Private Regulation and Public Policy: Toward Effective Restriction of Internet Hate Propaganda

Jane Bailey*

Internet hate propaganda revives debate regarding competing visions of freedom of expression and democracy—pitting the unregulated marketplace of ideas vaunted in US First Amendment jurisprudence on racist speech against approaches such as Canada's, which envision a role for the state in limiting de-liberating exercises of private power unchecked by the marketplace itself. Despite the relative ease with which Internet hate propagandists may shift the "location" of their message to First Amendment-protected servers in the US, national and international public regulation of hate propaganda have not outlived their usefulness. Existing private restriction of hate propaganda may assist in resisting First Amendment hegemony, but is not an adequate substitute for protecting fundamental national and international commitments to equality and diversity. The practical drawbacks of many private enforcement mechanisms are compounded by policy concerns underlain by a record of the private market's inadequacy in ameliorating the conditions of historically disadvantaged groups. Certain of these drawbacks might be alleviated through continuing expressions of policy pursuant to public regulation aimed at guiding private regulation and imbuing it with a degree of transparency and accountability. In the long term, creation and monitoring of an Internet Service Provider ("ISP") model code of conduct by a respected international body, such as the United Nations, might assist in more systematically harnessing private action in service of public human rights objectives.

La propagande haineuse sur Internet ravive le débat entre des conceptions divergentes de la démocratie et de la liberté d'expression. À l'idée d'un marché d'idées non réglementé, soutenue aux États-Unis par la jurisprudence sur le premier amendement de la constitution de ce pays, s'oppose l'approche canadienne. Au Canada, la constitution confère aux autorités gouvernementales le pouvoir de limiter l'exercice de la liberté d'expression là où le marché ne le fait pas. En dépit de la relative facilité avec laquelle la propagande haineuse peut élire domicile sur des serveurs américains protégés par le premier amendement, la réglementation publique nationale et internationale n'est toujours pas inutile. Les restrictions de nature privée imposées à la propagande haineuse peuvent contribuer à faire obstacle aux lacunes résultant de l'hégémonie du premier amendement, mais ne sauraient se substituer à la protection d'engagements nationaux et internationaux en faveur de l'égalité et de la diversité. L'auteur suggère qu'à ces inconvénients pratiques s'ajoute l'incapacité démontrée du marché à améliorer la condition de groupes historiquement désavantagés. Il serait possible de remédier à certains de ces inconvénients, dans la mesure où la réglementation publique puisse guider et surveiller les mécanismes privés de contrôle, eréant une certaine transparence et un certain degré de responsabilité. L'auteur conclut qu'à long terme, la eréation et la surveillanee d'un code de conduite pour les fournisseurs de services Internet (ISP) par une organisation internationale respeetée telle que les Nations Unies pourrait permettre de guider l'activité privée de manière à ce qu'elle puisse servir de manière plus systématique des objectifs publics liés aux droits de la personne.

* Assistant Professor, University of Ottawa Faculty of Law, Common Law Section, jbailey@uottowa.ca. Thanks to The Centre for Innovation Law and Policy and the Ontario Graduate Scholarship program for funding support, Shawn Pudsey for his interest and research assistance, Professor Trevor Farrow of the University of Alberta and two external reviewers for their thoughtful comments on earlier drafts. All shortcomings, however, remain those of the author. For purposes of full disclosure, readers should be aware that the author assisted as co-counsel for the complainant Sabina Citron in *Citron*, *infra* note 10.

Revue de droit de McGill 2003
To be cited as: (2003) 49 McGill L.J. 59
Mode de référence : (2003) 49 R.D. McGill 59

> We have exported to the world, through the architecture of the Internet, a First Amendment *in code* more powerful than our own First Amendment *in law*.
>
> Lawrence Lessig[1]

> Americans take free speech a bit more seriously than the Brits, the French, the Germans and the rest of the world. And, yes, America could become the guardian of free speech worldwide by offering the protection of the First Amendment over the Net to millions of people who have been denied the right to speak freely in their own countries.
>
> Adam D. Thierer, CATO Institute[2]

> Under the First Amendment the government must leave to the people the evaluation of ideas. ... Totalitarian governments today rule much of the planet, practicing suppression of billions and spreading dogma that may enslave others. One of the things that separates our society from theirs is our absolute right to propagate opinions that the government finds wrong or even hateful.
>
> The ideas of the Klan may be propagated. ... The Nazi Party may march through a city with a large Jewish population. ... People may seek to repeal laws guaranteeing equal opportunity in employment or to revoke the constitutional amendments granting the vote to blacks and women. They may do this because "above all else, the First Amendment means that government has no power to restrict expression because of its message [or] its ideas ... "
>
> *American Booksellers Association v. Hudnut*[3]

Introduction

The relatively low cost and the dissemination power of Internet communication make it an increasingly preferred medium for hate propagandists. Canada, other nations, and international collectives have developed or modified existing public regulation to address this growing problem. Unfortunately, First Amendment[4] protection of the growing tide of hate propaganda emanating from servers located in

---

[1] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) at 167 [emphasis in original].

[2] Adam D. Thierer, "Web Restrictions Unlikely to Muzzle Neo-Nazi Speech" (15 January 2001), online: Cato Institute <http://www.cato.org/cgi-bin/scripts/printtech.cgi/dailys/01-15-01.html>.

[3] 771 F.2d 323 (7th Cir. 1985) at 328, 106 S. Ct. 1172 [*Hudnut* cited to F.2d]. While this quote undoubtedly overstates the degree to which US First Amendment jurisprudence forbids government restriction of expression generally, this kind of language often surfaces in the context of restrictions on hate propaganda and pornography.

[4] U.S. Const. amend. 1.

the United States challenges the ability of other nations to pursue alternative public policies, such as the one underlying recent Canadian legislative amendments enacted to clarify the application of restrictions on Internet hate propaganda. The export of the First Amendment approach to Canada is not properly characterized as an export of free expression. The *Canadian Charter of Rights and Freedoms*[5] protects free expression and does so on the basis of a comprehensive conception of both public and private forces affecting individual liberty, in accordance with international human rights commitments.

The First Amendment challenge to restricting hate propaganda emanating from within the US suggests that technology has overtaken public regulation at both national and international levels. Given that private action is generally not subject to US constitutional scrutiny, emerging regulation by private actors in the US presents an opportunity to restrict the cross-border flow of hate propaganda. For both practieal and policy reasons, private regulation is an inadequate substitute for public regulation, particularly in the area of human rights. Nevertheless, ongoing ad hoc private efforts to restrict hate propaganda and other illegal and offensive content invite consideration of the ways in which public initiatives may be used to encourage more systematic private efforts while at the same time imbuing them with a degree of public accountability.

This paper explores these issues in seven parts. Part I describes the scope of the Internet hate propaganda problem. Part II examines the Canadian approach to hate propaganda, focusing on legislative amendments designed to specifically address the Internet. Part III contrasts Canadian and US approaches, demonstrating the First Amendment challenge to restrieting the cross border flow of hate propaganda emanating from the US. Part IV briefly discusses the different underlying democratic visions animating the two approaches, arguing that the US approach has no prior claim in furthering the interests of democracy. Part V explores the degree to which the First Amendment undercuts the efficacy of public international responses based on state action, suggesting an investigation of private regulatory opportunities is necessary. Part VI identifies and discusses practical and policy limitations to some current private on-line content regulation. Part VII comments on the prospect for an internationally facilitated strategy that seeks to integrate more publicly accountable and systematic private regulation with vigilant enforcement of public regulation.

I. Internet Hate Propaganda: The Scope of the Problem

Hate propaganda[6] is disseminated on the Internet using a variety of applications, from Web sites to newsgroups to e-mail to on-line games. The exact scope of the

---

[5] Part I of the *Constitution Act, 1982* being Schedule B to the *Canada Act 1982* (U.K.) 1982, c. II [*Charter*].

[6] Unless otherwise defined (e.g., as defined in legislation), the term "hate propaganda" describes messages aimed at; or with the effect of, inciting hatred or contempt for individuals or groups of

problem remains unclear. While there has been some effort to collect and analyze Internet hate propaganda based on race, ethnicity, and national identity ("racist propaganda"), until recently there has been less focus on hate propaganda based on other grounds, such as gender and sexual identity. Nevertheless, the available reports suggest widespread and growing use of the Internet to disseminate messages of hate against groups identifiable on all of these grounds, as well as against the individual members of those groups.

Reports suggest that racist Web sites alone have grown steadily from a single white supremacist Web site in 1995[7] to a reported 4,000 racist Web sites in 2001, an estimated 2,500 of which emanate from US servers.[8] Groups such as the Ku Klux Klan, the National Alliance, and a number of self-proclaimed Christian-right organizations use their Web sites to broadly convey their message and attract potential new members to their causes, often combining racist attacks with attacks based on religion, gender, and sexual identity.[9] As is often the case with hate propaganda, the vitriol of many of the messages is camouflaged with attractive packaging and, in some cases, pseudo-academic approaches.[10] Nevertheless, the hateful nature of the messages is rarely far from the surface[11] and can be combined with information on bomb making or advocacy of other violent activity.[12] Connections between on-line hate propaganda and "real world" violence serve as a

---

individuals identifiable on the basis of personal characteristics such as race, religion, ethnicity, gender, family status, marital status, and sexual identity that have historically formed the basis of socially imposed disadvantage.

[7] Anti-Defamation League, "Hate on the World Wide Web: A Brief Guide to Cyberspace Bigotry", online: Anti-Defamation League <http://www.adl.org/special_reports/hate_on_www/print.asp> [Anti-Defamation League, "Hate on the Web"].

[8] Wendy McAuliffe, "Europe Hopes to Outlaw Hate Speech Online" *CNET News.com* (12 November 2001), online: CNET <http://news.com.com/2100-1023-275708.html?legacy=cnet>.

[9] Southern Poverty Law Center, "Hate on the Internet," online: Tolerance.org <http://www.tolerance.org/hate_internet/index.jsp>. See also Raymond Franklin, "The Hate Directory", online: <http://www.bcpl.net/~rfrankli/hatedir.htm>.

[10] Two Web sites recently subjected to Canadian Human Rights Tribunal ("CHRT") cease and desist orders, for example, attempt to accredit their messages of hate by associating them with "noted historians" such as David Irving, or publishing organs such as the Institute for Historical Review, an organization that claims to be committed to debunking the "myth" of the Holocaust. See *Citron v. Zundel*, [2002] 41 C.H.R.R. D/274 T.D.1/02 (CHRT) [*Citron*] and *Warman v. Kyburz*, 2003 CHRT 18 [*Warman*].

[11] For example, the home page of one anti-gay and lesbian Web site, recently ordered shut down by a CHRT, states: "Warning! This site contains material that is deemed offensive by homosexual pedophiles" (Citizens Research Institute, online: <http://www.citizensresearchinst.com/>).

[12] For example, the Creativity Movement (formerly the World Church of the Creator) operated a Web site known as Skinheads of the Racial Holy War, though the group disclaimed participation in or advocacy of violence: Anti-Defamation League, "World Church of the Creator: 'Racial Holy War' on the Web", online: Anti-Defamation League <http://www.adl.org/poisoning_web/wcotc.asp>. Other Web sites advocate or condone violence in a somewhat less direct fashion by posting articles advocating extermination and violence. See *e.g. Warman*, *supra* note 10 at paras. 20-26.

chilling reminder of the potential impact of words on action, particularly words targeted at vulnerable consumers such as children.[13]

It may well be that the reported scope of Internet hate propaganda represents only the tip of the iceberg. Hate group activity has spread from Web sites to other Internet applications, such as e-mail, chatrooms, and newsgroups, which are currently more difficult to track. Further, the Internet is used to advertise and distribute other hateful materials, such as music and video games.[14] By restricting access to these applications, hate groups can foment and reinforce hateful attitudes and approaches among like-minded individuals while avoiding the backlash of negative publicity created when their messages are readily available to other Internet users. In other cases, these forums are generally available to all members of the connected public.[15] These applications may be used to incite "lone-wolf acts" as hate groups attempt to distance their organizations from violent action resulting from their messages.[16]

The known scope of Internet hate propaganda has prompted national and international attention and calls for action, focusing predominantly on racist propaganda. The Council of Europe ("COE") held an international forum in 2001 relating to illegal and harmful content on the Internet, in which racist propaganda was a central focus.[17] Subsequently, a number of COE member states signed a protocol to address racist and xenophobic acts through computer networks (the "Additional Protocol").[18] Although Canada has yet to sign the Additional Protocol, it has taken action at the national level, amending provisions of both the *Canadian Human Rights Act*[19] and the *Criminal Code* ("Code")[20] to specifically address dissemination of hatred through computer networks (collectively, the "Amendments").[21] The

---

[13] See Peter J. Breckheimer II, "A Haven for Hate: The Foreign and Domestic Implications of Protecting Internet Hate Speech Under the First Amendment" (2002) 75 S. Cal. L. Rev. 1493 at 1496-99.

[14] See Anti-Defamation League, "Hate on the Web", *supra* note 7; Franklin, *supra* note 9.

[15] The CHRT in *Warman* (*supra* note 10 at paras. 57-60) found that the hate propagandizing tactics of the respondent in that case included use of group e-mail and a Web forum in which membership was open generally to the connected public.

[16] See Anti-Defamation League, "'Lone Wolf' of Hate Prowls the Internet" (2000), online: Anti-Defamation League <http://www.adl.org/anti5/default.asp>.

[17] Council of Europe, "European Forum on Harmful and Illegal Cyber Content" (22 November 2001), online: Council of Europe <http://press.coe.int/cp/2001/884a(2001).htm>. See also International Telecommunications Union, World Summit on the Information Society, "Draft Plan of Action" (12 December 2003) DOC.WSIS-03/GENEVA/Doc-5-E, online: International Telecommunications Union <http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!MSW-E.doc>.

[18] *Additional Protocol to the Convention of Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*, 28 January 2003 Eur. T.S. 189 [*Additional Protocol*]. For the Chart of Signatures and ratifications to the *Additional Protocol*, see online: Council of Europe <http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=189> [Chart of signatures].

[19] *Canadian Human Rights Act*, R.S.C. 1985, c. H-6 [*CHRA*].

[20] *Criminal Code*, R.S.C. 1985, c. C-46 [*Code*].

[21] *Anti-Terrorism Act*, S.C. 2001, c. 41, ss. 10, 88 [*ATA*].

