COMBATING EXTREMISM IN CYBERSPACE:

THE LEGAL ISSUES AFFECTING INTERNET HATE SPEECH

TABLE OF CONTENTS

I. INTRODUCTION: LAW AND THE INTERNET

Across the United States and throughout the world, the Internet is revolutionizing the way people do business and live their lives. With the development of this new, exciting medium, however, come novel political and legal questions:

What actions constitute crimes on the Internet?

Who has jurisdiction over crimes committed on the Internet?

Who has the right to a domain name?

When must a company plying its goods in cyberspace charge sales tax?

What state or country's laws govern activity on the Internet?

Lawyers must grapple with these difficult questions every day. Law schools are establishing courses to teach about law and the Internet. Cases are being litigated. Indeed, rarely, if ever, has the legal community been as challenged by a new development as it is currently with the advent of the Internet. The impact of this new technology is felt throughout the law: criminal, intellectual property, commercial and constitutional law principles have been tested so far.

While some scholars assert that there is no "law of the Internet" — and that traditional laws simply must be adapted and applied to regulate behavior on the Internet — others believe that new laws must be crafted specifically to fit this new medium. Regardless, it is clear that the Internet presents novel, exciting and difficult legal questions.

One area of particular concern to the Anti-Defamation League is how to effectively and legally combat hate on the Internet. The Internet has become the new frontier in hate, ensnaring both inexperienced and frequent visitors to the World Wide Web. When most people venture onto the Internet, especially newcomers to cyberspace, the last thing they expect to encounter is a swastika or a burning cross. Those seem like relics of the past, and the Internet represents the future.

So it is jarring, and profoundly upsetting, to go online and see such graphic examples of how hate survives from generation to generation, and how it has somehow managed to migrate from leaflets in parking lots to Web sites and chat rooms. Whereas extremists once had to stand on street corners spewing their hate and venom — reaching only a few passersby — now they can rant from the safety of their own homes; anyone can easily create a Web site, propelling their message, good or bad, to the entire world.

The Internet generation, unfortunately, is seriously at risk of infection by this virus of hate. Not only is this virus present on the Internet today; it is being spread around the globe, in the wink of an eye — or, more accurately, with the click of a mouse. This exciting new medium allows extremists easier access than they have ever had before to a potential audience of millions, a high percentage of whom are young and gullible. It also allows haters to find and communicate cheaply and easily with like-minded bigots across borders and oceans, to promote and recruit for their cause while preserving their anonymity, and even to share instructions for those seeking to act out their intolerance in violent ways.

The spread of this virus poses one more important question. What is the most effective way to respond to this dark side of the Internet?

Clearly there are educational responses. Extremist propaganda can be illuminated, dissected and analyzed, and several organizations, including the Anti-Defamation League, have been doing that in numerous reports and publications.

There are also filtering tools available on the market. These software programs, including the ADL HateFilter® discussed in more detail later in this report, do not deny extremists access to the Internet. Rather, they make it possible for parents to keep offensive material off their children's computers. While extremists have the constitutional right to stand on the street corner or in the middle of a public park professing anti-Semitic, racist or other hateful beliefs as well as to create Web pages advancing these same deplorable ideas, individuals need not invite such hurtful hate into their homes. ADL's filter erects a firewall which hate cannot breach.

Educational materials and filtering devices do not address the more controversial question of whether hate on the Internet can or should be regulated by the government. The balance of this report will attempt to address this complicated, multidimensional legal question. In so doing, the report will focus first on governmental regulation of online hate in the United States, taking into account the different features of the Internet such as electronic mail, chat rooms and the World Wide Web. It will also compare use by adults to use by children, and will examine the relative responsibilities of government, the computer industry, universities and private organizations. Finally, the report will note relevant differences in American constitutional law, foreign law and international law, and, taking note of the evolving nature of this area of the law, will peer into the proverbial looking glass and offer some thoughts regarding its future direction.

II. Governmental Regulation of Online Hate in the United States

A. The First Amendment

The First Amendment of the U.S. Constitution protects the right of all Americans to express their opinions, even when they make unpopular or offensive statements. Federal, state and local governments may intrude upon this right only in very limited situations. In the "marketplace of ideas" model adopted long ago by the U.S. Supreme Court, good and bad ideas compete, with truth prevailing. Thus, Americans are willing to tolerate harmful speech because they believe that it ultimately will be tested and rejected. To date, courts have shown little inclination to treat speech on the Internet differently from the print media, the broadcast media, or even the traditional soapbox in a public park.

In fact, the Supreme Court has made clear that traditional First Amendment considerations govern speech on the Internet. Looking forward, it appears likely, then, that courts will continue to scrutinize hate speech on the Internet under the traditional constitutional framework used to analyze the permissibility of government regulation of speech in other media. *Reno v. ACLU*, 521 U.S. 844 (1997).

The First Amendment's Free Speech Clause rigorously protects most expression. Constitutionally protected speech may only be restricted if the government can demonstrate a compelling state interest in doing so. Further, the government must show a close nexus between its goals and its actions. Under this "strict scrutiny" standard, courts examine the law closely to see if its objective is compelling and its approach "narrowly tailored" to meet that objective.[1]

While the government's right to promulgate content-based restrictions is quite limited, it can legally apply *content-neutral* speech regulations more freely. These regulations, which generally pertain to the time, place, or manner of speech, apply equally to all speech, regardless of the message conveyed. For instance, the government can limit the amount of noise allowed at a public event, regardless of whether it is a white supremacist rally or a Veterans' Day parade, so long as the regulations are applied consistently and are not overly restrictive. Or, the government may limit leafleting as long the applicable laws ban all flyers, regardless of their content.

Time, place, and manner regulations do not translate well into the world of the Internet. Traditional concepts of time and place have little meaning in cyberspace, where there are virtually an infinite number of equally accessible "places" to post hate propaganda regardless of the time of day. Nor are conventional conceptions concerning the manner of speech, such as its audible volume, applicable in cyberspace.

B. Examples of Unprotected Speech

Before the Internet was ever conceived, the U.S. Supreme Court, for decades, had been interpreting the First Amendment and crafting a free-speech doctrine. In a series of cases, the Court firmly established many important principles. For instance while hate speech is odious, the Court has made clear that First Amendment protections usually extend to such speech. Unless the speech contains a direct, credible "true" threat against an identifiable individual, organization or institution; it meets the legal test for harassment; or it constitutes incitement to imminent lawless action likely to occur, little recourse will be

available under American law. The constitutional theory of unprotected speech has withstood the development of new technology before, and it translates rather well to today's new media, such as the Internet.

