databases be searched online, but in most cases, without testing the software itself, an online content provider would not know if its webpage was being blocked by the filtering software. Considering the number of such software products, it is an impossible task to find whether one blocks a certain website and for what reason.

²⁹¹ Letter from Computer Professionals for Social Responsibility to Solid Oak, makers of CyberSitter (18 December 1996) online: CPSR <<http://www.cpsr.org/cpsr/nii/cyber-rights/>>.

content-blocking attempts, including those by the likes of CyberSitter and NetNanny.²⁹² One of the main motivations for developing *Circumventor* was Peacefire.org's desire to bypass censorship of political websites. It is a well-known fact that almost all Internet users in China²⁹³ and the Middle East²⁹⁴ are prevented from accessing a considerable number of political websites. Technologies like *Circumventor* can help Internet users in censored countries to access such websites. In addition to *Circumventor*, websites providing anonymous proxy services and anonymous web surfing (such as anonymizer.com, the Electronic Frontier Foundation's (EFF) TOR network,²⁹⁵ and onion routers) can also be used to bypass filtering. It is, however, often the case that the filters block such well-known websites and proxy servers, which is why *Circumventor*, accessed through an unknown IP address (or one known to a limited number of users), provides better success in circumvention and avoids possible unintended risks associated with circumvention technologies.²⁹⁶

v. Freedom of Expression and Censorship

Problems associated with rating and filtering systems were also acknowledged at the European Union level. As the Economic and Social Committee of the European Commission pointed out in its report on the European Commission's Action Plan on promoting safe use of the Internet,²⁹⁷ it is highly unlikely that the proposed measures will result in a safe Internet in the long term, with the task of rating and classification of all information on the Internet being "impracticable".²⁹⁸ More importantly, the Committee was worried that the possibility of ISPs using filtering and rating systems at the level of entry would render these systems, dubbed as "user empowering", an instrument of control, "actually taking choice out of citizens' hands". The Committee concluded that there was "little future in the active promotion of filtering systems based on rating."²⁹⁹

²⁹² For further information about Peacefire.Org's *Circumventor*, see <<http://www.peacefire.org/circumventor/simple-circumventor-instructions.html>>.

²⁹³ See *Probing Chinese search engine filtering* (August 2004), online: OpenNet Initiative <<http://www.opennetinitiative.net/bulletins/005/>>.

²⁹⁴ See generally Jonathan Zittrain & Benjamin Edelman, *Documentation of Internet Filtering Worldwide* (Berkman Center for Internet & Society, 2003), online: Harvard Law School <<http://cyber.law.harvard.edu/filtering/>>.

²⁹⁵ See <<http://tor.eff.org/>>.

²⁹⁶ See further *Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran* (May 2004), online: OpenNet Initiative <<http://www.opennetinitiative.net/advisories/001/>>.

²⁹⁷ EC, Commission, *Opinion of the Economic and Social Committee on the 'Proposal for a Council Decision adopting a Multiannual Community Action Plan on promoting safe use of the Internet'*, [1998] O.J. C 214/29.

²⁹⁸ *Ibid.* at para. 4.1.1.

²⁹⁹ *Ibid.* See further Yaman Akdeniz, "The Regulation of Internet Content in Europe: Governmental Control versus Self-Responsibility" (1999) 5(2) *Swiss Political Science Review* 123.

vi. *Blocking Rather Than Removal*

As highlighted in this article, racist Internet content is often difficult to categorize and accordingly is not always categorized as illegal content. If such content does not pass the illegality threshold, then it must always be recognized that such speech or content will *not* be prohibited at its source. Although the content could be regarded as harmful and offensive to some audiences, it is a matter for those audiences to decide whether they want to access the expression in question. Filtering software can help audiences make that decision and block access to certain types of Internet content. This prevents the removal of such legal content from public networks, an action that would be inconsistent with fundamental human rights such as freedom of expression.