Amendments are consistent with the Canadian constitutional approach to restrictions on hate propaganda, as well as Canada's international human rights obligations. However, the First Amendment continues to protect a significant body of Internet hate propaganda emanating from servers located in the United States.

II. Canadian Approach to Hate Propaganda

A. *Amendment of the* CHRA *and the* Code

The federal government's first direct legislative attempt to explicitly restrict Internet hate propaganda arose in the context of the *Anti-Terrorism Act*—legislation designed to address terrorism following the attacks on the US on 11 September 2001.[22] The *ATA* extends to the Internet specific pre-existing *Criminal Code*[23] and *CHRA*[24] restrictions on defined categories of hate propaganda, which were previously determined by the Supreme Court of Canada to be consistent with freedom of expression under the Charter (as discussed in detail below in subsection B).

The objectives of the *ATA* and the context surrounding its passage underscore continuing concern about links between hate propaganda, intolerance, and violence. Then Justice Minister Anne McClellan specifically linked the objectives of the *ATA* to the context of the September 11 attacks, stating:

> The horrific events of September 11 remind us that we must continue to work with other nations to confront terrorism and ensure the full force of Canadian law is brought to bear against those who support, plan and carry out acts of terror—we will cut off their money, find them and punish them.[25]

Representatives of the federal government characterized the Amendments as a mechanism for addressing the root causes of hatred underlying terrorist acts,[26] stating:

---

[22] *Ibid.*

[23] *Code*, *supra* note 20.

[24] *CHRA*, *supra* note 19.

[25] Department of Justice Canada, News Release, "Government of Canada Introduces *Anti-Terrorism Act*" (15 October 2001), online: Department of Justice Canada <http://canada.justice.gc.ca/en/news/nr/2001/doc_27785.html>.

[26] In the House of Commons, Liberal members of Parliament relied on the Amendments in responding to harsh criticisms by members of the opposition parties relating to other provisions of the *ATA* that create a significant risk of targeted law enforcement against, and surveillance of, individuals from certain religious and cultural backgrounds. See *e.g. House of Commons Debates*, 095 (16 October 2001) at 1705 (Libby Davies) and 1230 (Sarmite Bulte), online: Government of Canada <http://www.parl.gc.ca/37/1/parlbus/chambus/house/debates/indexE/a-37-1_4-e.htm> ["Bulte Debate"]; *House of Commons Debates*, 095 (17 October 2001) at 1625 (Anita Neville), online: Government of Canada <http://www.parl.gc.ca> ["Neville Debate"]. See also R.J. Daniels, P. Macklem, and K. Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001).

> This is a struggle against terrorism, and not against any one community, group or faith. Diversity is one of Canada's greatest strengths, and the Government of Canada is taking steps to protect it. Measures will be included ... to address the root causes of hatred and to ensure Canadian values of equality, tolerance and fairness are affirmed in the wake of the September 11 attacks. These include:
>
> - amending the *Criminal Code* to eliminate online hate propaganda ... ; and
> - amending the *Canadian Human Rights Act* to clarify that the prohibition against spreading repeated hate messages by telephonic communications includes all telecommunications technologies.[27]

The federal government linked the Amendments to the "war on terrorism" in two ways. First, restricting messages inciting racial hatred might reduce the risk of incitement of terrorist conduct. Second, such restrictions should protect those of certain identifiable racial, ethnic, and religious origins from being wrongfully subjected to hatred or contempt as the result of terrorist acts.[28]

The Amendments comprise two components—one relating to the *CHRA* (the "*CHRA* Amendment") and the other to the *Criminal Code* (the "Code Amendment").

1. *CHRA* Amendment

Section 88 of the *ATA* amended subsection 13(2) of the *CHRA* by specifically indicating that provisions of 13(1) apply to computer and Internet communication.[29] As amended, subsections 13(1) and 13(2) provide that it is a discriminatory practice for a person or a group of persons acting in concert to use, among other things, a computer or group of interconnected or related computers to communicate or to cause to be communicated, repeatedly, any matter that is likely to expose a person or persons to hatred or contempt by reason of their identifiability based on a prohibited ground of discrimination. The prohibited grounds of discrimination under the *CHRA* include race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability, and conviction for which a pardon has been granted.[30]

Subsection 13(1) may be applied to those communicating or causing communication of messages located outside of Canada, provided that the victim of the practice was, at the time, a citizen or permanent resident of Canada.[31] In the Internet context, this may also include certain Internet Service Providers ("ISP"s)

---

[27] Department of Justice Canada, *supra* note 25.

[28] See *e.g.* "Bulte Debate", *supra* note 26; "Neville Debate", *supra* note 26.

[29] In *Citron*, *supra* note 10, a CHRT had already determined prior to passage of the clarification in the *CHRA* Amendment that subsection 13(1) applied to Internet communication via the World Wide Web.

[30] *CHRA*, *supra* note 19, s. 3(1).

[31] *Ibid.*, s. 40(5)(c).

involved in causing communication, unless their only role in the communication is by virtue of others using their undertaking for purposes of transmission.[32]

Where a discriminatory practice is made out under subsection 13(1), a Canadian Human Rights Tribunal ("CHRT") may require the person found to have engaged in such a practice to: (i) cease that practice and to take measures in consultation with the Canadian Human Rights Commission ("CHRC") to redress the practice or prevent it from recurring; (ii) compensate a victim specifically identified in the communication; and (iii) pay a penalty of up to $10,000.[33]

2. Code Provisions and Amendment

Even prior to the *ATA*, reflecting Canada's international human rights obligations,[34] it was a crime in Canada to:

(i) advocate killing or deliberately inflicting conditions of life calculated to bring about the physical destruction of a section of the public identifiable on the basis of colour, race, religion, or ethnic origin (an "Identifiable Group");[35]

(ii) publicly incite hatred against an Identifiable Group where the incitement was likely to lead to a breach of the peace;[36] and to

(iii) publicly communicate statements willfully promoting hatred against an Identifiable Group (subject to the defences of good faith and truth, among others).[37]

Section 10 of the *ATA* amended the Code to explicitly empower a judge to address on-line hate propaganda by: (i) issuing a warrant of seizure of, among other things, hate propaganda as defined in sections 318 and 319 of the Code ("Hate Propaganda") stored on and made publicly available through a computer system

---

[32] *Ibid.*, s. 13(3).

[33] *Ibid.*, s. 54(1).

[34] See especially *International Convention on the Elimination of All Forms of Racial Discrimination*, 4 January 1969, 660 U.N.T.S. 212 [*CERD*] (signed by Canada 24 August 1966 and ratified 14 October 1970); Canada, Law Reform Commission, *Hate Propaganda* (Ottawa: The Commission, 1986) at 17; *International Covenant on Civil and Political Rights*, 23 March 1976, 999 U.N.T.S. 172 [*ICCPR*].

[35] *Code*, *supra* note 20, s. 318. The prohibited grounds of discrimination under the *Code* are notably more restricted than those under the *CHRA*. However, a majority of the House of Commons voted on 17 September 2003 to include sexual orientation as a prohibited ground in the *Code* provision. See Bill C-250, *An Act to amend the Criminal Code (hate propaganda)*, 2d Sess., 37th Parl., 2002 and Peter O'Neil, "Homosexuals to be Covered by Anti-Hate Legislation" *Ottawa Citizen* (18 September 2003) A5.

[36] *Code*, *ibid.*, s. 319(1).

[37] *Ibid.*, s. 319(2).

within the jurisdiction of the court[38] and, after a hearing, (ii) ordering the seized material deleted if it meets the statutory criteria.[39] While the hearing regarding deletion may involve individuals residing outside of Canada,[40] it is questionable whether deletion orders will be made in respect of computer systems in other jurisdictions.[41]

B. Canadian Constitutional Review of Hate Propaganda Restrictions

Prior to enactment of the Amendments, the Supreme Court had found, in *Taylor*[42] and *Keegstra*[43] respectively, that the restrictions imposed by subsection 13(1) of the *CHRA* and by subsection 319(2) of the Code constituted justifiable limits on expression in a free and democratic society. The Court concluded that these provisions restricted non-violent attempts to convey meaning and thus violated subsection 2(b) of the Charter,[44] but were nevertheless justifiable in that:

(i) Hate propaganda as defined in the provisions lay far from the core values of the search for the truth,[45] democratic participation,[46] and self-fulfillment[47]

---

[38] *Ibid.*, s. 320.1(1).

[39] *Ibid.*, s. 320.1(5).

[40] *Ibid.* Subsection 320.1(2) requires notification of the person posting the offending information with respect to the impending hearing as well as the opportunity to attend and to make submissions with respect to why the material should not be ordered deleted. See also subsection 320.1(4), which specifically contemplates that the person posting the material may reside outside of Canada and provides that a deletion order may be made even if the person posting the material does not attend the hearing.

[41] While a court could theoretically interpret "within the jurisdiction of the court" (*ibid.*, s. 320.1(1)) widely and attempt to assert control over a computer system located outside of Canada, the legislative intention behind the provision appears to require that the computer system must be physically present in Canada in order to issue a warrant in relation to it. See *House of Commons Debates*, 095 (16 October 2001) at 1015 (Anne McLellan), online: Government of Canada, <http://www.parl.gc.ca>. In practice, if investigative authorities had reasonable grounds to believe that evidence in the US would assist in proving a violation within Canada of the hate propaganda provisions under the *Criminal Code* through a computer system, it is likely that Canadian authorities would request their American counterparts to obtain a US search warrant pursuant to the *Treaty Between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters*, Canada and the United States, 18 March 1985, Can. T.S. 1990 No. 19 (entered into force 24 January 1990). Under the treaty, the US Central Authority may deny assistance to the extent it considers Canada's request to be contrary to US public policy (art. (V)). Further, the US Central Authority would be required to obtain a warrant, at which point a US court's willingness to issue could be affected by whether the warrant sought related to First Amendment protected expression.

[42] *Canadian (Human Rights Commission) v. Taylor*, [1990] 3 S.C.R. 892, 75 D.L.R. (4th) 577 [*Taylor* cited to S.C.R.].

[43] *R. v. Keegstra*, [1990] 3 S.C.R. 697, [1991] 2 W.W.R. 1 [*Keegstra* cited to S.C.R.].

[44] See *Irwin Toy Ltd. v. Quebec (A.G.)*, [1989] 1 S.C.R. 927, 58 D.L.R. (4th) 577.

[45] Applying this approach, the Court found that the restricted expression did not facilitate the search for truth, noting both that it was premised upon untruths and partial truths, and that it could not be assumed that an unregulated marketplace of ideas would necessarily facilitate the search for truth

underlying freedom of expression, making their restriction more easily justifiable;[48]

(ii) The Code and *CHRA* provisions served pressing and substantial objectives underscored by other Charter values such as equality and multiculturalism, as well as Canada's international human rights obligations,[49] respectively being aimed at: limiting the risk of harm that hate propaganda poses to target group members and to racial, ethnic, and religious harmony in Canada[50] and promoting equality of opportunity unhindered by discriminatory practices based upon membership in, among others, a particular racial, religious, or ethnic group;[51]

(iii) Prohibiting the dissemination of hate propaganda as defined in the provisions was rationally connected with their objectives in that censure of

---

(*Keegstra*, *supra* note 43 at 747). The dissenting reasons in *Zundel* echoed these conclusions, noting that "[w]e are warned quite properly that history has many lessons to teach. One is that the marketplace of ideas is an inadequate model; another is that minorities are vulnerable to censure as speakers": *R. v. Zundel*, [1992] 2 S.C.R. 731 at 825, 95 D.L.R. (4th) 202 [*Zundel* cited to S.C.R.]. While the majority in *Zundel* held that untruths could play a useful role in the search for truth, it is unlikely that the majority view in that case would bear upon an analysis of the constitutionality of the Amendments. The Court's more recent comments in *Thomson* reaffirm that harmful effects associated with hate propaganda render restrictions on it more easily justified: *Thomson Newspapers Co. v. Canada (A.G.)*, [1998] 1 S.C.R. 877 at paras. 90-92, 159 D.L.R. (4th) 385 [*Thomson* cited to S.C.R.]. Further, the provision at issue in *Zundel* related to "false news"—a restriction originally aimed at protecting the aristocracy from scandalous remarks. The Amendments, are aimed at, among other things, promoting social harmony.

[46] The Court found that hate propaganda argues "for a society in which the democratic process is subverted and individuals are denied respect and dignity simply because of racial or religious characteristics ... [a] brand of expressive activity ... wholly inimical to the democratic aspirations of the free expression guarantee" (*Keegstra*, *supra* note 43 at 764).

[47] The Court accepted that the hate propaganda at issue facilitated the individual self-fulfillment of the speaker, but undermined the fulfillment of target group members, reasoning that

> self-autonomy stems in large part from one's ability to articulate and nurture an identity derived from membership in a cultural or religious group. The message put forth by individuals who fall within the ambit [of the hate provisions of the *Code*] represents a most extreme opposition to the idea that members of identifiable groups should enjoy this aspect of the 2(b) benefit. The extent to which the unhindered promotion of this message furthers free expression values must therefore be tempered insofar as it advocates with inordinate vitriol an intolerance and prejudice which views as execrable the process of individual self-development and human flourishing among all members of society (*ibid.* at 763).

[48] See *Keegstra*, *ibid.*, as reaffirmed in *Thomson*, *supra* note 45 at paras. 90-92.

[49] See *Keegstra*, *ibid.* at 746-50.

[50] See *ibid.* at 758.

[51] See *Taylor*, *supra* note 42 at 918.

the expression restricted fostered the protection of target group members and promoted equality, diversity, and multiculturalism in Canadian soeiety;[52] and

(iv) The provisions were tailored to restrict public, rather than private dissemination of the expression in issue and, as such, their likely salutary effects on equality, multiculturalism, and protection of target group members outweighed their deleterious impact on expression.[53]

The Court concluded that the provisions in question were consistent with Canada's international human rights obligations under the *International Convention on the Elimination of All Forms of Racial Discrimination*[54] and the *International Covenant on Civil and Political Rights*,[55] which oblige signatory states to respect freedom of expression and prohibit hate propaganda, suggesting that the two are not necessarily mutually exclusive. The Court further noted that a Human Rights Committee, appointed under the Optional Protocol to the *ICCPR*, dismissed Taylor's complaint that subsection 13(1) of the *CHRA* violated his right to free expression. The Committee held that "the opinions which Mr. Taylor seeks to disseminate through the telephone system clearly constitute the advocacy of racial or religious hatred which Canada has an obligation under article 20(2) of the [*ICCPR*] to prohibit."[56]

Although decided without regard for the Amendments, two recent CHRT decisions under the pre-amendment version of subsection 13(1) of the *CHRA* relied on the *Taylor* and *Keegstra* constitutional analyses to conclude that the provision remains valid, even as applied to hate propagation through World Wide Web

---

[52] The Court found that the provisions were rationally connected to these objectives in three ways. First, limiting or eliminating hate propaganda reduced the risk that target group members would be harmed through direct exposure to it. Second, the restrictions on dissemination of hate propaganda reduced the risk that equality, diversity, and multiculturalism would be undermined through recruitment of Canadians to the cause of racism. Third, the restrictions served to publicly denounce hate propaganda, thereby affirming the Canadian constitutional values of multiculturalism and equality (see *Keegstra*, *supra* note 43 at 769-71; *Taylor*, *ibid.* at 922-24).