Threats

Generally defined as declarations of "intention to inflict punishment, loss, or pain on another, or to injure another by the commission of some unlawful act,"[2] true threats receive no First Amendment protection. *US v. Watts*, 394 U.S. 707 (1969), *R.A.V. v. St. Paul*, 505 U.S. 377 (1992). This principle applies to threats involving racial epithets or those motivated by racial animus.[3] A threatening private message sent over the Internet to a victim, or even a public message displayed on a Web site, of an intention to commit acts of racially motivated violence, could be lawfully punished.[4]

In order to be legally actionable, threats must be "true." Under an objective test employed by some courts, a reasonable person must foresee that the statement would be interpreted by the recipient as a serious expression of intent to harm or assault. Recent decisions such as *Planned Parenthood of the Columbia/Willamette v. American Coalition of Life Activists*, *United States v. Machado*, and *United States v. Kingman Quon*, have held online threatening speech punishable. These cases are discussed in more detail below.

Harassing Speech

While courts have yet to fully consider the constitutionality of harassing speech, they still have managed to set forth a few guidelines that are generally accepted. Targeting an individual with harassing speech is not a constitutionally protected activity under U.S. law because the speech in question usually amounts to impermissible conduct, not just speech. In order for speech to be considered harassing, it must be persistent and pernicious and must inflict significant emotional or physical harm. Furthermore, harassment, like threats, must be directed at specific individuals. Blanket statements expressing hatred of an ethnic, racial or religious group in general cannot be considered harassment, even if those statements distress individual members of that ethnic group. However, if a person continually directs racist statements at a single victim, such speech may rise to the level of harassment even if the racist remarks do not specifically mention the victim.

It may be possible to prosecute racially motivated harassing speech transmitted over the Internet as a violation of state or Federal laws prohibiting harassment. In *Commonwealth of Pennsylvania v. ALPHA HQ*, which is discussed below, the Pennsylvania Attorney General, for example, charged a Web user with terroristic threats, harassment, harassment by communication, and ethnic intimidation arising from material on a racist Web site.

Incitement to Imminent Violence

Incitement to imminent violence or other unlawful action is also not protected by the First Amendment. The Supreme Court established the imminent incitement principle in *Brandenburg v. Ohio*,[5] distinguishing between speech that is "directed to inciting or producing imminent lawless action and is likely to incite or produce that action" and speech which is not likely immediately to incite such action.

In flyers or on the Web, individuals can propose violent reactions to contemporary problems or threaten menacing actions, but unless such a call is actually likely to result in violence and the violence is likely to occur imminently, the speech will be protected.

The *Brandenburg* standard is a high bar to meet and online hate speech will rarely be punishable under this test. Even an E-mail (or Web site) that specifically calls for lawless activity would probably not be actionable under *Brandenburg* because it would be difficult to prove the imminence required. Since the speaker and listener are separated and often do not even know each other, it is doubtful that a call to arms on the Internet would result in immediate violence. Commentators often state their belief that it is unlikely that someone who reads hate on the Internet will immediately rush out of his home to commit a violent act.

Libelous Speech

Online "group libel" — libelous hateful comments directed toward Jews, Blacks or any other religious or racial group in general — is not actionable. Since first enunciated, the theory of group libel has died a quiet — but certain — death. The courts have repeatedly held that libel directed against religious or racial groups does not create an actionable offense.

Libel directed toward a particular person, persons, or entity may be legally actionable if certain criteria are met. The Supreme Court has distinguished between two categories of persons — public officials and private persons. According to *New York Times v. Sullivan*, 376 U.S. 254 (1964), public officials may not bring suit against critics of their official conduct, unless the official can prove "actual malice." This refers to someone who utters a false statement "with knowledge that it was false or with reckless disregard of whether it was false or not." A much lower standard exists for proving libel against a private person. Pursuing a libel case would be no different if the offending message were spread online than if it had been made orally.

C. Hate Speech as Evidence in Hate Crime Prosecutions

Most hate crimes statutes, including model legislation first drafted by ADL almost two decades ago, provide that when a victim is targeted because of race, religion, ethnicity, sexual orientation or other immutable characteristics, the perpetrator may face an enhanced penalty. A racial assault, anti-Semitic vandalism, or gay-bashing, or any similar crime is treated more seriously than other forms of assault or vandalism because of the broader impact such crimes have on our society.

While hate speech is not punishable, it may provide important evidence of motive in a hate crime case. A good example is the landmark *Wisconsin v. Mitchell* case in which the Supreme Court upheld the penalty enhancement approach to hate crimes laws by a 9-0 vote. The defendant incited a group of young Black men who had just finished watching the movie "Mississippi Burning" to assault a young white man by asking "do you feel all hyped up to move on some white people?" This statement was appropriately used by prosecutors to demonstrate that the white victim was assaulted because of his race. Hateful views expressed via the Internet may be used in a similar manner.

Federal Laws Prohibiting Racially Motivated Crimes

While recent efforts to pass comprehensive Federal hate crimes legislation have been rebuffed, there still is some limited protection at the Federal level against hate crimes. Federal civil rights law, 18 U.S.C. § 245, prohibits intentional interference, by force or threat of force, with the enjoyment of a Federal right or benefit (such as voting, going to school or employment) on the basis of race, color, religion or national origin. Thus, if a white supremacist interferes with an African-American's right to vote or to attend a public school because of his skin color, the perpetrator may be prosecuted under Federal law. This statute was the basis for two noteworthy online hate speech cases discussed below: *United States v. Machado* and *United States v. Kingman Quon*.

This statute is deficient, however, because it only protects certain Americans and because it only applies in limited circumstances. Another bill giving additional authority to Federal officials to investigate and prosecute cases in which the bias violence occurs because of the victim's real or perceived sexual orientation, gender or disability is currently pending in Congress. The bill, the Hate Crimes Prevention Act, would also enable Federal prosecutors to move forward in hate crimes cases without requiring them to prove that the victim was attacked *because* he or she was engaged in a Federally protected activity.

Another Federal law, the Hate Crimes Sentencing Enhancement Act, was enacted in 1994. This law provides a sentencing enhancement for bias-motivated attacks and vandalism that occur in national parks and on other Federally owned property.