(E) *Information, Education and Awareness Campaigns*

The Internet itself can be an effective tool in the fight against racism.³⁰⁰ The need to promote the use of new information and communication technologies, including the Internet, to contribute to the fight against racism, racial discrimination, xenophobia and related intolerance is recognized by the UN Durban Declaration.³⁰¹ According to the Declaration, “new technologies can assist the promotion of tolerance and respect for human dignity, and the principles of equality and non-discrimination”.³⁰² As noted by an April 2000 UN report leading into the Durban World Conference, governments, intergovernmental organizations, national human rights institutions and non-governmental organizations are using the Internet to inform the public about their work and to spread positive messages of equality and non-discrimination.³⁰³ A number of initiatives aim to assist parents and teachers in preparing children for safer use of the Internet,³⁰⁴ and within this context a recent Partners Against Hate initiative report highlights critical thinking skills as “one of the most effective tools to provide young people with protection against hate on the Internet.”³⁰⁵

The same approach has been adopted at the OSCE level with recommendations that “Internet users should be educated about tolerance and that cooperation should

³⁰⁰ See *Reports, studies and other documentation for the Preparatory committee and the World Conference: Consultation on the use of the Internet for the purpose of incitement to racial hatred, racial propaganda and xenophobia*, UN GAOR, UN Doc. A/CONF.189/PC.1/5 (2000).

³⁰¹ Durban Declaration, *supra* note 203 at para. 92.

³⁰² *Ibid.*

³⁰³ *Supra* note 300.

³⁰⁴ See especially Partners Against Hate, *Hate on the Internet: A Response Guide for Educators and Parents* (December 2003), online: Anti-Defamation League <http://www.partnersagainsthate.org/publications/hoi_full.pdf>.

³⁰⁵ *Ibid.* at 30. The report cites John Dewey describing critical thinking skills as “active, persistent, and careful consideration of any belief or supposed form of knowledge in the light of the grounds that support it and the further conclusion to which it tends”. See further John Dewey, *Experience and Education* (New York: Macmillan Publishers, 1938).

be promoted among all actors, particularly nongovernmental organizations and associations working to combat racist, anti-Semitic and xenophobic propaganda on the Internet.”³⁰⁶

Another good example of this line of argument is a pilot study of websites in English conducted by the European Monitoring Centre on Racism and Xenophobia (EUMC) to be used for intercultural training by children, young adults, teachers and trainers.³⁰⁷ A total of 273 good websites dealing with and promoting cultural diversity were identified by the pilot study in the first half of 2002.

States, international, and specialized organizations³⁰⁸ should continue to invest in education³⁰⁹ and awareness-raising³¹⁰ campaigns to “provide users, particularly young people, with accurate information on the dangers of racism and anti-Semitism so as to counter the influence of racist organizations.”³¹¹ Information, education, and awareness campaigns should be a component in any initiative or programme to combat racism.³¹² In January 2006, the UN Intergovernmental Working Group (IWG) on the effective implementation of the Durban Declaration and Programme of Action reaffirmed that States should promote the use of the Internet to create educational and awareness-raising networks against racism.³¹³ As stressed by the IWG, “States should increase awareness about the possibilities offered by new information technologies and continually develop tools to promote, among civil society, in particular parents, teachers and children on the use of the information networks.”³¹⁴ In this regard, practical measures should include the creation of a model anti-racism network for schools, the inclusion of anti-racism messages on websites accessed by young people, training courses for teachers on how to use the Internet, the promotion of digital inclusion, the ethical use of the Internet and the development of critical thinking skills for children.

³⁰⁶ Secretary-General, *supra* note 14.

³⁰⁷ Andreas Hieronymus, *Using the Internet for Intercultural Training! A pilot study of web sites in English for children, young adults, teachers and trainers* (2003), online: EUMC <http://eumc.europa.eu/eumc/material/pub/intercult/Intercultural_training_Internet.pdf>.