[53] In making this determination, the Court emphasized the constitutional imperative of protecting private spheres of communication from undue government intrusion. It noted that the *Code* provisions apply only to comments willfully made *publicly accessible* (see *Keegstra*, *ibid.* at 771-79), and that the *CHRA* provision would likely apply only to public forms of communication given the threshold of "hatred" imposed in the provision (see *Taylor*, *ibid.* at 936-38). The latter conclusion is buttressed by the Court's later decision that human rights code provisions are unlikely to apply to private organizations of intimates. See *Gould v. Yukon Order of Pioneers*, [1996] 1 S.C.R. 571, 133 D.L.R. (4th) 449.

[54] *CERD*, *supra* note 34, art. 4.

[55] *ICCPR*, *supra* note 34, art. 20(2).

[56] *Taylor and Western Guard Party v. Canada*, Communication No. 104/1981, Report of the Human Rights Committee, 38 U.N. GAOR, Supp. No. 40 (A/38/40) 231 (1983), decision reported in part at (1983), 5 C.H.R.R. D/2097.

("WWW") sites.[57] This approach was more recently cited with approval by the CHRT in *Warman*, a case in which there was some question whether the pre-amendment or post-amendment version of subsection 13(1) applied.[58] The prior constitutional conclusions reached in *Taylor* and *Keegstra* continue to apply, perhaps with even greater force, to restrictions on hate propaganda expressed via the Internet.[59] However, despite the constitutionality of the Amendments and pre-existing Code restrictions on hate propaganda in Canada (collectively, the "Canadian Provisions" or "Provisions") and their consistency with Canada's international human rights obligations, the public policy underlying them will be challenged by First Amendment protection against direct restriction of hate propaganda emanating from US servers.

III. First Amendment Protection of Hate Propaganda

The First Amendment states "Congress shall make no law abridging freedom of speech, or of the press," and generally protects hate speech.[60] Under the First Amendment, orders such as those likely to be sought or issued under legislation like the Canadian Provisions would be analyzed in two steps to determine: (i) whether they are directed at the communicative impact of expressive activity, and if so; (ii) whether the expression in question is excluded from First Amendment protection.[61]

Most orders issued under laws like the Canadian Provisions are likely to be aimed at minimizing the communicative impact of Internet hate propaganda, and thus to be considered a prima facie violation of the First Amendment.[62] Their constitutionality would then depend on demonstrating that they are aimed at unprotected expression—

---

[57] *Citron*, *supra* note 10; *Schnell v. Machiavelli and Associates Emprize Inc. and John Micka*, T.D. 11/02 (CHRT). For a more detailed discussion of these decisions, see Jane Bailey, "Of Mediums and Metaphors: How a Layered Methodology Might Contribute to Constitutional Analysis of Internet Content Regulation" Man. L.J. [forthcoming in 2004].

[58] *Warman*, *supra* note 10 at paras. 12-15, 55.

[59] Additional justification for restricting hate propaganda can be found in the Internet's tremendous potential breadth of dissemination, as well as a trend among Internet hate speakers to use key words that might cause unintentional accessing of their sites by unsuspecting Web searchers, presumably in order to attract attention to their "causes". See Breckheimer, *supra* note 13 at 1498-99.

[60] For a more detailed analysis of the evolution of US law relating to hate speech, including the constitutionality of legislation addressing racist expression less directly than the Canadian Provisions (such as increased penalties for racially motivated crimes), see Rachel Weintraub-Reiter, "Hate Speech Over the Internet: A Traditional Analysis or a New Cyber Constitution" (1998) 8 B.U. Pub. Int. L.J. 145 and William B. Fisch, "Hate Speech in the Constitutional Law of the United States" (2002) 50 Am. J. Comp. L. 463.

[61] See Laurence Tribe, *American Constitutional Law*, 2d ed. (Mineola, N.Y.: The Foundation Press, 1988) at 791-94.

[62] See *ibid.*

expression falling within an excluded category or the limitation of which is underlain by a "compelling state interest".[63]

Hate propaganda might have been interpreted to fall within one of the excluded categories identified in early US jurisprudence, such as words of "slight social value", libel, "fighting words", or words creating a clear and present danger of imminent violence.[64] Although the US Supreme Court in one instance found that hate propaganda fell within the libel exclusion,[65] subsequent decisions by US courts, such as that of the US Supreme Court in *R.A.V.*,[66] suggest that the excluded categories will be very narrowly interpreted and explicit restrictions on hate propaganda strictly scrutinized under the First Amendment.[67] Thus, enforceability is likely to depend upon demonstrating a compelling state interest.[68]

It is likely to be difficult for orders under legislation like the Provisions to meet the "compelling state interest" standard currently applied in the United States. US courts have found that direct prohibitions on parading in Nazi dress in a town in which the majority of residents are Jews[69] and on burning a cross on the lawn of a racialized family do not address sufficiently compelling state interests to pass constitutional muster.[70] Further, subsequent decisions suggest restrictions on Internet communication in general will be strictly scrutinized.[71] Nevertheless, some

---

[63] See *ibid.*

[64] See *Schenck v. United States*, 249 U.S. 47 at 52 (1919), 39 S. Ct. 247. See also *Chaplinsky v. New Hampshire*, 315 U.S. 568 at 572 (1941).

[65] See *Beauharnais v. Illinois*, 343 U.S. 250 (1952), 72 S. Ct. 725.

[66] *R.A.V. v. City of St. Paul*, 505 U.S. 377 at 2542-44 (S. Ct. 1992), 112 S. Ct. 2538 [*R.A.V.* cited to U.S.] (finding that the government may not directly prohibit acts that are known or should be known to arouse anger, alarm, or resentment on the basis of race, colour, creed, religion, or gender).

[67] See *Village of Skokie v. National Socialist Party of America*, 366 N.E.2d 347 (Ill. App. Ct. 1977) 51 Ill. App. 3d 279, rev'd in part, 373 N.E.2d 21 (S. Ct. Ill. 1978), 69 Ill.2d 605 [*Village of Skokie* cited to N.E.2d] (affirming the right to parade in Nazi dress, displaying swastikas in a town in which the majority of residents were Jews) and *Black v. Commonwealth*, 262 Va. 764, 553 S.E.2d 738 (following *Village of Skokie*).

[68] See Tribe, *supra* note 61 at 833-34. Orders issued under laws like the Canadian Provisions will only meet the "compelling state interest" test if it is shown that: (i) the state interest was actually considered by the legislator, (ii) a close nexus exists between the means chosen and the state interest to be served, and (iii) the limitation on expression is narrowly drawn. Satisfaction of the second and third criteria will depend largely upon the drafting of any particular order and is therefore more usefully assessed in the context of specific orders. In any event, the latter two criteria will only be relevant if the compelling state interest criterion ean be satisfied.

[69] See *R.A.V.*, *supra* note 66.

[70] See *Village of Skokie*, *supra* note 67.

[71] See *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F.Supp.2d 1181 at 1186 (N.D.Cal. 2001) [*Yahoo! v. Ligue*] (declaring unenforceable a French court order requiring a US-based ISP to prevent French citizens from accessing on-line auctions of Nazi memorabilia) and *Reno v. American Civil Liberties Union*, 521 U.S. 844, 117 S. Ct. 2329 (1997) [*Reno* cited to U.S.] (virtually equating the Internet with the ideal marketplace of ideas, requiring strict scrutiny of restrictions on Internet communication).

restrictions might be found to address the excluded category of expression presenting a clear and present danger of imminent harm, such as hate propaganda taking the form of "true threats" of violence made against a particular individual[72] or of broadly based terrorist threats.[73] The compelling nature of the state interest in regulating the second type of hate propaganda is arguably made more apparent by the September 11 attacks.[74] In either situation, however, an order is likely to be enforceable only where it is clear that the hate propaganda at issue is likely to lead to immediate action without the opportunity to avoid harm through response and discussion.[75]

IV. Conflicting Democratic Visions

The constitutionality of the Canadian Provisions in Canada and the likely unconstitutionality in the US of most orders issued under like provisions demonstrate the fundamentally different approaches to hate propaganda taken by two countries sharing a common commitment to democracy. The constitutional validity of the Provisions in Canada reflects other fundamental democratic values in addition to free expression, including multiculturalism and equality, which are also protected by international human rights instruments such as the *CERD* and *ICCPR*. Although the US is also a signatory to these instruments,[76] most orders issued pursuant to

---

[72] See Weintraub-Reiter, *supra* note 60 at 147-48, citing *U.S. v. Alkhabaz*, 104 F.3d. 1492 (6th Cir. 1997) [*Alkhabaz*].

[73] See Cass Sunstein, "Constitutional Caution" (1996) U. Chicago Legal F. 361 at 366-72.

[74] Like Canada, the US has enacted legislation in response to the 11 September 2001 attacks. The *USA PATRIOT Act* No. 107-56 (26 October 2001) significantly expands surveillance and investigative powers with respect to "terrorism". While the Senate preamble of the act expresses concern for and condemns violent acts toward Arab, Muslim, and South Asian Americans and focuses on electronic communications, none of its provisions parallel the Amendments in terms of restrieting hate propaganda. For an analysis of the act, see Electronic Frontier Foundation, "EFF Analysis of the Provisions of the *USA PATRIOT Act* that Relate to Online Activities" Electronic Frontier Foundation (31 Oetober 2001), online: Electronie Frontier Foundation <http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php>. This legislative signal of national security concerns could prompt a different judicial approach to restrictions on hate propaganda that could be brought within the rubric of terrorism.

[75] See Tribe, *supra* note 61 at 791, 833-34. Moreover, the applicability of this narrow exception is debatable in the Internet context. Some recent US decisions and academic commentary suggest that the physical distance that often separates the speaker from the listener in Internet communications may make it difficult to establish that harm is sufficiently imminent to justify restricting speech: *Alkhabaz*, *supra* note 72; Stuart Biegel, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge, Mass.: M.I.T. Press, 2001) at 339-40.

[76] Although the US ratified the *ICCPR* on 8 September 1992 and the *CERD* on 20 November 1994, it placed reservations on their ratifications, confirming that its obligations under these treaties will be interpreted in accordance with freedom of expression under the *U.S. Constitution*. See United Nations High Commissioner of Human Rights, *Status of Ratifications of the Principal International Human Rights Treaties* (7 July 2003), online: United Nations, Office of the High Commissioner for Human Rights <http://www.unhchr.ch/pdf/report.pdf> and United Nations Treaty Collection, Declarations and Reservations (5 February 2002), online: United Nations, Office of the High Commissioner for Human

legislation like the Canadian Provisions (however tailored and specific) are likely to be considered unenforceable violations of the First Amendment.

The difference in these two approaches does not reflect happenstance. The Court in *Keegstra*, adverted to the US approach to hate propaganda and deliberately chose to follow a different path. The majority reasoned that:

> Where s. 1 operates to accentuate a uniquely Canadian vision of a free and democratic society, however, we must not hesitate to depart from the path taken in the United States. Far from requiring a less solicitous protection of *Charter* rights and freedoms, such independence of vision protects these rights and freedoms in a different way. ... [I]n my view the international commitment to eradicate hate propaganda and, most importantly, the special role given equality and multiculturalism in the Canadian Constitution necessitate a departure from the view, reasonably prevalent in America at present, that the suppression of hate propaganda is incompatible with the guarantee of free expression.[77]

The path chosen by Canadian legislators and approved by the Court is one no less informed by a fundamental commitment to democracy than that adopted by the US Supreme Court. In fact, the Canadian approach, informed as it is by other fundamental and internationally recognized democratic values, such as equality and multiculturalism, arguably reflects a more comprehensive conception of both private and public forces affecting individual liberty than that adopted in the US. As I have suggested elsewhere,[78] materially different determinations as to the proper role of the state underlie the different approaches taken in Canada and the US.

The Canadian approach recognizes both public and private sources of oppression on individual liberty and expressly, through section 1 of the Charter, acknowledges the potential role for government in ameliorating the negative impacts of private sources of oppression on individuals.[79] In contrast, the current US approach[80] focuses almost exclusively on the state as the source of oppression and reflects an inherent distrust of state authority, even when used to address conflicts between groups of individuals.[81]

The cross-border flow of First Amendment protected hate propaganda from the US, facilitated by the Internet, poses a threat to the broader goals of multiculturalism

---

Rights <http://www.unhchr.ch/html/menu3/b/treaty2_asp.htm> (for the *CERD*) and <http://www.unhchr.ch/html/menu3/b/treaty19_asp.htm> (for the *ICCPR*).

[77] *Keegstra, supra* note 43 at 743.

[78] Bailey, *supra* note 57.

[79] Dickson C.J.C. (as he then was) cautioned that "one must be careful not to accept blindly that the suppression of expression [by government] must always and unremittingly detract from values central to freedom of expression" (*Keegstra, supra* note 43 at 765).

[80] See Cass Sunstein, *Democracy and the Problem of Free Speech* (New York: The Free Press, 1995). Sunstein notes that there is more than one historic approach to First Amendment interpretation and that the current First Amendment approach reflects the Holmesian "marketplace" tradition, largely ignoring the Madisonian tradition characterizing freedom of expression as critical to deliberative democraey.

[81] See *R.A.V., supra* note 66.

and equality underlying the particular democratic path consciously adopted in Canada and reflected in international human rights instruments. While the Canadian Provisions will continue to directly serve these broader goals by restricting the activities of the purveyors of hate within Canada, their ability to limit Canadians' access to propaganda emanating from the US will be challenged.[82]

In this way, the First Amendment approach to hate propaganda could be unilaterally exported to Canada and other connected jurisdictions around the world, seriously challenging their public regulatory approaches.[83] The emergence of private regulatory mechanisms presents an opportunity for co-operation between Canada and private actors in the US that may reduce the risk of potential First Amendment hegemony. Although private regulation[84] of on-line expression may effectively *supplement* public regulation, it is not an adequate *substitute*. In the context of on-line hate propaganda, Canadian public regulation aims at achieving broader goals of social harmony and equality that, for reasons discussed below, are not adequately addressed by private actors alone. Public regulation at both national and international levels could insure against the risk of the privatization of important issues of social justice and, through its denunciatory effect, guide the behaviour of private actors, and imbue private regulation with a degree of public accountability.