D. Court Decisions Concerning Hate Speech on the Internet

Although the intersection of law and the Internet promises to be one of the more fascinating legal developments in the early part of the 21st century, to date relatively few court cases have addressed hate speech on the Internet. This is due in part to the general difficulty of prosecuting hate speech because it usually receives constitutional protection. The dearth of litigation may also be linked to the difficulty of policing the Internet's vast expanse and tracing the perpetrators of online hate crimes. Web sites can be created, relocated, renamed, or abandoned overnight. Despite these obstacles to punishing online hate speech, a few recent prosecutions have been successful.

United States v. Machado

Twenty-one-year-old Richard Machado sent a threatening E-mail message signed "Asian Hater" in September 1996 to 60 Asian students at the University of California, Irvine, (UCI). Machado's message was titled "FUck [sic] You Asian Shit" and stated that he hated Asians and that if Asians were not at UCI, the school would be much more popular. He later blamed Asians for all crimes that occurred on campus and said that if the recipients and other Asians on campus did not leave, he would hunt all of them down and kill them. Machado wrote, "I personally will make it my life carreer [sic] to find and kill everyone one [sic] of you personally. OK?????? That's how determined I am…Get the fuck out, MOther FUcker (Asian Hater)."[6]

Machado did not sign his real name to the message and sent it from an account that did not readily indicate his identity. However, in two separate voluntary interviews with UCI police, he admitted sending the threatening messages. On August 19, 1997, the U.S. Attorney for the Central District of California charged Machado with violating Title 18 U.S.C. § 245, which prohibits interference with a Federally protected activity (attending a public college) because of the race, color, religion or national origin of the victim.

After a first trial ended in a hung jury, Machado was convicted of violating the Asian students' civil rights in February 1998. Additional evidence not admitted at the first trial may have swayed the jurors in the second trial. Evidence at the second trial indicated that Machado had been investigated for sending a threatening message to staff at the campus newspaper a year before he sent the "Asian Hater" message. Machado was sentenced to one year in prison.

Machado's actions could have been considered criminal even if the threatening messages he sent had not contained racial hatred or been aimed at students engaging in a "Federally protected" activity. Machado could have been prosecuted under a California State law criminalizing terroristic threats. Instead, however, he was prosecuted under Federal law because the messages he sent were motivated by racial bias and aimed at people engaged in a "Federally protected" activity.

United States v. Kingman Quon

Another college student, Kingman Quon, pleaded guilty to Federal civil rights charges in February 1999 after sending hateful E-mail messages to Hispanic professors, students and employees across the country. He received a two-year sentence for the crime.

Quon had sent E-mail messages to 42 faculty members at California State University at Los Angeles, to 25 students at the Massachusetts Institute of Technology and to numerous other people employed at various institutions and businesses nationwide. The racially derogatory messages, which stated that Quon would "come down and kill" them, discussed his hatred of Latinos and accused them of being too "stupid" to get a job, or accepted as students, without the help of affirmative action policies.

Commonwealth of Pennsylvania v. ALPHA HQ

In February 1999, a Pennsylvania court entered an injunction against Web site owner and controller Ryan Wilson, his white supremacist group ALPHA, and Stormfront, Inc. (which had been providing the ALPHA Web site with domain name service), barring them from displaying certain messages on the Internet.

The order stemmed from charges filed against Ryan Wilson for terroristic threats, harassment and ethnic intimidation. One of the pictures on Wilson's ALPHA Web site depicted a bomb blowing up the office of Bonnie Jouhari, a fair housing specialist who regularly organized anti-hate activities and focused on issues concerning hate crimes, racial hatred and the activities of local hate groups. Next to her picture, the ALPHA web site stated "Traitors like this should beware, for in our day, they will be hung from the neck from the nearest tree or lamp post." Wilson did not contest the state's action, and the site was removed from the Internet.

In early 2000, the Federal Office of Housing and Urban Development filed a civil discrimination suit against Wilson. The U.S. Department of Justice reportedly is also investigating Jouhari's case for possible criminal violations.

Planned Parenthood of the Columbia/Willamette, Inc. v. American Coalition of Life Activists, 23 F. Supp.2d 1182 (D. Or 1999)

In March 1999, a Federal jury determined that a coalition of anti-abortion groups were liable for making threats against abortion service providers. The jury rejected the defendants' free speech claims and ordered them to pay more than $100 million in damages. While this case did not address threatening speech motivated by racial, ethnic or religious bias, it articulated a legal theory that courts could use in addressing extremist speech and which could apply in cases involving threatening hate speech on the Internet.

"The Nuremberg Files" first appeared on the Internet in January 1997. It listed the names of 200 doctors who allegedly performed abortions. The site provided specific information about the doctors, including their photos, home addresses, license plate numbers, and the names of their spouses and children. Headlined "Visualize Abortionists on Trial" and depicting blood dripping from aborted fetus parts, the site called for these persons to be brought to justice for crimes against humanity as the Nazis were after WWII. The names of those doctors who had been wounded were listed in gray. Doctors who had been killed by anti-abortionists had been crossed out.

The plaintiffs, several doctors and abortion clinics, alleged that they had been the specific target of "true" threats to kill, assault or do bodily harm. The jury agreed, finding that the documents, viewed in the surrounding contextual history of violence against abortion service providers, threatened the plaintiffs.

The judge subsequently issued an injunction against the anti-abortion defendants. Relying on two Ninth Circuit U.S. Court of Appeals cases, *United States v. Orozco-Santillan*, 903 F.2d 1262 (9th Cir. 1990), and *Lovell v. Poway Unified School District*, 90 F.3d 367 (9th Cir. 1996), he determined that the speech was truly threatening. Under *Lovell* and *Orozco-Santillan*, the test is whether "a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates the statement, as a serious expression of intent to harm or assault." Following this analysis, the court considered the alleged threats in light of the surrounding context of violence against abortion providers. Ruling that the plaintiffs were threatened by the materials and no adequate remedy at law existed, the judge issued a permanent injunction to prevent the defendants from providing additional information to the Web site.

E. The Communications Decency Act and Internet Service Providers

During the early years of widespread Internet use, Internet Service Providers (ISPs) began to fear that they could be held legally responsible for damages caused by the Web pages and other user content they host. In order to maintain the free flow of information and ideas on the Internet — and the uninhibited atmosphere of free speech that thrives in cyberspace — Congress included provisions in the 1996 Communication Decency Act CDA) insulating ISPs from liability for customer-created content.