³⁰⁸ Council of Europe, ECRI, *Specialized bodies to combat racism, xenophobia, anti-semitism and intolerance_CRI(2006)5*, online: CoE <http://www.coe.int/t/e/human_rights/ecri/1-ecri/3-general_themes/2-examples_of_good_practices/1-specialised_bodies/SB_table.asp>.

³⁰⁹ See especially Canadian Heritage, *A Canada For All: Canada's Action Plan Against Racism* (Ottawa: Minister of Public Works, 2005), online: Canadian Heritage <http://www.pch.gc.ca/multi/index_e.cfm>.

³¹⁰ See for example the “Turn it Down” initiative, a campaign against white power music, and their Resource Kit at <http://turnitdown.newcomm.org/images/stories/tidresourcekit/turn_it_down_resource_kit.pdf>.

³¹¹ *Implementation of the Programme of Action*, *supra* note 190 at para. 71.

³¹² *Supra* note 300.

³¹³ *Report of the Intergovernmental Working Group*, *supra* note 55 at para. 103(b).

³¹⁴ *Ibid.* at para. 103(c).

In summary, there are currently only a limited number of specific self- and co-regulatory measures, including codes of conduct aimed at combating racist Internet content. However, significant questions remain regarding the effectiveness and efficacy of the various mechanisms and tools currently offered by the private sector.³¹⁵ Self- and co-regulatory measures may yet play an important role in the fight against racist Internet content, however, this will depend upon substantial improvement of existing systems or the devising of less problematic alternatives.

CONCLUSION

Speech that incites or promotes hatred towards individuals, on the basis of their race, gender, religion, sexual preference, and other forms of individual discrimination continues to be widely available on the Internet as in other kinds of traditional media. There is strong documented evidence to show that “far right and radical Islamist organizations are using the Internet as a key component in their campaigns of hatred.”³¹⁶ This article has sought to assess the possibilities of and challenges posed by the use of the Internet to propagate or to counter material of a racist nature. Measures taken at the national and international levels as well as by the private sector to combat racist Internet content have been highlighted.

A number of themes surface from this analysis with the most prominent being the fact that “States have yet to reach a political agreement on how to prevent the Internet being used for racist purposes and on how to promote its use to combat the scourge of racism.”³¹⁷ Some see harmonized national legislation and international agreements as the way forward; for example, the ECRI believes “national legislation against racism and racial discrimination is necessary to combat these phenomena effectively.”³¹⁸ Others strenuously oppose this position, citing objections on grounds of freedom of expression; it has been noted at the OSCE level that “the United States opposes any regulation, on freedom of expression, while the European countries are more in favour of a policy of monitoring and sanctions.”³¹⁹ Hence, fundamental “disagreements remain on the most appropriate strategy for preventing dissemination of racist messages on the Internet, including the need to adopt

³¹⁵ Marielle De Sarnez (Rapporteur), *European Parliament Report from the Committee on Culture and Education on the proposal for a recommendation of the European Parliament and of the Council on the protection of minors and human dignity and the right of reply in relation to the competitiveness of the European audiovisual and information services industry (2005) A6-0244/2005*, COM (2004) 341.

³¹⁶ Parliamentary Committee Against Antisemitism, *supra* note 30 at para. 20.

³¹⁷ Doudou Diène, *Racism, Racial Discrimination, Xenophobia And All Forms Of Discrimination - Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, Commission on Human Rights, 61st Sess., UN Doc. E/CN.4/2005/18 (2004).

³¹⁸ Council of Europe, ECRI, *General Policy Recommendation N° 7 on national legislation to combat racism and racial discrimination*, CRI (2003) 8 at para. 1 of the Explanatory Memorandum, online: CoE <http://www.coe.int/t/e/human_rights/ecri/1-ecri/3-general_themes/1-policy_recommendations/recommendation_n7/3-Recommendation_7.asp>.