V. First Amendment Limitations on State-Based International Regulation of Internet Hate Propaganda

The direct efficacy of public regulation of Internet hate propaganda under legislation such as the Canadian Provisions will be limited to the extent that it requires US public enforcement of restrictions on Internet speakers or content.[85] At

---

[82] Shifting the legislative focus to listeners within Canada would require the consideration of a possession offence, possibly emulating current restrictions on child pornography.

[83] For citizens of nations labouring under repressive regimes that restrict expression in order to squelch criticism of governing authorities, the export of the First Amendment may be viewed as democratizing. However, the same analysis does not necessarily apply to other democratic nations whose elected officials have enacted legislation, presumably reflecting the will of the people and, in many cases, checked by the constitutional authority of their courts. See Neil Netanel, "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory" (1999) 88 Cal. L. Rev. 395.

[84] For the purposes of this paper, private regulatory mechanisms refer to what is often characterized as the market (i.e., decisions or agreements arrived at without direct government compulsion). Public regulation refers to government regulation through public laws, including international agreements for state-based action.

[85] Nevertheless, existing regulation continues to be effective with respect to actors and content within Canada. It could be supplemented by other public regulatory mechanisms that are not dependent on extra-territorial enforcement. Canada could, for example, adopt the approach to other types of content taken in countries such as Australia, China, and Singapore, and either directly or through legislated codes of conduct, mandate the erection of firewalls designed to keep out hate propaganda emanating from other jurisdictions. This approach could supplement restrictions on speakers with prohibitions on "knowing access" or digital "possession" of hate propaganda within Canada. However, in addition to the practical limitations associated with technological solutions such

base, Internet hate propaganda presents a classic conflict of laws problem. International agreements seeking to harmonize signatory states' substantive law, procedural law, or both have been one of the key mechanisms for addressing inter-jurisdictional conflicts arising with increasing frequency as a result of the rapid pace of globalization. However, they are likely to bc of limited assistance in addressing First Amendment barriers to regulating hate propaganda. The European Council and other states have been involved in discussions regarding both procedural and substantive international agreements designed to address the heightened problem of inter-jurisdictional conflicts associated with Internet communication. To the extent that they require direct state restriction, they cannot resolve First Amendment barriers. Even if the US were inclined to sign either kind of agreement, both are certain to preserve the right of each signatory state to limit its compliance in accordance with its own public policy and constitutional approach.

A. *Procedural Agreements Calling for State Action:* Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters

The *Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters*[86] reflects an international effort to resolve inter-jurisdictional differences by establishing a reciprocal enforcement mechanism. The convention would provide rules as to when a signatory nation could properly assert jurisdiction over civil and commercial matters.[87] Provided that jurisdiction was assumed according to those rules, other signatory states would be required to cnforce the order issued, subject to certain exceptions.

---

as the mandatory filtering and blocking associated with firewalls, technological regulation and possession offences raise troubling privacy issucs likely to attract intense constitutional scrutiny. The focus of this paper, however, is not on further public national regulatory options, but on exploring the possibility of systematic and publicly accountable *private* enforcement mechanisms. For a more detailed discussion of public national regulatory options, see Jane Bailey, *The Future of Equality in the Age of the Internet: Toward Publicly Accountable Regulation of Hate Propaganda* (LL.M. Thesis, University of Toronto, 2001) [unpublished] and the sources listed therein.

[86] See online: Hague Conference on Private International Law <http://www.hccli.net/e/conventions/draft36e.html> [*Draft Hague Convention*]. As a result of issues arising from this draft, an informal working group was established in April 2002 to provide further working drafts. The first of these relates to the choicc of court in commercial matters. Sce Hague Conference on Private International Law, Permanent Bureau, "Preliminary Result of the Work of the Informal Working Group on the Judgments Project" Preliminary Document No. 8 of March 2003, online: Hague Conference on Private Intcrnational Law <ftp://ftp.hcch.net/doc/genaff_pd08e.pdf>. For a subsequent report on the draft, see Andrea Schulz, "Report on thc Work of the Informal Working Group on the Judgments Project, in Particular on the Preliminary Text Achieved at Its Third Meeting 25-28 March 2003" (June 2003), ouline: Hague Conference on Private Intemational Law <ftp://ftp.hcch.net/doc/jdgm_pd22e.doc>.

[87] *Draft Hague Convention, ibid.*, art.I.

Although not applicable to orders issued under criminal or administrative legislation, such as the Canadian Provisions, models such as the *Draft Hague Convention* could be used for inter-jurisdictional enforcement of restrictions on Internet hate propaganda in a number of ways. They might be used to enforce a civil award for posting material libeling a racially identifiable group in one jurisdiction against a speaker in another jurisdiction. They could also be used to enforce a damage award issued in one jurisdiction for failing to provide an on-line environment free from racial discrimination against an ISP[88] in another jurisdiction.

However, it is unlikely that these procedural mechanisms would be significantly more effective than the Canadian Provisions alone in restricting cross-border flows of hate from the US. Signatory states are certain to be explicitly entitled to refuse to enforce or recognize foreign orders they consider "manifestly incompatible with [their] public policy."[89] The US could be expected to rely on a provision such as this to refuse to enforce orders restricting hate propaganda.[90]

B. *International Agreements Harmonizing Substantive Law:* The Additional Protocol to the Cybercrime Convention

In 2001, thirty-three nations, including Canada and the US, signed the *Cybercrime Convention*, which provides, among other things, for the harmonization of laws among signatory states with respect to computer crimes and child pornography on the Internet.[91] While a number of European nations pressed for inclusion of a provision relating to hate propaganda during initial negotiations, the US successfully resisted, citing First Amendment concerns.[92] Recent experience regarding the Additional Protocol suggests the improbability of a state-based

---

[88] As discussed in greater detail, *infra*, a customer unsuccessfully sued AOL on the basis of this cause of action in the US. For the pleading, see Statement of Claim for *Noah v. AOL Time Warner* (August 2001), online: Council for American-Islamic Relations <http://www.cair-net.org/downloads/aol.pdf> and for the decision dismissing the claim summarily, see *Noah v. AOL Time Warner Inc.*, 261 F. Supp. 2d 532 (E.D. Va. 2003) [*Noah*].

[89] *Draft Hague Convention*, *supra* note 86, art. 28(1)(f).

[90] As it has done with respect to the *ICCPR*, *supra* note 34, and the *CERD*, *supra* note 34. Similar concerns arise with respect to proposed common law tests for determining whether a court should accept jurisdiction in any given case. With respect to "targeting", see Michael Geist, "Is There a There There? Toward Greater Certainty for Internet Jurisdiction" (2002) 16 Berkeley Tech. L.J. 1. Even if a US court were to accept that a Canadian court properly asserted jurisdiction over a Web site targeted at Canadians, public policy considerations would likely prevent enforcement of the Canadian judgment in the US. Furthermore, in the hate propaganda context, where the speaker's objective often appears to be to target anyone who will listen, it may be difficult to identify a "target" to establish jurisdiction.

[91] *Cybercrime Convention*, 23 November 2001, Eur. T.S. No. 185, art. 9, online: Council of Europe <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

[92] Carl S. Kaplan, "New Economy: Bracing for a Flood of Efforts to Control Speech Seen as Hateful or Terrorist" *The New York Times* (11 February 2002) C3, online: The New York Times <http://www.nytimes.com>.

international response to potential First Amendment hegemony over Internet hate propaganda.[93]

The COE approved the Additional Protocol in January, 2003.[94] It requires, subject to certain reservations, that signatory states establish criminal offences for using a computer system to:

a. Make racist and xenophobic material publicly available;
b. threaten a serious criminal offence against or publicly insult a person or persons due to their membership in a group distingnished by race, colour, descent or national or ethnic origin;
c. deny, grossly minimize, approve of, or justify acts of genocide or crimes against humanity; and
d. aid and abet commission of any of these offences.[95]

It defines "racist and xenophobic material" to include written material, images, and other representations of ideas or theories advocating, promoting, or inciting hatred, discrimination, or violence against an individual or group based on race, colour, descent, or national or ethnic origin, as well as on religion to the extent it is used as a "pretext" for the other factors.[96]

By June, 2003, sixteen COE members had signed the Additional Protocol, although none of the non-member states (including Canada) had done so.[97] Even before its approval by the COE, the Bush administration announced that the US would not support the Protocol, again citing First Amendment concerns.[98] At least in the short-term, there is likely to be little remaining political will on the part of the US and COE member states to negotiate any form of international agreement calling for state harmonization of substantive law with respect to Internet hate propaganda. In any event, so long as international agreements, such as the Additional Protocol, permit each signatory state to restrict compliance with its obligations according to its own public policy, this kind of arrangement is unlikely to expand the seope of legally

---

[93] US refusal to sign the Additional Protocol, however, does not necessarily indicate that there is no opportunity to harmonize national laws on this issue. The protocol would require legal restriction of broad categories of expression that are not restrictable under the current First Amendment approach. That is not to say, however, that there ean be no co-operation, at least with respect to the narrow category of hate propaganda not subject to First Amendment protection. The US Supreme Court's decision in *U.S. v. American Library Association, Inc.* 123 S. Ct. 2297, 156 L. Ed. 2d 221 [*American Library* cited to S. Ct.], *may* also signal the possibility of restricting hate propaganda indirectly by making requirements to limit its dissemination a condition of receiving federal funding or government contracting opportunities.

[94] *Additional Protocol*, *supra* note 18.

[95] *Ibid.*, arts. 4-7. The *Additional Protocol* specifically permits signatories to make reservations to avoid eriminalizing the acts referred to in paras. (a) to (c), except for racially motivated threats.

[96] *Ibid.*, art. 2.

[97] See Chart of signatures, *supra* note 18.

[98] See Declan McCullagh, "U.S. Won't Support Net 'Hate Speech' Ban" *CNET News.com* (15 November 2002), online: CNET <http://news.com/com/2100-1023-965983.html>.

enforceable restrictions against hate propaganda emanating from the US. Nevertheless, the Additional Protocol serves as an important first step in addressing on-line hate propaganda and, to the extent it is widely ratified, may have persuasive value in the development of US law and policy on this issue.

While the First Amendment limits the prospect for direct international public regulation, private actors are not generally confined by constitutional restraints. Some private actors in the US have in fact voluntarily undertaken to regulate on-line expression, even in the absence of any legal compulsion to do so, opening up a private and largely unscrutinized avenue for enforcement.

VI. Emerging Private Regulation

Private actors in the US and elsewhere are regulating on-line expression through technological solutions (such as filtering and zoning), terms of use clauses in service contracts, and self-regulatory organizations. While private regulation, generally free from First Amendment compliance constraints, constitutes a poor substitute for public regulation for both practical and policy reasons, the growing problem of Internet hate propaganda suggests the need to consider both public and private strategies.

A. Privately Implemented Technological Solutions

The two perhaps most frequently discussed technological measures for addressing unwanted Internet content are filtering and zoning.[99] Filtering enables those at the receiving end of Internet communications to block content from being delivered to them.[100] Zoning, which aims at a different link in the communication chain, permits speakers to prevent certain users from accessing their content.[101] Critics have questioned the technical ability of both measures to effectively disrupt the delivery of particular content. Nonetheless, private implementation of filtering or zoning at the user or ISP level has been the subject of a good deal of positive commentary as a facilitator of individual choice.[102]

It will be suggested, however, that private implementation of filtering and zoning fails to address the key social harms of concern in the context of hate propaganda: the threat to social harmony and equality posed by widespread adoption of hate propaganda's message. Further, where implemented at the ISP level, filtering and

---

[99] It is notable, however, that much of the discussion surrounding zoning and filtering focuses on World Wide Web content. This need not be the case, as certain of these solutions can also be applied to other Internet applications. For a relatively complete (albeit dated) discussion of this issue, see U.S., Commission on Online Child Protection, *Final Report of the COPA Commission* (20 October 2000), online: Commission on Online Child Protection <http://www.copacommission.org/report>.

[100] See Lessig, *supra* note 1 at 175-76.

[101] See *ibid.*

[102] See *e.g.* Weintraub-Reiter, *supra* note 60.

zoning may be associated with the collection of private information with little or no opportunity for public scrutiny.

1. Filtering

Individuals, organizations (such as ISPs[103]), or even countries (such as China) can implement filtering, either to allow access only to materials identified as acceptable or to block delivery of materials identified as unacceptable.[104] In order to block prohibited Internet content, someone, either the content provider or a third party, has to rate it and apply labels to be read by users' software applications. To the extent that the user has chosen a software application configured for blocking certain content, the application will deny access to that content based on the label attached to it.

Internet industry filtering initiatives in the early 1990s were largely designed to address public concern about the ready availability of Internet content considered harmful to minors.[105] The concept behind some of these efforts was to facilitate individual user choice in accessing content, including choice not only in configuring blocking preferences, but also in selecting rating systems compatible with personal values and preferences.[106] The basic approach was to enable individual users to filter out offensive content without interfering with the ability of others to aecess that content should they so choose.

The current state of the art in filtering liinits its efficacy. With the number of Web pages alone growing exponentially, the sheer scope of the labelling project is daunting to say the least,[107] and technologies, such as encryption, permit users to

---

[103] America Online, for example, relies on the software package produced by RuleSpace, a filtering system capable of surveying the content of up to 47 million Web pages a day, to power the parental control features that it markets as part of its service to subscribers: Jeffrey Benner, "AOL's New Filter on the Block" *Wired News* (7 May 2001), ouline: Wired <http://www.wired.com/news/privacy/0,1848,43576,00.html>.

[104] Blocking might be carried out on a number of bases such as blocking reception of content labelled hate propaganda, blocking all content emanating from a particular Uniforin Resource Locator ("URL"), or blocking key words associated with hate propaganda.

[105] See World Wide Web Consortium ("W3C"), "Statement on the Intent and Use of PICS: Using PICS Well" (1 June 1998), online: W3C <http://www.w3.org/PICS/>.