A significant portion of the CDA was struck down by the Supreme Court in *Reno v. ACLU*, 521 U.S. 844 (1997). However, Section 230, which protects ISPs from liability, remains intact. This section states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[7]

Three cases involving the Internet service America Online (AOL) have upheld the protections embodied in the law: *Blumenthal v. Drudge, Zeran v. America Online*, and *Doe v. America Online*. AOL not only provides its users with access to the Web, E-mail and newsgroups, it also allows them to use its own proprietary network, which contains private bulletin boards and additional content unavailable to other Internet users. Though these three cases all involve proprietary content on AOL (as opposed to content on the Internet), they appear to be applicable to the activities of other ISPs, such as hosting users' Web sites.

In *Doe v. America Online*, a Florida court ruled that the mother of a minor could not sue AOL, even though a pedophile, Richard Lee Russell, used AOL bulletin boards to find people interested in purchasing a videotape of him performing sexual acts with her 11-year-old son. The judge held that the mother's claims against AOL were barred by Section 230. Holding AOL liable for Russell's messages would "treat AOL as the 'publisher or speaker' of those communications," subjecting AOL to the same legal treatment Doe sought for Russell, the "actual 'publisher or speaker' of the statements at issue,"[8] the judge stated.

Blumenthal v. Drudge involved an article by cyber-columnist Matt Drudge that circulated rumors of domestic violence between an aide of President Clinton, Sydney Blumenthal, and Blumenthal's wife. Drudge retracted the story and apologized the next day, but the Blumenthals filed a libel suit naming Drudge and AOL. The article was posted in Drudge's area within AOL's proprietary network, and Drudge was under contract with AOL. The U.S. District Court judge dismissed AOL from the suit, ruling that Section 230 protects AOL despite some editorial control exercised over Drudge.[9]

In *Zeran v. America Online*, Kenneth Zeran sued AOL because of messages posted anonymously to an AOL message board, listing Zeran's phone number and advising AOL users incorrectly that Zeran was selling T-shirts featuring offensive slogans related to the Oklahoma City bombing. As a result of these misleading postings, Zeran received angry calls and death threats. Zeran sued AOL for taking too long to remove the messages; for refusing to post retractions of the messages; and for failing to screen for similar messages that were posted after the initial one.[10] Citing Section 230, the U.S. District Court for the Eastern District of North Carolina held in AOL's favor, and the U.S. Court of Appeals for the Fourth Circuit denied Zeran's appeal.

In upholding the lower court's decision, the U.S. Court of Appeals for the Fourth Circuit noted that "lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions — such as deciding whether to publish, withdraw, postpone or alter content" are barred by Section 230. The court declared that Congress enacted Section 230 precisely because it recognized the threat that lawsuits pose to freedom of speech on the Internet:

> Interactive computer services have millions of users. The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It

> would be impossible for service providers to screen each of their millions of postings for possible problems.[11]

The appellate court noted that Section 230 was included to encourage service providers to "self-regulate the dissemination of offensive material over their servers." The court cited the case of *Stratton Oakmont Inc. v. Prodigy Servs. Co.*, 12 in which the plaintiffs sued Prodigy, an online service similar to AOL, for defamatory statements made anonymously on one of Prodigy's bulletin boards. The court held in favor of the plaintiffs, reasoning that Prodigy acted like a publisher of the defamatory message because it advertised its practice of controlling content on its service and because it actively screened and edited bulletin board messages. "Under that court's holding," the Fourth Circuit wrote, "computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher." According to this court, "Congress enacted Section 230 to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision."

Section 230 of the Communications Decency Act clearly prohibits Internet Service Providers from being held liable for speech located on their servers. However, ISPs may choose to regulate what their users say on their services. How ISPs have chosen to control the content of speech found on their systems is the subject of the following section of this report.

III. Internet Service Providers and Online Hate: Choices to Make

Internet Service Providers in some countries have formed industry associations that enforce codes banning hate speech. Such codes often mirror these nations' laws criminalizing hate speech. For instance, the Code of Practice of the Internet Service Providers Association (ISPA) of the United Kingdom states that British ISPs "shall use their reasonable endeavors to ensure … service and promotional material do not contain material inciting violence, sadism, cruelty or racial hatred."[13] In the United States, just as there are no laws criminalizing hate speech, no industry-wide body regulates the hosting of hate sites by ISPs. Rather, each ISP makes its own determination as to whether or not to host hate sites.

Of the thousands of access providers[14] in the United States, relatively few regulate hate speech per se. Instead, many choose to ban speech unprotected by the First Amendment, such as libelous or defamatory speech. Providers establish such rules voluntarily; legally they do not have to do so. In fact, Section 230 of the Communications Decency Act specifically states that providers cannot be held criminally liable for the speech of their users. For some companies, defense of "free speech" is the rationale for not prohibiting hate speech, even though they are not bound by the First Amendment's free speech protections.

Free Web-based hosting services and services with proprietary networks have been more willing to ban hateful sites and other racist content. There are fewer of these services, and, in general, they are available nationwide; have a prominent public profile; and are owned by large corporations. Some may have chosen to regulate hate speech out of public relations considerations, since they do not want the public to perceive them as haters' allies.

Regardless of whether they prohibit hate speech, the vast majority of access providers, free page-hosting services and services with proprietary networks openly proclaim their right to discharge their customers or delete content created by those customers entirely at their own discretion. As private entities these companies can legally act on their content policies at will and with impunity, whatever those policies may be.

A. Some ISPs Reject Hate Sites

Free Web-based page-hosting services such as GeoCities, Tripod and XOOM.com refuse to host hate sites. XOOM.com of San Francisco, California, bans "hate propaganda" and "hate mongering." Tripod, a subsidiary of Lycos, Inc. of Waltham, Massachusetts, prohibits "clear expressions of bigotry, racism or hatred." GeoCities, a subsidiary of Yahoo! Inc., prohibits "providing material that is grossly offensive to the online community, including blatant expressions of bigotry, prejudice, racism, hatred or excessive profanity."[15]

In February 1998, the free Web-based page-hosting service Angelfire also a subsidiary of Lycos, joined these services by banning hateful pages from its servers. The new Angelfire rules stated that "pages can not contain, or contain links to, any of the following: nudity, sex, pornography, foul language, hate propaganda, anything illegal, mail fraud or pyramid schemes."[16] Reserving "the right (for any reason or no reason) to remove any page," Angelfire also explained that persons creating the pages it hosts are, by doing so, stating that their creations do not promote "hate group propaganda."