³¹⁹ Secretary-General, *supra* note 14.

regulatory measures to that end.”³²⁰ This lack of consensus threatens the implementation of legal sanctions in accordance with relevant international human rights legal instruments, in particular the ICERD as recommended by paragraph 147 of the Durban Declaration. It is possible that the strengthening and updating of international instruments, most notably the ICERD, may result in wider agreement. At the same time, the absence of a global consensus on the limits of freedom of expression remains an obstacle to regulatory harmonization through the CoE Additional Protocol or any other future international agreement or convention.

Another associated factor to emerge from this article is the extent of duplication of efforts at both the supranational/regional and the international levels of governance. This duplication has resulted in delays in finalizing policies within relevant international organizations, and in its subsequent implementation at the national level to address Internet related problems. Governments and international organizations are, however, responding to the dissemination of racist content through the Internet,³²¹ as awareness of the problem grows with use of the Internet by terrorist organizations for spreading propaganda³²² and inciting terrorist violence,³²³ as well as the resurrection of Nazi ideology in Europe,³²⁴ and violent radicalization.³²⁵ For example, the European Union’s May 2006 revised *Action Plan on Terrorism*³²⁶ includes the development of policies and measures to detect misuse of the Internet by extremist websites, and to enhance co-operation of States against terrorist use of the Internet. The EU will also consider developing further legal

³²⁰ Meeting on the relationship between racist, xenophobic and anti-Semitic propaganda on the Internet and hate crimes held by the (OSCE) in Paris on 16-17 June 2004.

³²¹ Secretary-General, *Global efforts for the total elimination of racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action*, UN GA, 60th Sess., UN Doc. A/60/307 (2005).

³²² See generally Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington: U.S. Institute of Peace, 2006).

³²³ See *Threats to international peace and security caused by terrorist acts*, SC Res. 1617, UN ESCOR, 2005, UN Doc. S/RES/1617. See also *JIHAD Online: Islamic Terrorists and the Internet* (2002), online: Anti-Defamation League <http://www.adl.org/internet/jihad_online.pdf>; Weimann, *supra* note 18.

³²⁴ Council of Europe, *supra* note 27; See also Council of Europe, P.A., 2003 Ordinary Sess. (Fourth Part) *Racist, xenophobic and intolerant discourse in politics*, Texts Adopted, Res. 1345 (2003) online: CoE <<http://assembly.coe.int/Main.asp?link=http://assembly.coe.int/Documents/AdoptedText/ta03/ERES1345.htm>>. See further Council of Europe, P.A., 2003 Ordinary Sess. (Fourth Part) *Report of the Committee on Legal Affairs and Human Rights*, Documents, Doc. 9904 (2003), online: CoE <<http://assembly.coe.int/Main.asp?link=http://assembly.coe.int/Documents/WorkingDocs/doc03/EDO C9904.htm>>.

³²⁵ Council of the European Union, *The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism*, 14347/05 JAI 414 ENFOPOL 152 COTER 69, Brussels (25 November 2005).

³²⁶ Council of the European Union, *Revised Action Plan on Terrorism*, 10043/06, Brussels (31 May 2006).

frameworks to remove illegal content from the Internet, including websites that incite terrorist action, and those providing manuals or instructions for homemade explosives or bombs.³²⁷

FUTURE DIRECTIONS

As Farber rightly states, “hate on the Internet will not disappear overnight. But the intractability of the problem does not absolve us of the responsibility to engage in its resolution. The very size of the problem requires us to pursue multiple approaches for partnership with government, police services, schools, community groups and service providers.”³²⁸ Looking to the future, one can expect a trend towards “governance” rather than “government”, where the role of the nation-state is not exclusive and where more varied forms of regulation, many in the private sector, come into play. Internet governance will continue to evolve at the national and international levels,³²⁹ “regardless of frontiers”,³³⁰ and policy initiatives will need to reflect the Internet’s decentralized nature.