[106] For example, non-governmental human rights groups, such as the Anti-Defamation League ("ADL"), also manufacture filtering software, some of which is available free of charge on the Internet. The ADL's filtering program, known as HateFilter, allows consumers to filter Web content based on the ADL's philosophical approach and values. See Gwendolyn Mariano, "Anti-Hate Group Updates Web Filter" *CNET News.com* (21 March 2002), online: CNET <http://news.com.com/2102-1023-866153.html>.

[107] In the context of anti-social speech such as hate propaganda, leaving accurate labelling to speakers is probably unrealistic. To the extent that the objective of hate propagandists is to reach as wide an audience as possible, in the absence of public compulsion, they may have little incentive to accurately label their content.

circumvent filters imposed by others.[108] Further, the task of labelling either leaves out critical aspects of human judgment (such as recognizing the importance of context) or is done highly subjectively and with little opportunity for users to understand the nuanced criteria employed by the labeler.[109] Given the exigencies of rating and labelling, as well as circumvention techniques, expert evidence called at one US trial suggested that, at that time, filters excluded innocuous material twenty-one per cent of the time and offensive material only sixty-nine per cent of the time.[110] Figures such as these may raise practical concerns about the current advisability of primary reliance on privately implemented filtering technology[111] as a mechanism for addressing Internet hate propaganda.[112]

More importantly, privately implemented filtering is inconsistent with at least one material objective underlying the Canadian Provisions. It may be appropriate to encourage private implementation of filters configured to reflect individual preferences in relation to *legal* eontent offending a particular user.[113] However, Canadian restrictions on hate propaganda are not aimed solely at ensuring that

---

[108] See Internet Law & Policy Forum, *The Internet Law and Policy Forum Working Group on Content Blocking* (May 1997), online: ILPF <http://www.ilpf.org/groups/content/tech.htm>.

[109] For a more thorough discussion of the criticisms of rating, see Jonathan Weinberg, "Rating the Net" (1997) 19 Hastings Comm. & Ent. L.J. 453, online: Wayne State University Law School <http://www.law.wayne.edu/weinberg/rating.htm>.

[110] Reuters, "Experts Lambaste Smut Filters" (26 March 2002) *Wired News*, online: Wired <http://www.wired.com/news/business/0,1367,51338.00.html>; *American Library*, *supra* note 93. Despite figures suggesting over-blocking, the US Supreme Court upheld legislation mandating public libraries to filter content harmful to minors as a condition for receiving federal funding, noting that adult patrons could request that the filters be disabled.

[111] On the other hand, if we were to examine the efficacy of legal restrictions alone, we might find that technological solutions consistently delivering 69 per cent efficacy in eliminating access to offensive material compare quite favourably with the results of legislative prohibitions.

[112] See Lawrence Lessig & Paul Resnick, "Zoning Speech on the Internet: A Legal and Technical Model" (1999) 98 Mich. L. Rev. 395. For these same practical reasons, the publicly compelled use of filters, either by individual users, ISPs, or govemment is an unlikely policy alternative in the short term. In addition, privacy concerns arise in the context of publicly mandated filtering, to the extent that such measures require or encourage ISPs or governments to monitor the content accessed by individual subscribers. Although international protocols obliging signatory nations to impose accurate labelling requirements on their citizens could assist in the daunting task of content labelling, without changes in the state of the art of the filtering software itself, questions remain as to both the efficacy of this approach and the more pressing issues of the risks of monitoring and concerns about invasion of privacy.

[113] For regulatory purposes, there is an important distinction between illegal content and legal, but offensive, content. The European Council has conceptually segmented illegal from merely harmful content, recognizing that the two merit different regulatory responses. See Beth Simone Noveck, "European Forum on Harmful and Illegal Cyber Content: Rapporteur's Report," online: Council of Europe <http://www.coe.int/T/E/Human_Rights/media/4_Cyberfora/1_Self-regulation/1_European_Forum/2_Reports_&videos/reports.asp>. While the categorization of illegal versus harmful is not a particularly meaningful one given that content is often determined to be illegal because it is harmful, the attempt to delineate may be helpful in thinking about regulatory options.

individual listeners are not offended or directly harmed. They also focus on reducing or eliminating the risk of harm to the broader societal goals of equality and multiculturalism posed by widespread adoption of hate propaganda's message.[114] While filtering controlled by individual users or their ISPs may mitigate the psychological harm suffered by target group members by reducing the risk that they will be exposed to hate propaganda, it does not address these broader societal concerns. Further, individually implemented filtering of hate propaganda makes it invisible to those who might otherwise be mobilized to address it, while the hate propaganda industry itself is permitted to thrive among those with attitudes that pose the greatest risk of social harm.

2. Zoning

Internet speakers may prevent certain recipients from accessing their content based on specific user characteristics. Technological developments facilitate recognition of personal characteristics of the user (such as age), as well as the user's geographic location (referred to as "geolocational" technology). Zoning based on the user's personal characteristics could, for example, assist a speaker in prohibiting a child from accessing adult content posted on a Web site. Geolocational technology assists speakers in denying access to users in countries where the content they seek to access is illegal.[115]

Significant Internet industry players, such as AOL Time Warner Inc. ("AOL") and Google, rely on zoning software applications to build user profiles based on hundreds, and even thousands, of demographic attributes of Web site visitors.[116] Others, such as on-line gambling businesses, use geolocational technology to deny access to those in jurisdictions where their content is prohibited or subject to severe restriction.[117] Similarly, US-based hate speakers or ISPs providing Internet services to hate speakers could implement geolocational technology to prevent citizens in countries where it is illegal from accessing that content.[118] However, while some ISPs not creating their own content may be so inclined, hate speakers are unlikely to implement zoning technology. Businesses offering on-line gambling are likely to be

---

[114] See *Taylor*, *supra* note 42; *Citron*, *supra* note 10; *Keegstra*, *supra* note 43.

[115] For a more complete discussion of zoning software applications, see Geist, *supra* note 90.

[116] See *e.g.* Digital Envoy, Press Release "Digital Envoy Announces NetAcuity 3.0 Geo-Intelligence Solution: Flexible Data Modules Offer Increased Targeting Depth" (29 April 2002), online: Digital Envoy <http://www.digitalenvoy.net/press_room/press_releases/2002/pr_042902.shtml>.

[117] See Ariana Eunjung Cha, "Rise of Internet Borders Prompts Fears for Web's Future" *The Washington Post* (4 January 2002) E01, online: The Washington Post <http://www.washingtonpost.com>.

[118] See Jack Goldsmith, "Against Cyberanarchy" (1998) 65 U. Chicago L. Rev. 1199. It has, however, been rightly pointed out that the effective enforcement of territorially-based laws would require content providers to be aware of the laws in every country and to tailor their content to meet them. As Goldsmith indicated, though, businesses operating in multiple jurisdictions are required to, and do, familiarize themselves with local regulations and refuse to comply with them at their peril.

primarily motivated by economic return and thus be adverse to negative publicity, as well as expenditures for defending against prosecution for violation of the laws of other jurisdictions.[119] Hate speakers may be less motivated by economic returns and more interested in self-aggrandizement and attracting a following, goals that may well cause them to disregard the potential legal consequences of their actions, particularly to the extent that they understand that the First Amendment protects them.

Like filtering, zoning has been squarely criticized for technical reasons. Technologies designed to circumvent geolocational technology abound,[120] not to mention logical flaws identified in certain software.[121] At a more philosophical level, zoning has been criticized for contributing to the balkanization of the Internet, by re-enabling enforcement of territorially based laws, a result inconsistent with the original anarchic sentiments of many Internet stakeholders.[122] Perhaps of more concern are the risks to privacy presented by these technologies, to the extent that they facilitate the often unauthorized collection of pools of potentially quite personal data, including user location.[123]

B. Acceptable Use Policies

A number of ISPs require their subscribers to abide by acceptable use policies ("AUP"s), some of which include expected standards respecting on-line behaviour possibly applicable to hate propaganda. These kind of provisions have been primarily

---

[119] The perceived risk of prosecution may be greater in the context of US-based on-line gambling services, since gambling laws vary from state to state, but may well be enforceable against residents in other states.

[120] See "Putting It in Its Place", *The Economist* (11 August 2001) at 18, online: The Economist <http://www.economist.com/>. Users can evade geolocational technology by accessing sites through computers in other countries, enerypting or anonymously sending their e-mail, and/or using software to cloak their on-line identities.

[121] See Anick Jesdanun, "The Potential and Peril of National Internet Boundaries" *The San Francisco Examiner* (4 March 2001), online: The San Francisco Examiner <http://www.examiner.com>.

[122] See Joel R. Reidenberg, "The Yahoo! Case and the International Democratization of the Internet", Fordham Law & Economics Research Paper No. 11 (April 2001), online: Social Science Research Network Electronic Library <http://papers.ssrn.com/sol3/delivery.cfm/SSRN_ID267148_code010419520.pdf>. Reidenberg, however, has argued eompellingly that effective territorially based regulation of Internet activity acts as a democratizing force, returning decisions about what rules should govern from an elite technocracy to the officials of sovereign nations.

[123] Publicly compelled zoning at the national level is implausible, as Canada is a single zone with respect to current restrictions on hate propaganda. As such, it would make little sense for the Canadian government to require hate speakers within the country to screen out Canadian users seeking access. At the international level, while jurisdictions could agree to co-operate in cross-border zoning, it is unclear whether such measures would survive US First Amendment scrutiny, particularly in the hate propaganda context. However, at least one member of the US Supreme Court has not ruled out the possibility that publicly mandated zoning on the Internet may be constitutional (see Lessig & Resniek, *supra* note 112).

motivated by efforts to immunize these businesses and organizations from liability that may flow from certain types of on-line conduct by their customers (particularly defamation).[124] One US court has suggested that, from a First Amendment perspective, AUPs may be preferable to government regulation for achieving the public policy objective of limiting young library patrons' access to harmful content.[125] However, as the following analysis of AOL's AUP demonstrates, AUPs are at best likely to play only a limited role in restricting Internet hate propaganda.

1. The America Online Model

AOL is a provider of on-line services, including e-mail and chat rooms. To subscribe for its services, customers must agree to AOL's "Terms of Service", which include a "Membership Agreement" and "Community Guidelines" ("Guidelines") that outline rules and expected standards of on-line behaviour. The Terms of Service specify that AOL does not pre-screen content posted to its site and reserves for itself the decision to remove or block access to harmful or offensive Internet content. Violation of the Guidelines may result in AOL issuing a warning to the member or unilaterally terminating the member's service.[126]

The Guidelines begin by stating:

> Like any city, we take pride in—and are protective of—our community. That's why our community standards are important. Communities of all sizes rely on civic pride and the duty of all citizens to help with things like picking up litter, getting out of the way of ambulances, reporting crime, and abiding by the law. These Community Guidelines tell you what you can expect from AOL, as well as the kind of on-line behavior we expect of you.[127]

They specify that AOL takes no responsibility for content that is not removed, and explicitly state that "the AOL Community Guidelines ... including AOL's enforcement of those policies, are not intended to confer, and do not confer, any rights or remedies upon any person."[128] As a result, AOL reserves its right to remove the content, warn members, and/or terminate their service where their behaviour is inconsistent with community standards, but does not confer on members any legal right to insist on enforcement against other members. Nevertheless, the Guidelines

---

[124] Their aggressive implementation has been described as an attempt to "manage, avoid and/or mitigate every potential risk imaginable" (Karen K. Harris, "Issues for Healthcare Companies When Contracting with ASPs" (2001) 19 J. Marshall J. Computer & Info. L. 569 at 584). Note, however, that ISPs in the US are also statutorily protected from liability in certain situations. See *Telecommunications Act of 1996*, 47 U.S.C. § 230.

[125] *American Library*, *supra* note 93.

[126] AOL, "Member Agreement", online: AOL Legal Department <http://legal.web.aol.com/aol/aolpol/memagree.html> [AOL, "Member Agreement"].

[127] AOL, "Community Guidelines", AOL Legal Department online: <http://legal.web.aol.com/aol/aolpol/comguide.html> [AOL, "Community Guidelines"].

[128] AOL, "Member Agreement", *supra* note 126.

request that members report content that may violate the standards and state explicitly that "[h]ate speech is never allowed,"[129] specifying, in material part, that service may be terminated for members who:

> Harass, threaten, embarrass, or do anything else to another member that is unwanted. This means: don't say bad things about them, don't keep sending them unwanted Instant Messages, don't attack their race, heritage, etc. If you disagree with someone, respond to the subject, not the person.
>
> Transmit or facilitate distribution of content that is harmful, abusive, racially or ethnically offensive, vulgar, sexually explicit, or in a reasonable person's view, objectionable. Community standards may vary, but there is no place on the service where hate speech is tolerated.[130]

The Guidelines articulate a "zero tolerance policy" with respect to illegal behaviour by members, warning them that AOL will terminate their service and cooperate with law enforcement authorities. Members are admonished to obey off-line rules, including the law of foreign jurisdictions, when on-line. Again, however, this aspect of the Guidelines is not couched in language that would permit members to *require* AOL to enforce it.

The Guidelines for members are buttressed by terms and conditions of use purportedly binding all users[131] of any communication services offered through AOL's site, including chat rooms, message boards, and newsgroups, to its rules of user conduct ("Terms and Conditions").[132] The Terms and Conditions prohibit using AOL's site for an unlawful purpose, including uploading, posting, or otherwise distributing or facilitating distribution of any content that is, among other things, unlawful or threatening, or that "victimizes, harasses, degrades, or intimidates an individual or group of individuals on the basis of religion, gender, sexual orientation, race, ethnicity, age, or disability."[133] While the Terms and Conditions reiterate that AOL does not generally pre-screen, monitor, or edit the content that may be available through its site, they reserve to AOL the sole discretion to remove any content that, in its judgment, does not comply with the Terms and Conditions or is "otherwise harmful, objectionable, or inaccurate."[134]

---

[129] AOL, "Community Guidelines", *supra* note 127.

[130] *Ibid.*

[131] The term "user", as opposed to "member", presumably is intended to secure "agreement" as to AOL's discretion with respect to content from non-members, who are not bound by the Membership Agreement and the Guidelines.

[132] AOL, "AOL.com Terms and Conditions of Use", online: AOL.com <http://www.aol.com/copyright.adp>.

[133] AOL, "Agreement to Rules of User Conduct", online: AOL.com <http://www.aol.com/copyright/rules.html>.