Angelfire had hosted many pages of the racist National Association for the Advancement of White People that were removed under the service's new rules. "Can you please send out the word that Angelfire.com has destroyed all of the NAAWP Web sites," enraged NAAWP leader Ray Thomas wrote in the *Klan E-Mail* News Internet newsletter. "They pulled everyone [sic] of them without a notice of any kind."

Like free Web-based page-hosting services, some online services that function as ISPs but also provide proprietary content have banned hate speech. For instance, Prodigy Internet bars "blatant expressions of bigotry, racism and/or hate" from its users' Web pages.[17] Though many of these services, including Prodigy and Compuserve, have become less popular and shed much of their proprietary programming, one continues to grow: America Online (AOL) of Dulles, Virginia. Currently, AOL comprises "the largest interactive online community in the world," with a membership of more than 20 million households.[18]

Like Angelfire, AOL changed its policy on hate speech, infuriating the bigots who had until that time housed their pages on its servers. In April 1997, ADL wrote to AOL about its hosting the Web site for the "Realm of Texas" of Thom Robb's Knights of the Ku Klux Klan. ADL encouraged AOL to enforce its own, publicly posted "Rules of the Road," which at that time declared that "hateful language … is not allowed" and prohibited attacks based on "a person's race, national origin, ethnicity or religion."

AOL declined to remove the Realm of Texas site, explaining that the site was "historical" in nature and therefore not a violation of its "Rules of the Road." Additionally, AOL asserted that the "Rules" applied primarily to the contents of its proprietary network, not necessarily the publicly available Web pages its users created.

However, AOL finally removed the Realm of Texas site and several other hateful pages from its servers on July 15, 1998, when its new "Terms of Service" (TOS) went into effect. The new TOS, to which all AOL users must agree as a prerequisite for using the service, state that users "will be considered in violation" if they "transmit or facilitate distribution of content that is … racially or ethnically offensive." Additionally, the new TOS flatly declares that "there is no place on the service where hate speech is tolerated," either on AOL's proprietary network or on the Web pages it hosts. "Hate speech is never allowed," the new TOS declares. Furthermore, like Angelfire and other services, AOL reserves the right to "terminate or cancel" any customer's membership "at any time."

As a result of this policy change, the Web pages of Alex Curtis and other extremists were removed from AOL's servers. In his *Nationalist Observer* E-mail magazine, Curtis chastised AOL, alleging that Jewish pressure led to its change of policy:

> Next time some weak-minded individuals who can't stand the heat of the jew [sic] censor you, only take it as an opportunity to be stronger and freer to do what needs to be done. The Nationalist Observer will dump jew-corroded [sic] AOL … I endorse all racialists to dump AOL as well, and whenever the opportunity arises, to do as much physical or financial damage to AOL as possible.[19]

In place of the KKK Realm of Texas site, that site's administrator placed a page that recognized AOL's policy change. "All of the sites that are pro-White in nature have been taken down," the page read.

It listed disapprovingly "a few of the sites that *are* approved by AOL," including the "Today in Black History" page, a Black book catalog, and the Chevron Lesbian and Gay Employees Association site.

B. ISPs Allowing Hate Speech

While most Internet access providers have acceptable use policies, most such policies do not ban hate speech. Some of these services have cited defense of the First Amendment's free speech guarantees in explaining their policies, though as private businesses they are not bound by the First Amendment.

EarthLink of Pasadena, California, raises the issue of free speech in its "Acceptable Use Policy." EarthLink "supports the free flow of information and ideas over the Internet" and does not "actively monitor" or "exercise editorial control over" the "content of any web site, electronic mail transmission, mailing list, news group or other material created or accessible over EarthLink services." However, using EarthLink "for illegal purposes or in support of illegal activities," such as "threatening bodily harm or property damage to individuals or groups," is considered a "violation" of EarthLink's policy. EarthLink hosts the neo-Nazi Web site *For Folk and Fatherland* that reprints Hitler's *Mein Kampf* and more than two dozen of Hitler's speeches.

Another major ISP, GTE.NET of Irving, Texas, voices even stronger support for free speech. GTE.NET stands by "the rights and privileges established within the First Amendment of the Constitution of the United States." It "will not censor any content of information passing through its network unless the information is deemed illegal" by law enforcement authorities, in which case it will cooperate with those authorities "in the investigation of any suspected criminal or civil order of infringements."

Many sites hosted by EarthLink, GTE.NET and other large access providers have addresses that include the name of the service that hosts them. (This is also true for services with proprietary content, such as AOL, and free Web page hosting services, such as Angelfire.)

However, it is not immediately apparent which service is hosting certain hate sites. Technologically sophisticated haters and established hate groups purchase their own domain names. (Domain names, such as "k-k-k.com" are the central, identifying portion of Web site addresses). These domain names do not point to the ISPs that host their sites. Most significant hate sites fall into this category.

For instance, BitShop, an Internet service in College Park, Maryland, hosts the official *National Alliance* Web site that does not mention BitShop. BitShop's "Terms and Conditions" prohibit the "transmission or storage of any information, data or material in violation of any United States Federal, State or City law" including "material legally judged to be threatening or obscene." BitShop also prohibits "pornography and sex-related merchandising," but it fails to mention hate speech.

Welcoming Hate Speech

Some Web services associated with hatemongers welcome hate speech. For instance, Don Black, creator of *Stormfront*, leapt into the business of hosting extremist sites. Black writes:

> Stormfront is an association of White activists on the Internet whose work is partially

> supported by providing webhosting for other sites. With increasing pressure to censure politically unfashionable ideas, we must work even harder to ensure our point of view continues to be accessible.

At least one extremist removed from another online service because of his hateful words has already taken refuge on Black's server. Alex Curtis's *Nationalist Observer* Web site, once hosted by America Online, now resides there. No matter how many mainstream ISPs refuse to service a bigoted site, those determined to set up a racist Web site will find bigots like Black willing hosts.

III. UNIVERSITIES AS INTERNET SERVICE PROVIDERS

A. Background

Though commercial Internet services host the vast majority of hate sites, a few have called university Web servers home. Like commercial services, private universities can legally choose to host hate sites or refuse to host them. While public universities must respect First Amendment protections of speech, this does not necessarily force them to host hate sites. They could still choose not to host any personal sites at all.