As this article has sought to demonstrate, in the fight against racist Internet content, no one approach promises to be entirely effective. The emergence of Internet governance entails a more diverse and fragmented regulatory network with no presumption that these regulations are anchored primarily in nation-states. Although legal regulation will doubtless continue to form an important part of future efforts to tackle the problem of online racism, it will only ever form *part* of the solution. Ultimately, it will prove necessary to rely on additional measures in the form of self- and co-regulatory initiatives. The success of these measures will, in turn, depend upon substantial improvement of existing systems including the development of ISP codes of conduct, complaint systems, and other mechanisms aimed at combating racist Internet content as recommended by the Durban

³²⁷ In August 2006, Ministers representing the current Finnish EU Presidency, the future EU Presidencies (Germany, Portugal, Slovenia and France), the U.K. Home Secretary and Vice-President Frattini of the European Commission emphasised “the need to make the Internet a hostile environment for terrorists and those who seek to radicalise young people, spread messages of hate and plan mass murder”: Ministers of U.K., Finland, Germany, Portugal, Slovenia, France and the Vice-President of the European Commission, Joint Press Release, “Informal London Meeting on Counter-Terrorism” (16 August 2006), online: <http://www.eu2006.fi/news_and_documents/other_documents/vko33/en_GB/1155736629535/_files/75742366748508254/default/joint_press_statement_london.pdf>. See further “ISPs Wary About ‘Drastic Obligations’ on Web Site Blocking” *Washington Internet Daily* (18 August 2006).

³²⁸ Bernie Farber, “The Internet and Hate Promotion: The 21st Century Dilemma” in *Hate on the Net*, (Ottawa, Association for Canadian Studies, Spring 2006) 12, online: Canadian Human Rights Commission <http://www.chrc-ccdp.ca/pdf/hateoninternet_bil.pdf>.

³²⁹ See the World Summit on the Information Society, *Tunis Commitment 2005*, UN Doc. WSIS-05/TUNIS/DOC/7 (2005).

³³⁰ Article 10(1) of the European Convention on Human Rights; Article 19 of the Universal Declaration of Human Rights. See further Global Internet Liberty Campaign, *Regardless Of Frontiers: Protecting The Human Right to Freedom of Expression on the Global Internet* (Washington: Center for Democracy & Technology, 1998), online: CDT <<http://www.cdt.org/gilc/report.html>>.

Declaration.³³¹ If successful, these measures could be more flexible and more effective than prescriptive government legislation.

Consistent with recommendation 141 of the Durban Declaration, education about racist content on the Internet and how to foster tolerance, is arguably the single most effective way of combating racist content.³³² The importance of education to promote respect and fight intolerance is highlighted in other broader forums, especially following the events of 11 September 2001, with the rise of Islamophobia and Anti-Semitism.³³³ It is often argued that the development of good practice initiatives to reduce prejudice and “cultural, academic and educational initiatives, supplemented by a range of inter-religious and intercultural awareness events” is the best way to address such problems.³³⁴ The role the Internet can play as a powerful instrument to combat racism should not be underestimated or discounted.

³³¹ *Supra* note 203 at para. 144.

³³² See *Report of the High Commissioner for Human Rights*, *supra* note 42.

³³³ See ODIHR, *Education on the Holocaust and on Anti-Semitism: An Overview and Analysis of Educational Approaches* (April 2006), online: OSCE <http://www.osce.org/publications/odih/2006/04/18712_586_en.pdf>.

³³⁴ Christopher Allen & Jorgen S. Nielsen, *Summary Report on Islamophobia in the EU after 11 September 2001* (Birmingham: University of Birmingham, 2002), online: EUMC <http://eumc.europa.eu/eumc/material/pub/anti-islam/Synthesis-report_en.pdf>. See further EUMC, *The fight against Anti-Semitism and Islamophobia - Bringing Communities together* (2003), online: EUMC <<http://eumc.europa.eu/eumc/material/pub/RT3/Report-RT3-en.pdf>>.