[134] *Ibid.*

AOL has an administrative mechanism through which complaints relating to content are reviewed and decided upon.[135] While providing a potential avenue for private enforcement of restrictions on hate propaganda emanating from AOL's site in the US, the language of the Guidelines and Terms and Conditions minimizes the opportunity for consistent enforcement.

2. Limitations on Effective Restriction Through AUPs

Effective restriction of the dissemination of Internet hate propaganda from the US through private enforcement of relevant provisions in AUPs, such as AOL's, is limited in that they are drafted to maximize flexibility for ISPs. Provisions restricting on-line conduct can be expected to be drafted to impose obligations on users, while preserving the discretion of the ISP to determine both whether those obligations have been satisfied and whether any penalty is appropriate in the circumstances.[136] AOL's AUP provides an important illustration of this point.

Unlike many other ISPs, AOL is certainly not known for taking an anarchie, "anything goes" approach to on-line conduct. In fact, it has been criticized for taking quite the opposite approach to create a very "managed" community. In particular, critics note AOL's purported attempt to extend its Terms and Conditions beyond its subscribers to the wider body of Internet users that may access its on-line services.[137] Even AOL's AUP, however, preserves significant discretion for AOL to determine what constitutes unacceptable behaviour and whether to impose penalties. AOL has made clear that it does not consider itself bound by its Terms of Service to take any action at all in relation to hate speech on its site, and was successful in obtaining a court ruling to that effect.[138]

---

[135] For an insider's perspective on the functioning of this internal mechanism, see Rita Ferrandino, "Terms of Service: Sweaty Scenes from the Life of an AOL Censor" *The Village Voice* (27 March 2001), online: <http://www.villagevoice.com/issues/0112/ferrandino.php>.

[136] Further, the anti-regulation culture prevalent among many ISPs, particularly smaller independent ones, as well as often limited financial resources, may lead them not to impose AUPs or, at minimum, to ensure they have plenty of scope to avoid imposing penalties in relation to conduct-based restrictions.

[137] See *e.g.* Janelle Brown, "Velvet Rope Bolts over AOL 'Censorship'" *Wired News* (23 July 1997), online: Wired <http://www.wired.com/news/culture/0,1284,5420,00.html>; Rhoda Yen, "Free Speech on the Internet: Regulating Web Authorship by Students" (2000) Computer L. Rev. & T. J. 61.

[138] See *Noah*, *supra* note 88 at 535, in which the court summarily dismissed a former AOL member's claim that AOL had violated its Terms of Service and was discriminating in the provision of a public service by refusing to remove anti-Muslim slurs made in two AOL chatrooms between 1999 and 2001. Although the court dismissed the claim, its reasons confirmed Noah's position that the comments complained of were "offensive, obnoxious and indecent". It is possible, however, that ISPs could be held liable for false or deceptive trade practices if they fail to deliver on promises of "hate-free" environments made in their AUPs and other marketing material: *Federal Trade Commission Act*, 15 U.S.C. §45.

C. US-Based Self-Regulatory Organizations

Private regulation by Internet intermediaries is not limited to contractual restrictions implemented by individual ISPs. ISPs, frequently in efforts to stave off public regulation, have formed self-regulatory organizations. Some of these organizations impose codes of eonduct that require members to take various lcvels of action in rclation to illegal and offensive eontent emanating from their subscribers, including co-operating with hotlines receiving reports from Internet users. While many ISP organizations are tcrritorially based in particular jurisdictions around thc world, some have formed co-operativc links with organizations from othcr jurisdictions. These organizations, again, present the prospect of relying on privatc actors to assist in restricting Internet hate propaganda. Given the focus of this paper on mechanisms for addressing hate propaganda emanating from the US, this section will focus on US-based organizations.

1. ISP Organizations in the US

New Commerce Communications reported, as of June 2003, three national and thirteen state ISP organizations in the US.[139] Of the national associations, only one—the United States Internet Service Providers Association ("USISPA")—provides direct guidance to members with respect to content regulation, and none provides a code of conduct for mcmbers. Of the thirteen state ISP organizations, it appears that only two—Florida and Virginia—even tangentially address the issue of content. The Florida ISP Association provides members with a specific code of ethics that encourages compliance with laws and the reporting of on-line obscenity through a hotline.[140] The Virginia ISP Alliance provides standards of excellence for members, which encourage them to maintain free expression and privacy.[141] Although the USISPA is the American association most directly addrcssing eontent regulation

[139] These national organizations include the Internet Service Providers' Consortium, the American ISP Association, and the USISPA. State organizations are reported in California, Colorado, Florida, lowa, Missouri, Nevada, New Hampshire, New Mexico, Ohio, Texas, Virginia, Washington, and Wisconsin. See New Commerce Communications, "The Internet's Most Complete Site of ISP Business Organizations and Associations" (2003), online: <http://www.com-broker.com/modules.php?name=Links>. In addition, the New York State Telecommunications Association, Inc. includes ISPs as its members: online: NYSTA <http://www.nysta.com/member_directory_Details.asp>.

[140] Florida Internet Service Providers Association, "Code of Ethics" (2003), online: <http://www.fispa.org/public/codeofethics.asp>. Morality in Media, Inc. operates the obscenitycrimes.org Web site, which provides a mechanism for reporting potential online violations of US obscenity laws, and for requesting their investigation by a US Attorney General. The site indicates that US attorneys' offices received 2,232 reports of on-line obscenity in May 2003 and a total of 24,929 in the period from June 2002 through May 2003 (Morality in Media, Inc., "Number of Reports to US Attorneys' Offices June 2002 thru May 2003" online: obscenitycrimes.org <http://www.obscenitycrimes.org/complaint/ObscCrimesReports-Jun02-May03.htm>).

[141] Virginia ISP Alliance, "Standards of Excellence" (2003), online: Virginia ISP Alliance <http://www.vispa.org/standards.cfm>.

(albeit very vaguely), neither it, nor any of the other US-based associations require their ISP members to report on their activities with respect to restricting or reporting offensive or illegal Internet content.

The USISPA was formed in January 2002 by several large ISPs, including AOL, Verizon, and Earthlink, to focus on issues of significance to large service providers, including obligations relating to domestic and international law enforcement initiatives.[142] Rather than implementing codes of conduct with respect to individual members' addressing illegal or offensive content, the USISPA has articulated "founding principles" relating to Internet content. Unsurprisingly, these principles reflect a desire to maximize flexibility for ISPs in relation to content, while immunizing them from liability for that content. The principles state:

- As a general rule, liability for Internet content should rest with the creator or initiator of the illegal content and not with an entity that retransmits, hosts, stores, republishes, or receives such content.
- When serving as conduits for Internet traffic in transit, ISPs should have no liability or responsibility for the content of such traffic. However, ISPs should have the right to block or filter such traffic in order to protect the interests of the ISP or others and should obtain "Good Samaritan" immunity from liability for such action.
- When serving as the hosts for Internet content, whether on a website, news group, chat room, third-party transaction site or other application, ISPs should have no liability for content that was not created by the ISP. But ISPs should accept responsibility for disabling access to such hosted content in accordance with procedures in an applicable law, such as the Digital Millennium Copyright Act, or a court order. ISPs should retain the right to voluntarily disable access to content that they host and should obtain "Good Samaritan" immunity from liability for such action.
- An ISP's obligation to disable access to hosted content should be based upon: (a) clear and specific identification of the content in question; (b) the technical and economic feasibility of disabling access to the content in question; and (c) a legal framework or court order establishing the ISP's obligation to disable access to the content in question, and immunity from liability if they do so.
- As a general rule the law applicable to Internet content should be the law of the jurisdiction in which the content is stored. Such a rule creates predictability and incentives for safe and secure electronic commerce.[143]

Further, although the USISPA is allied formally with the European Internet Service Providers Association ("EuroISPA"), an umbrella group of ISP associations ("ISPAs") from throughout the EU, it would not appear that participation in the

[142] David McGuire, "ISP Giants Form New Lobbying Group" *Newsbytes* (14 January 2002), online: USISPA <http: //www.cix.org/articles.html>.

[143] USISPA, "USISPA Founding Principles", online: USISPA <http://www.cix.org/founding.html>.

alliance requires any particular form of content regulation by USISPA members.[144] While there is no indication that members of the USISPA are required to co-operate with hotlines situated in either the US or the EU, the US is an associate member of the Internet Hotline Providers Association of Europe ("INHOPE"), a co-opcrative of EU based hotlines focusing largely on on-line child pornography.[145]

2. Limitations on Effective Enforcement Through US ISPAs

There appears to be no internal mechanism for enforcing USISPA member compliance with its broad statements about content regulation. Indeed, an enforcement mechanism would make little sense, given the breadth of discretion reserved to members with respect to content regulation. Nevertheless, the USISPA's decision to ally itself with EuroISPA and its constituent members may create an opportunity for pressuring USISPA members to comply with reasonable requests to remove offending material, either through hotlines or direct requests between associations. Restricting dissemination of Internet hate propaganda through existing hotline arrangements, however, may be of limited efficacy in the short-term in two respects. First, hotlines currently focus predominantly on child abuse and child pornography, rather than hate propaganda, except in cases such as the UK where on-line racist incidents are reportable.[146] Second, to the extent that US-based hotlines such as www.obscenitycrimes.org focus on reporting content that may be illegal in the US, most forms of hate propaganda are unlikely to be addressed.

D. Ad Hoc US ISP Responses to Extra-Territorial Public Policy

US-based ISPs have voluntarily undertaken on an ad hoc basis to address content considered illegal in other jurisdictions. In the first case, US-based ISPs have voluntarily agreed to proactively monitor and take measures to disable access to Internet content likely to be deemed illegal or offensive according to the public policy of the nation in which they are operating, albeit without the express benefit of a public determination with respect to the legality of the content. In the second situation, US-based ISPs have removed Internet content from US servers following court or tribunal pronouncements of illegality in other jurisdictions. While the latter type of response better ensures public accountability and transparency, both demonstrate that regardless of issues of legal enforceability, public regulation continues to play an important role in regulating Internet content by guiding private decision-making.

---

[144] The precise terms of the memorandum between the USISPA and EuroISPA have not been located. However, even with respect to its EU members, EuroISPA has left content regulation to eaeh national association. See online: EuroISPA <http://www.euroispa.org>.

[145] See online: INHOPE <http://www.inhope.org/english/about/membership.htm>.

[146] See Internet Watch Foundation, "Internet Watch Foundation Annual Review 2002", online: Internet Watch Foundation <http://www.iwf.org.uk/about/annual_report/annual2002.htm>.

1. "Pledging" Proactive Observance of "Local" Laws

Three hundred ISPs operating in China, including US-based Yahoo!,[147] recently signed a "Public Pledge on Self-Discipline" ("Pledge"),[148] which requires them to: "abide by the state regulations on Internet information service management conscientiously [and refrain from] producing, posting or disseminating pernicious information that may jeopardize state security and disrupt social stability ... [or] establishing links to Web sites that contain harmful information."[149] In fulfilling these obligations, members are expected to "inspect and monitor the information on ... domestic and foreign websites ... [and] refuse ... access to those Web sites that disseminate harmful information."[150] Prospective violations of the Pledge are reportable to an executing agency, vested with authority to investigate and publish findings, as well as to revoke membership in some circumstances.[151]

The Pledge seems to require ISPs to make private decisions as to the legality in China of content that they host or to which they provide access. The Pledge itself is obviously not a mechanism for addressing Internet hate propaganda flowing into Canada. Further, it is limited in scope to the operations of US-based ISPs outside of the US. It does not explicitly impose a duty to eliminate offensive or illegal content from servers located within the US, but simply to work toward disabling access to that content in China. Nevertheless, it presents a model to be considered in terms of US-based ISP operations within Canada. It is suggested, however, that voluntary agreements to reactively address hate propaganda in response to public determinations, described in subsection 2, are preferable with respect to public accountability.

2. Private Enforcement in Response to Public Decisions

A French court ordered US-based ISP, Yahoo!, to take measures to prevent French citizens from accessing on-line auctions of Nazi memorabilia.[152] The memorabilia included items featuring swastikas and other Nazi-related symbols that violate French penal code restrictions on racist content. Even before Yahoo! successfully challenged the enforceability of the French court order under the First

---

[147] See "Yahoo's China Concession" Editorial, *The Washington Post* (19 August 2002) A12, online: The Washington Post <http://www.washingtonpost.com>.

[148] Digital Freedom Network, "Pledging Self-Discipline" (1 April 2002), online: <http://web.archive.org/wcb/20030605113002/www.dfn.org/voices/china/selfdiscipline.htm>.

[149] Digital Freedom Network, "Public Pledge for Self-Discipline for China Internet Industry" (1 April 2002), art. 9, online: Archive.org <http://web.archive.org/web/20030217152053/http://www.dfn.org/voices/china/selfdiscipline.htm> ["Pledge"].

[150] *Ibid.*, art. 10.

[151] *Ibid.*, arts. 22-23.

[152] *League Against Racism and Antisemitism v. Yahoo! Inc.*, County Ct. of Paris, 20 November 2000, No. RG: 00/05308, online: Center for Democracy & Technology <http://www.cdt.org/speech/international/001120.yahoofrance.pdf>.

Amendment,[153] it had already announced that it would "no longer allow items that are associated with groups which promote or glorify hatred and violence, to be listed on any of Yahoo's commerce properties."[154] The privately imposed ban, while arguably narrower in terms of the content limited, was clearly broader in the scope of its application than the restriction ordered by the French court. Yahoo! banned the related content altogether, rather than limiting the ban to French citizens. Yahoo!'s public position was that its decision was motivated by pressure from human rights groups such as the Simon Wiesenthal Center and the Anti-Defamation League, rather than by the French court decision.[155] However, the timing of Yahoo!'s policy makes it difficult to imagine that French public regulation had *no* impact on its decision to impose a ban.

Subsequently, the ISP Qwest[156] agreed to terminate service to the "Zundelsite", a Web site including contents that the CHRT in *Citron* found violated subsection 13(1) of the *CHRA*. The CHRT noted that the practical impact of its cease and desist order would be limited, given that the respondent no longer resided in Canada and that "the technology involved in the posting of materials to the Internet ... arguably makes it much easier to avoid the ultimate goal of eliminating the material from telephonic communication."[157] While there was no attempt to enforce the cease and desist order against the related content provider or his ISP in the US, the CHRT's public denunciation of the Web site encouraged Qwest to terminate service to it. A Qwest official stated that it removed the site after receiving notice of the CHRT's decision. Qwest's AUP prohibits distribution of hateful, obscene, abusive, or excessively violent material.[158] As with the Yahoo! case, it would appear that the denunciatory impact of a public determination of illegality influenced the exercise of private discretion in accordance with public policy outside of the US.[159]

The Yahoo! and Qwest examples demonstrate that public regulation and decisions made pursuant to it can serve as effective guides for private enforcement mechanisms. Private decision-makers are relieved of the obligation to assess the legality of any particular content and are able to point to the law, rather than a private taste for censorship, as the basis of their decisions.[160] While the law may influence

---

[153] *Yahoo! v. Ligue*, *supra* note 71.