B. Universities Hosting Hate Sites

Holocaust-denier Arthur Butz is an Associate Professor of Electrical and Computer Engineering at Northwestern University, a private institution located in Evanston, Illinois. In 1976, he wrote *The Hoax of the Twentieth Century*, one of the earliest English-language Holocaust-denial books. In mid-1996, Butz established a home page on the Web server at Northwestern reserved for the personal use of students and faculty. At this site, Butz has posted a few of his Holocaust-denial articles and a prominent link to the Web site of the Institute for Historical Review (IHR), arguably the most important outlet for Holocaust-denial propaganda in the world.

Northwestern was criticized by the public and in the press for providing a home for views that are, as the *Chicago Tribune* wrote, "demonstrably false." The *Tribune* argued that the university was "metaphorically giving Butz free stationery with NU's letterhead on it. In effect it also is paying Butz … to make his material denying the Holocaust available to millions of Internet users around the world." Many were angered that the university, a center of legitimate academic research, could provide a forum for anti-Semitism masquerading as "scholarship." Even Northwestern President Henry S. Bienen condemned Butz's views, calling them "a contemptible insult" to all who experienced the Holocaust.

Yet Butz's page remains on Northwestern's servers. Defending Northwestern's decision to allow the site to stay, Bienen echoed the university's stated policy: that its network is "a free and open forum for the expression of ideas, including viewpoints that are strange, unorthodox, or unpopular."[20] Furthermore, according to its "WWW Disclaimer," Northwestern "is not responsible for the content of every page" on its servers, and the "opinions expressed in personal or nondepartmental home pages should be construed as those of its author, who is responsible for the information contained therein."

While ADL opposes attempts to control the content of material on the Web, it encourages the condemnation of hate speech. ADL commended Bienen for his press release, which forcefully conveyed that manipulating historical facts to spread anti-Semitic propaganda, as Butz does, foments hate. ADL encouraged Northwestern to keep Bienen's statement posted on its Web site as a way of promoting a positive response to hate messages in cyberspace.

Though Northwestern, as a private institution, could legally ban hateful pages like Butz's from its servers, it chooses otherwise, citing "the value of diversity and free speech." In contrast, public universities like Washington State University have no choice but to respect "free speech" if they decide to

house the personal Web sites of students, staff and faculty on their servers.

WSU voices its respect "for the principles of freedom of speech, freedom of expression and academic freedom," reserving the right to remove Web pages only if they "may violate state or Federal law." WSU claims that the pages it hosts do "not represent the official statements or views of Washington State University" and denies any responsibility for "the content, accuracy, or timeliness of information contained" on such pages.[21]

Like Arthur Butz's home page, a page hosted by WSU, the Students Revisionist Resource Site, spreads Holocaust-denial propaganda. Using the pseudonym "Lawrence Pauling," WSU undergraduate Justin Reid maintains the site, posting the works of well-known Holocaust deniers such as Bradley Smith in addition to the writings of Neil Camberly, allegedly a student at the University of Washington in Seattle. Reid's site houses a copy of the *Zündelsite*, a major source of Holocaust-denial propaganda on the Web, and real-time video presentations by denier David Irving, whom Reid brought to speak at the WSU campus on April 13, 1998.

Though WSU cannot bar constitutionally protected speech from its servers simply because that speech is hate-filled, it could choose to restrict use of its servers to official university business. By doing so, it would refuse to serve students, faculty and others wishing to create personal home pages, including hate propagandists like Reid.

C. Universities Not Hosting Hate Sites

One public university that enforces restrictions is the University of Illinois, which supplies space only for Web sites "in support of the educational, research and public service missions of the University" and declares that sites on its servers "must be limited to those purposes."[22]

Similarly, the University of Massachusetts at Amherst specifies that its employees and students may use university computing resources "only for work done for the University, and only when it is appropriate that the work be supported by public funds."[23] In 1996, when German ISP T-Online denied its customers access to the *Zündelsite*, a student at the University of Massachusetts at Amherst posted a copy of that site on his school's servers. The university removed the copy, claiming that its policy prohibited the use of public resources for political purposes.

V. PROTECTING INTERNET USERS: FILTERING ONLINE CONTENT

Visiting a Web page involves two essential parties: the Web user accessing the page and the server hosting it. While ISPs and other organizations that host Web sites can restrict hate speech on one end of this transaction, by refusing to harbor a hate site, hate speech can also be restricted on the other end, by using a "filter" or other software that denies the Web user the ability to access sites containing certain speech.

One technology that can be used to screen out unacceptable content is the Platform for Internet Content Selection (PICS), proposed by the World Wide Web Consortium, an international computer industry organization. PICS can rate the content of Web sites based on a number of factors, such as language or violence. A Web site can voluntarily rate itself using the PICS criteria. In addition, multiple, independent labeling services can rate a site. Web users wishing to employ PICS can use a site's own ratings or those of a third party. Based on the ratings employed, the Internet user's Web browser allows or denies access to a given site.

A number of commercial Internet filtering software products, some using PICS, are readily available. These programs contain built-in opinions of the appropriateness of Web sites, often judging them on a variety of criteria, from drug references to nudity. Such software, which can be easily installed on home computers, prevents users of a particular computer or computer system from accessing certain online content, such as pornography or hate speech.

A. Private Use of Filtering Software

Bigots have the right to post hate propaganda, but Web users have the right to choose not to look at it. When private persons and entities voluntarily use software that helps them avoid hateful sites, the First Amendment is not implicated since no government action is involved.

Eager to protect children from damaging online materials, the U.S. Congress explicitly praised parental use of filtering software in Section 230 of the Communications Decency Act. "It is the policy of the United States," that section reads, "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."[24]

Like private individuals, private schools and corporations that supply access to the Internet may legally use filtering software. Numerous corporations filter the Internet access they provide to their employees so those employees cannot spend their time in the office using online resources unrelated to their work.

B. Public Use of Filtering Software

While private individuals, schools and corporations have the right to use filtering software, using them in public schools and libraries raises complex legal and policy questions. Funded by government bodies, these institutions are bound by the First and 14th Amendments. Protected speech may not be screened out; however speech falling within established categories of unprotected speech, such as incite-

ful, threatening, libelous or obscene speech, may be restricted. Hate speech rarely falls into traditional categories of unprotected speech. The extent to which public institutions can filter information found on the Internet has been hotly debated in the media and has resulted in a few notable lawsuits.