[154] Troy Wolverton & Jeff Pelline, "Yahoo to Charge Auction Fees, Ban Hate Materials" *CNET News.com* (2 January 2001), online: CNET <http://news.com.com/2100-1017-250452.html>.

[155] See Lisa Guernsey, "Yahoo to Try Harder to Rid Postings of Hateful Material" *The New York Times* (3 January 2001) C2, online: The New York Times <http://www.nytimes.com>.

[156] See online: Qwest <http://www.qwest.com>.

[157] *Citron*, *supra* note 10 at para. 298.

[158] See Adrian Humphreys, "U.S. Internet Giant Pulls Zundel's Web Site: Canadian Rights Panel Warned Firm of Hate Literature" *National Post* (13 May 2003) A9.

[159] This example demonstrates the practical limitations of ad hoc private responses following public decisions. The Zundelsite was back up and running using another host server by 12 May 2003 (*ibid.*).

[160] These examples illustrate Sunstein's argument that some market players who do not wish to discriminate rely on regulation to eliminate the choiee about whether to eater to demands for

and shape market behaviour and norms, the influence of demands by vocal non-governmental human rights groups on the exercise of private discretion in these situations should not be underestimated.[161] The ad hoc and purely voluntary nature of these kinds of private enforcement choices make them unreliable mechanisms for protecting important matters of public policy. Moreover, in the absence of public reporting, it is difficult to gauge either the breadth of these private practices or their consistency with public policy.

E. Private Regulation Is Not a Substitute for Public Regulation

Private regulatory mechanisms present an opportunity for restricting the dissemination of hate propaganda from the US., given the general absence of First Amendment scrutiny of private action. In addition, purely private regulation may be more flexible than state regulation and thus better able to react quickly to new phenomena, such as transmission through Internet applications other than the relatively accessible WWW.[162] However, practical factors associated with each of these mechanisms limit their efficacy in restricting the flow of Internet hate propaganda emanating from the US. More pressingly, there are broader policy concerns as to the wisdom of relying too heavily on the private market to regulate harmful discriminatory behaviour. The question then becomes whether the greater breadth and peer pressure that may be associated with group-based self-regulation through codes of conduct can be harnessed to encourage individual ISPs to privately regulate in accordance with the policy goals articulated in national public regulation and international human rights instruments.

1. Practical Limits

The current state of the art limits the ability of filtering and zoning technologies to effectively restrict Internet hate propaganda. The labelling of content necessary to

---

discriminatory content in the markctplace: Cass Sunstein, *Free Markets and Social Justice* (New York: Oxford University Press, 1997) at 154 [Sunstein, *Free Markets*].

[161] The Simon Wiesenthal Center, the ADL, and BiasHELP (an anti-discrimination group) appear to have had significant impact on the policies of individual ISPs and on-line content providers in connection with regulating racist expression on-line. See *e.g.* Troy Wolverton, "eBay Asked to Pull KKK Items from Site" *CNET News.com* (2 February 2000), online: CNET <http://news.com.com/2100-1017-236426.html>; Troy Wolverton, "eBay Heeds Call to Ban Hate Materials in Auctions" *CNET News.com* (3 Fcbruary 2000), online: CNET <http://news.com.com/2100-1017-236508.html>; "Japan Times Pulls Story on 'Nazi' Bar After Jewish Protest" *Japan Today* (13 March 2002), online: Japan Today <http://www.japantoday.com/gidx/news205708.html>.

[162] Sce Sabine Frank, "Co-operativc Forms of Regulating the Internct" (Report at the Council of Europe Forum on Harmful and Illegal Cyber Content: Self-Regulation, User Protection and Media Competence, Strasbourg, 28 November 2001), online: Council of Europe <http://www.coe/int/T/E/Human_Rights/media/4_Cyberfora/1_Self-regulation/1_European_Forum/2_reports_&_videos/reports.asp>; Bradford Smith, "The Third Industrial Revolution: Policymaking for the Internet" (2002) 3 Colum. Sci. & Tech. L. Rev. 1.

enable filtering, even if restricted to WWW content, presents a daunting task. First Amendment protection from the risk of prosecution and penalties means that US-based hate speakers are unlikely to be motivated to accurately label or to block access to their message, regardless of whether that message is illegal in the jurisdiction where it is accessed. The prospective efficacy of filtering and zoning is further limited by relatively effective technological circumvention measures. Finally, filtering and zoning at the ISP level raise concems with respect to monitoring and recording of a potentially highly private body of user data by ISPs.[163]

Private regulation through AUP's or ISP self-regulation, as currently structured in the US, is also limited by practical difficulties. AUPs, even those drafted by interventionist ISPs such as AOL, reserve maximum flexibility for ISP discretion and judgment. Further, while there are instances of individual ISP regulation of content in response to public determinations of illegality outside of the US, in the absence of a more organized and concerted effort to pressure for compliance, this presents an ad hoc avenue at best. Although US-based ISP organizations could act as focal points for asserting international pressure to self-regulate Internet hate propaganda, the absence of enforceable codes of conduct among US-based organizations and the current focus of hotline efforts on on-line child pornography limit the likelihood of restriction through this form of private regulation, at least in the short term.

Identification of these practical limitations, however, is not intended to suggest that private regulation through the implementation of technological measures, AUPs, or self-regulatory organizations should necessarily be rejected. Rather, it is intended to highlight that, despite the general absence of a First Amendment barrier, private regulation, like public regulation, offers at best a partial solution for restricting the extraterritorial flow of Internet hate propaganda emanating from the US. Of more fundamental concern is whether primary or substantial reliance on private market solutions in the context of hate propaganda would divest public authorities of their responsibility to safeguard Canadian public policy, with no degree of certainty that private market responses would serve national and international collective commitments to equality and diversity.

2. Policy Issues

Privatization or shifting responsibilities and power previously within the purview of the state to private actors is an expanding trend in Canada, the US, and indeed,

---

[163] It is not suggested that privacy related issues completely undermine the concept of ISP-based filtering or zoning by individual content providers. However, such issues do merit attention to ensure that uscrs are aware of and provide some form of meaningful consent to any filtering or zoning technologies privately implemented. Current privacy protection laws should be reviewed to determine their adequacy in addressimg issues raised by the implcmentation of these technologies. See Geist, *supra* note 90.

internationally.[164] As jurisdictions become increasingly interconnected economically and technologically, academic commentators have noted the push toward competitive advantage through the purported efficiencies of an unregulated private market, even in areas such as family and human rights law.[165] Many Internet stakeholders and theorists have urged governments in connected jurisdictions around the world to take a similar approach to the regulation of the Internet and its content, with some measure of success.[166] In fact, some ISPs and their self-regulatory organizations openly admit that moves toward self-regulation were designed to stave off public regulation and capitalize on what they see as the efficiency and flexibility of private enterprise.[167] Perhaps the most disturbing aspect of this trend is the shift in responsibility for collective goals away from the state to the invisible hand of the private market, often generating calls for those historically most disempowered by a free market system to take action to protect their own interests.

Arguments in favour of individually implemented filtering and zoning reflect this shift, admonishing individuals offended by particular content to take private measures to avoid it. However, as suggested above, this approach completely misses one of the fundamental commitments underlying Canadian restrictions and international provisions relating to hate propaganda: the broader risk to equality and multiculturalism associated with the adoption of discriminatory attitudes by those *not* offended by hateful messages.

Further, the private market has an unimpressive historic record in correcting discrimination based on personal characteristics such as race, gender, and sexual identity.[168] Unfortunately, this record is arguably consistent with rational behaviour by suppliers in seeking to meet consumer preferences. To the extent that there is demand for hateful content sufficiently widespread to sustain profitable economic activity, rational suppliers acting in their own economic self-interest will supply product to

---

[164] The presence of multinational corporations in physical jurisdictions around the globe, and their seeming immunity to both domestic and international law, has already been the subject of substantial commentary and concern. For an overview, see Trevor Farrow, "Globalization, International Human Rights Law and Civil Procedure" (2003) 41 Alta. L. Rev. [forthcoming].

[165] See Brenda Cossman & Judy Fudge, eds., *Privatization, Law, and the Challenge to Feminism* (Toronto: University of Toronto Press, 2002); Sarah Krieger, "The Dangers of Mediation in Domestic Violence Cases" (2002) 8 Cardozo Women's L.J. 235.

[166] See *e.g.* U.S., Department of Commerce, *Management of Internet Names and Addresses* (S. Doc. No. 980212036-8146-02), online: National Telecommunications and Information Administration <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm>; Canadian Radio-Television and Telecommunications Commission, Broadcasting Public Notice CRTC 1999-84, "New Media" (17 May 1999), online: CRTC <http://www.crtc.gc.ca/archive/eng/Notices/1999/PB99-84.htm>. In telling contrast, large media companies have not hesitated to insist on government intervention to protect copyright interests. See Lawrence Lessig, *The Future of Ideas* (New York: Random House, 2001).

[167] Frank, *supra* note 162.

[168] The historic failure of the private market with respect to racist propaganda, and the devastating results that flowed from this failure are chronicled in Alexander Tsesis, "Prohibiting Incitement on the Internet"(2002) 7 Va. J.L. & Tech. 5.

meet that demand.[169] There is no reason to expect that economic actors in the Internet market will behave any differently. To the extent that there exists a sufficiently widespread demand for discriminatory content among Internet consumers, or indeed, that the Internet can be used to stimulate demand, economically rational suppliers can be expected to meet it.

Additionally, in the context of the Internet, the economic rationality behind supplying discriminatory content combines with relatively widespread idealization of the Internet as a wide open, anarchic marketplace of ideas, to work against effective restriction of Internet hate propaganda solely through private regulation. ISPs considering private regulation of hate propaganda will have to weigh the potential reputational effects of continuing to carry hateful content versus being branded as censors interfering in the operation of the marketplace. Unfortunately, economic rationality may dictate that some ISPs will refuse to restrict content in relation to the least powerful members of society, reasoning that these groups are least able to bring economic pressure to bear.[170]

Assuming an economic incentive to supply hateful content, what then has prompted some ISPs to impose private restrictions on Internet hate propaganda? In the US, it is almost certainly not the threat of prosecution, imposition of legal penalties, or impending public regulation, given First Amendment protections. These responses may be attributable to concerns that demand for certain types of hate propaganda is not sufficiently widespread to merit the risk of reputational harm that may arise from being associated with its continued supply. However, in the absence of some mechanism for public scrutiny, decisions on whether to restrict this type of content are unlikely to be affected by reputational concerns. It is in this regard that continued public regulation and more widespread self-regulatory organizations with the ability to assert peer pressure can perhaps be of greatest efficacy by publicly exposing what are currently private decisions.[171]

---

[169] For a more complete articulation of the inability of the market to address discrimination based on personal characteristics, such as race, that are otherwise irrelevant to decisions such as hiring and promotion, see Sunstein, *Free Markets*, *supra* note 160 at 151-54.

[170] For example, in the aftermath of the 11 September 2001 attacks, persons of the Islamic faith have been increasingly targeted by on-line messages of hate. These messages may, however, carry very little weight in terms of the rational economic decision-making of ISPs, given what appears to be a relatively broad-based vitriol toward persons of Middle Eastern and Asian dissent in the US, and given the racial profiling and targeting of members of these groups resulting from legislative and law enforcement initiatives aimed at terrorism. See Salah D. Hassan, "Arabs, Race and the Post-September 11 National Security State" *Middle East Report* 224 (Fall 2002), online: Middle East Report <http://www.merip.org/mer/mer224/224_hassan.html>; but see Steve Lohr, "Internet Access Providers Curb Both Terrorist Postings and an Anti-Islamic Backlash" *The New York Times* (17 September 2001) C8, online: The New York Times <http://www.nytimes.com>.

[171] Likewise, public accountability will also be important to ensure that private actors do not restrict expression beyond what is democratically neeessary, for example, by restricting criticism of government action. See generally Lessig, *supra* note 1.

Part VII briefly comments on the question "where do we go from here?" first exploring the goals we might wish to achieve in relation to existing private regulation and then turning to the more practical issues of who might assist in achieving them and how they might be advanced.

VII. Organizing Private Action to Work Toward Public Goals

A. Goals for "Publicizing"[172] Private Action

The suggestions in subsection B below as to who might assist with organizing private action in service of national and international human rights objectives, and how they might go about doing that, are motivated by two goals. First, although public regulation of human rights issues such as hate propaganda is generally preferable, given First Amendment constraints on state enforcement of public regulation, we ought to explore ways to supplement public regulation by capitalizing on and expanding existing examples of private regulation. Second, in doing so, we ought to look for ways to make private regulation more systematic, transparent, and publicly accountable.

With these goals in mind, subsection B turns to the question of how the project of publicizing private action in a more systematic fashion might be advanced, having regard for the wisdom gained with respect to UN and Organization for Economic Cooperation and Development ("OECD") efforts to address multinational corporate compliance with, among other things, internationally proclaimed human rights.[173]

B. Advancing the Project

1. Who Might Be of Assistance?

There are at least four groups that might be individually or collectively involved in advancing the project of mobilizing private regulation in service of internationally

---

[172] For a discussion of how privatization might actually be used to extend, rather than retract, public norms and policy, see Jody Freeman, "Public Values in an Era of Privatization: Extending Public Law Norms Through Privatization" (2003) 116 Harv. L. Rev. 1285.

[173] Although there are a myriad of international initiatives to encourage private corporate compliance with international standards, norms, and law, this paper relies upon and refers primarily to two: The Global Compact and the OECD Guidelines for Multinational Enterprises. See United Nations, "Overview: What is the Global Compact?", online: UN <http://www.unglobal compact.org/Portal/> and OECD, Directorate for Financial, Fiscal and Enterprise Affairs, Committee on International Investment and Multinational Enterprises, *The OECD Guidelines for Multinational Enterprises: Text, Commentary and Clarifications*, Doc. No. DAFFE/IME/WPG(2000)15/Final 2001), online: OECD <http://www.olis.oecd.org/olis/2000doc.nsf/c5ce8ffa41835d64c125685d005300b0/d1bad a1e70ca5d90c1256af6005ddad5/$FILE/JT00115758.pdf> [*OECD Guidelines*].

defined human rights[174] reflected in the Canadian Provisions: collective international organizations such as the UN and the OECD, national governments, ISPAs, and independent human rights NGOs.

International collectives such as the UN and the OECD are ideally suited to assert a considerable degree of clout that is likely to be of assistance in encouraging private actors to comply with international norms and standards. While both organizations are concerned with addressing human rights on a global scale, the UN may be better situated to address hate propaganda,[175] given its related committees' and rapporteurs' oversight powers in relation to compliance with the *CERD*, the *ICCPR*, and the *Universal Declaration of Human Rights*.[176] While the UN is thus arguably well placed to address this human rights issue, the OECD's developed expertise on issues of Internet regulation should be capitalized upon.[177]

Involving national governments to encourage US ISPs to comply with internationally established human rights that animate legislation like the Canadian Provisions offers the important element of additional clout to the protection of these rights and the potential for legal mechanisms of enforcement. Government involvement would forestall criticisms like those leveled at the Global Compact. NGOs, comparing the Global Compact to the OECD Guidelines, have rightly noted that national government involvement in monitoring and reporting on compliance

---

[174] Notably, however, any international approach premised on the *CERD* and the *ICCPR* will focus on racist propaganda only, whereas the Canadian *CHRA* provisions address a broader range of discriminatory grounds.

[175] For example, the UN Commission on Human Rights ("UNCHR") recognized at its 2001 World Conference the role of emerging technology both in alleviating and perpetuating racism, racial discrimination, and xenophobia. While it urged states and the private sector to develop self-regulatory measures to combat racism, the UNCHR did not assume an active role in implementing or monitoring such measures. See UNCHR, "Report of the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance" (Durban: 2001), A/CONF.189/12, online: UN <http://www.un.org/WCAR/aconf189_12.pdf>.

[176] G.A. Res. 217(III) UN GAOR, 3d Sess., Supp. No. 13, UN Doc. A/810 (1948) 71 provides both for protection of equality (art. 2) and freedom of expression (art. 19), subject to such "limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of mecting the just requirements of morality, public order and the general welfare in a democratic society" (art. 29).

[177] The OECD has already been involved in facilitating discussion of ISP self-regulation. See *e.g.* OECD, *BIAC/OECD Forum: Internet Content Self-regulation* (Paris: OECD, 1998), online: OECD <http://www.oecd.org/document/36/0,2340,en_2649_34255_1814628_119808_1_1_1,00.html>, proffering guidelines relating to consumer protection in e-commerce. For a 2003 report on these guidelines, see OECD, Directorate for Science, Technology and Industry Committee on Consumer Policy, *Consumers in the Online Marketplace: The OECD Guidelines Three Years Later*, Doc. No. DSTI/CP(2002)4/FINAL (2003), online: OECD <http://www.olis.oecd.org/olis/2002doc.nsf/43bb6130e5e86e5fc12569fa005d004c/af6ec39d8631ca3ac1256cc2005c0edf/$FILE/JT00138646.pdf>.
Subsequently, thc OECD proposed specific Internet content guidelines relating to "spamming". See OECD, *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* (2003), online: <http://www.oecd.org/dataoecd/24/19/2956420.pdf>.

moves the OECD Guidelines a step closer to *binding* private enterprise than does the Global Compact.[178]

In the Internet hate propaganda context, it may well be possible to involve national governments in monitoring and reporting, as well as enforcement, as reflected in co-operative efforts such as the Additional Protocol. However, given the current First Amendment approach, US government involvement is unlikely, thereby eliminating the participation of a key player. Nevertheless, like-minded countries including Canada ought to involve themselves in these kind of efforts. In this regard, the OECD Guidelines present a useful model, requiring adhering states to identify national contact points obligated to, among other things, monitor and report on compliance by private enterprise within their jurisdiction and to attend annual meetings overseen and facilitated by an OECD committee.[179]

Unlike the situation in the US, a number of ISPAs in other jurisdictions have implemented codes of conduct that require their members to address illegal and offensive content. Some also require co-operation with privately organized hotlines and hotline coalitions that receive and act on reports relating to offensive and illegal content.[180] These organizations, and the affiliations among them, present the opportunity for more broadly based and consistent private regulation. Like individual ISP regulatory decisions, however, the implementation of their codes is frequently not

---

[178] See *e.g.* National Policy Association, "The UN Global Compact and the OECD Guidelines", online: Public Policies to Promote Corporate Social Responsibility <http://www.multinationalguidelines.org/csr/ungc_vs_oecd.htm>.

[179] *OECD Guidelines*, *supra* note 173 at 46-50.

[180] The Canadian Association of Internet Providers, for example, sets out a fair practices policy statement that provides that its members will not knowingly host illegal content or conduct and will take action when notified of either: Canadian Association Internet Providers, *Fair Practices Document* (31 August 2000) at 11, online: <http://www.caip.ca/issueset.htm>. The United Kingdom Internet Service Providers Association ("UKISPA") requires members to take steps to ensure services and promotional material (although not third party content) do not contain material inciting violence, sadism, cruelty, or racial hatred and to comply with notification of illegal content issued by the Internet Watch Foundation ("IWF"). The UKISPA reserves the right to impose a variety of penalties on members who fail to abide by its code, including membership suspension and termination, as well as publication of the member's identity and the ISPA's findings with respect to any complaint relating to that member: UKISPA, "Code of Practice" (as amended 19 April 2002), art. 8, online: UKISPA <http://www.ispa.org/uk>. The Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (Association for the Voluntary Self-Monitoring of Multimedia Service Providers) ("FSM") in Germany goes further, requiring members to self-monitor for a variety of categories of impermissible and illegal content, including content inciting hatred and violence against minority groups and instigation of racial hatred. Members agree not to provide this content directly or to provide a switch for its use. The code includes a complaints and hearing mechanism, which can result in the publication of reprimands. In addition, the code provides a mechanism for reviewing and issuing public reprimands in relation to *non-member* ISPs that provide impermissible content or switches for its use in order to encourage non-members to remove or disable access to that content: Freiwillige Selbskontrolle Multimedia-Diensteanbeiter, "Code of Conduct" (9 July 1997), online: FSM <http://www.fsm.de/sprachen/en/verh.pdf>.

subject to public review and, in any event, appears to be uneven at best.[181] Nevertheless, the breadth of these organizations and their potential to harness peer pressure among members ought to be taken into account when fashioning an approach to more effectively restrict Internet hate propaganda.

NGOs play an ongoing and important role in monitoring and reporting on failures by government and private industry to observe basic human rights.[182] However, as one group pointed out in relation to multinational corporate compliance with international human rights obligations:

> Contrary to the assertion of some, it is not enough to suggest that nongovernmental organizations (NGOs) will assume this monitoring and enforcement function. Human Rights Watch has devoted substantial resources to promoting corporate respect for human rights, but our efforts are just a drop in the bucket. Neither we nor other NGOs begin to have sufficient resources to assume an enforcement role that should be the province of governments and the UN.[183]

Given the experience of the UN and its related committees and rapportours in addressing human rights issues, Canada ought to encourage it to become more directly involved with regulating Internet hate propaganda. While the Global Compact may have some impact on encouraging private actors in the Internet industry to comply with international human rights initiatives, by June 2003, few, if any, had actually "signed on" to participate.[184] As such, a more directed effort toward Internet hate propaganda may be merited, one targeting inclusion of interested national governments,[185] ISPAs, and existing human rights-based NGOs.

---

[181] Canadian Secretariat, World Conference Against Racism Advisory Committee, *Combatting Hate on the Internet* (Issue Position Paper, Hate and New Media Working Group) (31 January 2001), online: Canadian Heritage <http://www.pch.gc.ca/progs/multi/wcar/advisory/hate-on-net_e.shtml>.

[182] See *e.g.* online: Human Rights Watch <http://www.hrw.org>; Simon Wiesenthal Center, *supra* note 161; online: ADL <http://www.adl.org/main_internet.asp>; Southern Poverty Law Group, *Intelligence Project*, online: SPLG <http://www.splcenter.org/intel/intpro.jsp>.

[183] Kenneth Roth, "Corporate Social Responsibility," Letter to UN Secretary General Kofi Annan, (28 July 2000), online: HRW <http://www.hrw.org/advocacy/corporations/>.

[184] The UN reported that by June 2003, 1,018 companies from 56 countries had notified the Compact office of their intention to participate in the Compact, although it could not advise as to the status of these companies' compliance with the Compact's stated principles. Of the companies listed as participants, only 45 were from the US, 7 from Canada, and 22 from the UK, compared to 176 from Poland, 86 from India, and 147 from France. From a review of their names, very few appeared to be ISPs. See United Nations, "Global Compact Participants by Country" (10 June 2003), online: UN <http://www.unglobalcompact.org/content/Companies/list_pc_100603.pdf>.

[185] Other UN members, such as France, may be highly motivated to participate, even though participation by the US (and possibly other member states) is unlikely.

2. What Steps Should Be Taken?

As suggested by the Canadian Secretariat to the World Conference Against Racism Advisory Committee, the UN could establish an independent coordinating agency to: (i) develop a code of conduct for the Internet; (ii) monitor and report annually on Internet hate propaganda; and (iii) develop educational programs to help governments at all levels to recognize the impact of Internet hate propaganda and the need for its regulation.[186] The development of a code would need to be done in consultation with key players, including those listed above.

The monitoring and reporting function and the involvement of ISPs and ISPAs in the process from the outset would ideally generate an incentive for ISPs and ISPAs, particularly in the US, to adopt the model. The model should also provide for a central agency to which individual ISPs or ISPAs report activities relating to the restriction of offensive or illegal content to foster public accountability and a degree of transparency. It might also include a notice and takedown system, with notice being provided to ISPs by the coordinating agency itself or through a designated hotline responsible for reviewing content in accordance with the strictures of the *ICCPR* and *CERD*, thereby unburdening ISPs of the task of independently assessing the legality of particular content.

C. Shortcomings

The skeletal framework suggested here is at once an ideal and a compromise. It is idealistic in the sense that it would require mobilization of international resources at a time when US resistance to international solutions on the issue has been made perfectly clear and international tension on issues of human rights and terrorism is high. Further, it would require expenditure of resources not just by national and international public agencies, but also by private ISPs and ISPAs, potentially undermining their willingness to participate.

It is a compromise in the sense that it accepts private regulation and seeks to build into it a degree of accountability, rather than a direct mechanism for legal enforcement. Undoubtedly, its non-binding nature and dependence upon what is effectively moral suasion to encourage private participation and compliance is less than ideal. As a result, it is likely to attract the participation only of larger private actors who are concerned about the reputational effects of the monitoring and reporting suggested, leaving behind a not insignificant group that is impervious to these effects due to commitments to a vision of an anarchic Internet marketplace or their non-commercial objectives. Nevertheless, this approach seeks to build on

[186] Canadian Secretariat, *supra* note 181.

experience gained in ongoing international efforts to address transnational problems and offers the potential for publicizing ongoing private regulation.[187]

Even if the international mobilization necessary to develop, monitor, and report on a model code of conduct never comes to fruition, Canada should continue its efforts to comply with its international obligations by vigorously enforcing the Canadian Provisions. Public decisions pursuant to that legislation continue to provide valuable guidance triggering private enforcement against the growing body of Internet hate propaganda emanating from the US. Further, Canada should sign the Additional Protocol, joining forces with other nations around the world seeking to address dissemination of these destructive messages.

Conclusion

The export of a First Amendment in code more powerful than that in law may well,[188] as Thierer predicts, allow the US to "[offer] the protection of the First Amendment over the Net to millions of people who have been denied the right to speak freely in their own countries."[189] However, in Canada, First Amendment imperialism, particularly on the issue of hate propaganda, holds no freedom-enhancing promise. Rather, the export of the current US approach to hate propaganda threatens essential public policy reflected in Canada's democratically enacted and constitutionally sanctioned restrictions on this "de-liberating" exercise of private power. The thinner conception of liberty as freedom from government restriction underlying the US approach fails to take sufficient account of the de-liberating impact of hate propaganda on target group members and broader public concerns for equality and multiculturalism, which are entrenched Canadian constitutional commitments.

Ongoing regulation by private Internet actors, in particular ISPs, could limit the impact of the current First Amendment approach on Canada's public policy objectives. However, private regulation alone is not enough. Achieving the goals of equality and multiculturalism, and the mutual respect for diversity essential to them, should not be primarily entrusted to largely unscrutinized choices made by individuals in private settings or be foist on target group members by expecting them to adopt technological means of avoidance. Nevertheless, the comparative advantage

---

[187] Voluntary approaches, initiated in the context of existing public national and international regulation, have enjoyed some history of success, if on no other basis than raising awareness and encouraging reporting. See *e.g.* International Labour Organization, "MNE Declaration" (9 April 2003), online: ILO <http://www.ilo.org/public/english/employment/multi/history.htm>, reporting on the International Labour Organization's "Tripartite Declaration of Principles Concerning Multinational Enterprises and Social Policy" (1977), online: ILO <http://www.ilo.org/public/english/standards/norm/sources/mne.htm>. With respect to the apparel and footwear industry, see Jennifer L. Johnson, "Public-Private-Public Convergence: How the Private Actor Can Shape Public International Labor Standards" (1998) 24 Brook. J. Int'l L. 291.

[188] Lessig, *supra* note 1.

[189] Thierer, *supra* note 2.

of private regulation with respect to the First Amendment roadblock makes it worth considering as a regulatory supplement.

Existing private regulatory practices and structures might be enlisted in service of public goals, an approach modeled in numerous international responses to multinational corporations. Key to this effort will be identifying a sufficiently powerful international oversight body capable of garnering the respect necessary to encourage private Internet actors to participate and report. If nothing else, monitoring and reporting requirements would facilitate a more comprehensive empirical understanding of existing private regulatory efforts, offering the possibility of increased public accountability and transparency. In this regard, with or without an international initiative, a Canadian agency such as the CHRC might undertake its own empirical analysis of ongoing private initiatives.

In the interim, the importance of ongoing enforcement of public regulation should not be underestimated. Violations of the Canadian Provisions should be vigilantly prosecuted. Resulting judgments should publicly denounce hate propaganda's inconsistency with Canada's defining constitutional commitments to equality and multiculturalism and guide private decision-making regarding restriction of content currently granted safe haven by the First Amendment.