C. Litigation on Filters

Mainstream Loudoun v. Board of Trustees of the Loudoun County Library, 24 F. Supp. 2d 552 (E.D. Va. 1998)

In November 1998, a Federal District Court declared unconstitutional a Loudoun County Library Board policy requiring the installation of filtering software on every public library Internet terminal in Loudoun County, Virginia. The court held that the Board's policy violated the First Amendment by wrongfully restricting "the access of adult patrons to protected material just because the material is unfit for minors." The court agreed with the plaintiffs, owners and operators of Web sites screened out by the filtering software, who argued that the filters blocked speech that is constitutionally protected with regard to adults. The Board's policy mandated the use of filtering software on all library Internet terminals, denying adults using those terminals their right to view constitutionally protected speech.

The court's decision relied in part on the Supreme Court case, *Board of Education v. Pico*, 457 U.S. 853 (1982), which involved a policy of removing certain books from a high school library if the books were deemed "anti-American, anti-Christian, anti-Sem[i]tic, and just plain filthy."[25] Based on this decision, the court held that a library could select those materials it wanted for its collection, but had considerably less discretion with respect to *removing* materials. The Library Board's action of installing filtering software was characterized by the court as a removal decision, not an acquisitional one. Therefore, the First Amendment considerably limited the discretion of the library to take the action. The court noted that installing filtering software on some, but not all, of a library's computers might provide a more appropriate option, though the court refrained from ruling on the constitutionality of doing so.

Kathleen R. v. City of Livermore

While *Mainstream Loudoun* dealt with the constitutionality of public libraries regulating access to online speech, *Kathleen R. v. City of Livermore* addressed the failure of a library to take such action. The plaintiff, a parent of a child who used a computer at a public library to download pornography, sought to compel that library to install filtering software on its computers designated for children's use. In her complaint, she asserted that the library's lack of filtering software was a "nuisance"; that its unfettered access constituted "a waste of public funds"; and that this access made the library "unsafe for children."[26]

In January 1999, a California state court dismissed the suit. Echoing briefs filed by the City of Livermore and the American Civil Liberties Union (ACLU), the court ruled that the city cannot be held liable for children downloading pornography from the Internet because the library is protected by Section 230 of the Communications Decency Act which prohibits the imposition of liability on an "interactive computer service," in this case a library, for providing access to online material while not acting as the "publisher" or "speaker" of that material. An appeal in the case is pending.

D. General Trends

Although too early to tell how the courts will answer the questions concerning the constitutionality of public libraries and schools using filters, some general trends may be inferred from the above cases and existing First Amendment jurisprudence. Libraries that provide Internet access to their patrons may not install filtering devices on all of their computers, unless the filtering devices block only those categories of speech which are unprotected. However, most filters block not only hard-core pornography, but also nudity, adult language, hate speech and other types of speech which are protected by the First Amendment's Free Speech Clause. Less restrictive alternatives to using filtering devices on all library terminals may withstand constitutional scrutiny. It is still unclear whether filtering some, but not all, Internet terminals in public libraries is constitutionally permissible. The dismissal of *Kathleen R. v. City of Livermore* suggests that public libraries are not liable for exposing children to inappropriate online material. Despite this ambiguity, 14.6 per cent of U.S. public libraries use filtering software on some or all of their Internet workstations.[27]

E. Filtering Products That Screen Hate

Though most of the public attention concerning filtering software has focused on blocking pornography, many products also block hate speech. For example, in addition to blocking gambling sites and sexually explicit pages, the product *SurfWatch* also filters out hate speech. Users of this program will find that they cannot access Don Black's *Stormfront*, David Duke's Web site or the home page of the Knights of the White Kamellia, among others. The filtering software product *Bess* blocks online content that advocates "discrimination against others based on race, religion, gender, nationality or sexual orientation."

In 1998, ADL released its own filtering software, *HateFilter*®, which blocks access to sites that promote hatred or hostility towards groups on the basis of their religion, race, ethnicity, sexual orientation or other immutable characteristics. *HateFilter* affords parents the ability to exercise discretion over which Internet materials their children access. An integral component of *HateFilter* is to educate Web users about the nature of bigotry. When an individual using a computer with ADL *HateFilter* tries to view a hate site, access is blocked. Instead, the user sees a special ADL *HateFilter* screen, which allows the user to continue to a section of ADL's Web site that provides detailed information about different kinds of hate groups.

This feature reinforces ADL's central response to online bigotry: challenging the lies of haters by exposing their agendas. In addition to helping Web users avoid hate sites, *HateFilter* teaches them why those sites should be rejected, why we should all renounce the bigotry in our midst.

VI. Examples of Foreign Regulation of Online Hate: Germany and Canada

Hate speech on the Internet is not just an American phenomenon. Globally, computer users, attorneys, and lawmakers are struggling to find ways to combat this complex problem, a challenge made more difficult because cyberspace has no boundaries. Therefore, a computer user in Western Europe can access sites made available by American service providers, and U.S. citizens can read Web sites created thousands of miles from American borders. Countries across the world have had to decide which actions (e.g., viewing controversial sites, creating offensive sites, offering access to prohibited sites) should be punished. Not surprisingly, many different approaches have been tried, and many foreign countries, not bound by constraints such as the First Amendment, have been more aggressive than the United States in attempting to fight hate on the Internet. Most Western democracies, for instance, already have enacted laws more restrictive of hate speech than those found in the United States. These countries — including France, Germany, and Canada — seek to balance the right to free expression, including speech on the Internet, with their society's need to protect its citizens from bigotry.

Denmark and other nations have successfully prosecuted bigoted speech that in the United States would likely have been protected by the First Amendment. Among these, Canada and Germany are of particular interest, since both of these nations have already engaged in campaigns to combat hate speech on the Internet.

However, hate speech laws in these countries cannot stop local bigots from creating and maintaining hateful Web sites. American free speech protections create a "safe haven" for foreign haters: they can always establish Web sites on the servers of U.S. Internet Service Providers (ISPs). Still, international efforts to combat hate on the Internet are important as examples of different methods of stopping online bigotry and prejudice. It is instructive, therefore, to consider some of the more notable attempts worldwide to regulate Internet hate.

A. Germany

Germany's approach to the protection of speech is markedly different from the United States; this divergence is largely due to Germany's unique history involving religious and racial hatred. The German Constitution was constructed, and has subsequently been interpreted by Germany's Constitutional Court, so as to permit free expression within tight limits. In particular, racially biased speech and extremist political parties are not tolerated under Germany's Constitution.

Adopted in 1949, Article 5 of the German Constitution, known as the German Basic Law, affirms freedom of opinion and expression, stating that "everybody has the right freely to express and disseminate their opinions orally, in writing or visually and to obtain information from generally accessible sources without hindrance." This right is not absolute, however and is balanced against other societal interests. The second clause of Article 5 subjects this right to "the citizen's right to personal respect" and the guarantee of human dignity set out in Article 1 of the Basic Law.

Article 5 has also come into conflict with German criminal laws. Criminal Code sections relevant to

hate speech include those which prohibit the defamation and denigration of the character of deceased persons; one that makes incitement to violence and hatred a punishable offense; and another which criminalizes the depiction of violence. Additionally, when speech includes a claim of fact, that speech is protected by Article 5 only to the extent that its basis in fact can be verified. An April 1994 ruling of the Federal Constitutional Court confirmed that Holocaust denial is not protected speech under Article 5 because it expresses a "claim of fact that has been proven untrue."

These laws have been used to vigorously prosecute hate speech. For example, in December 1999, neo-Nazi Manfred Roeder was sentenced to two years in prison for referring to the Holocaust as "humbug" during an August 1998 rally.[28]

In 1995 and 1996, Germany began investigating the applicability of its Criminal Code to the Internet. These investigations focused both on ISPs providing access to illegal material and the creators of such material. In 1995, the Munich Public Prosecutor's office investigated the ISP CompuServe (a subsidiary of the American firm of the same name) for hosting pornographic sites. In 1996, the ISP T-Online, a subsidiary of the German phone company Telekom, reported that it was blocking access to the *Zündelsite*, a well-known Holocaust-denial Web site, after it heard that German prosecutors were investigating the site. The Public Prosecutor's office in Manheim, Germany charged Canadian Holocaust-denier Ernst Zündel with violating Criminal Code Section 131 (depiction of violence) and acknowledged that the ISPs providing their subscribers with access to the *Zündelsite* might be criminally liable.[29]

On July 4, 1997, Germany took steps towards clarifying the application of its laws to Internet bigotry by passing the so-called "Multimedia Law." Under this law, ISPs can be prosecuted if they knowingly make illegal content, such as Holocaust denial material, "available for use" and it is "technically possible and reasonable" to refrain from doing so. ISPs are not liable for automatically and temporarily storing illegal material due to a user's request, as when a German user accesses a hateful Web site hosted outside of Germany.[30]

In May 1998, Felix Somm, former managing director of CompuServe's German division, was found guilty of violating the "Multimedia Law" because he had made illegal pornographic USENET newsgroups available to CompuServe's German users.[31] In November 1999, a Bavarian court overturned the Somm verdict, ruling that Somm could not have reasonably done more about the newsgroups than he did. Somm had requested that CompuServe, which housed the newsgroups accessible to German users on its servers in the United States, block access to them.

The German government realizes that German extremists can still create Web sites with impunity by using pseudonyms and finding providers in the United States, Canada, or other nations to host their sites. As of March 1998, the Federal Office for Protection of the Constitution had found 10 Web sites, some of which "disseminate seditious propaganda," that German extremists operate via foreign providers. In addition, German neo-Nazis have posted hate pages written in English on servers in the U.S., and extremists outside Germany have begun posting German-language hate propaganda online.[32]

German authorities have also been concerned about hateful Web sites that are neither written in German nor created by residents of Germany but are accessible there. Holocaust-denier Frederick Toben of Norwood, Australia, is the creator of the Adelaide Institute Web site, which is hosted by an Australian

ISP. Toben visited Mannheim, Germany, in April 1999 with the intention of discussing Germany's laws prohibiting Holocaust denial with prosecutor Hans Klein.[33] At a meeting with Klein, Toben was arrested by German authorities and charged with violating those laws.

This case against a nonresident of Germany was not unprecedented. In August 1996, a Hamburg court found longtime hatemonger Gary Lauck guilty of incitement to violence and incitement of hatred as a result of his distribution of German-language neo-Nazi publications and propaganda materials. In convicting Lauck, the court cited Section 9 of the Criminal Code, which declares that a crime is committed where its effect is felt. The court considered Lauck, a citizen and resident of the United States, to have committed a crime in Germany, where his propaganda was distributed.

Toben was convicted in November 1999 and sentenced to 10 months in prison, seven of which he had already served. German sympathizers raised the funds necessary to win his early release.

Yet Klein, who prosecuted the case, had argued for a much harsher sentence. The punishment was not more severe because the presiding judge determined that Toben could not be penalized for posting online material in English on a server outside of Germany. The judge deemed only Toben's printed Holocaust-denial material a violation of German law.[34]

Klein immediately filed an appeal, warning that the court's decision set a dangerous precedent. "This is the first time a court in Germany has decided that some things which are said in Germany on the Internet cannot be subject to German laws. This is a very bad thing. It will undermine our laws which are very important for ensuring that history in Germany is not repeated.''[35]

B. Canada[36]

Though free speech is protected by the Canadian Charter of Rights and Freedoms, Sections 318 through 320 of the Canadian Criminal Code, which criminalize hate speech, have been upheld as constitutional by the country's Supreme Court. Additionally, the Canadian Human Rights Act, a civil measure, targets hate speech.

Section 318 of the Criminal Code states that "every one who advocates or promotes genocide" is "guilty of an indictable offence and liable to imprisonment." Section 320 allows judges who have "reasonable grounds" for believing that there exists "hate propaganda" within their jurisdiction to issue warrants authorizing seizure of that propaganda. Barring certain exceptions, Section 319 aims to punish people who, "communicating statements" outside of private conversation, "willfully" promote "hatred against any identifiable group." This Section may be particularly effective as applied to the Internet, for "communicating" is meant to include communication "by telephone, broadcasting or other audible or visible means."

Section 13 of the Canadian Human Rights Act, like Section 319 of the Criminal Code, addresses the telephonic communication of bigotry. That Section declares it "a discriminatory practice" when people repeatedly "communicate telephonically" materials that are "likely to expose" people to "hatred or contempt" because they are "identifiable on the basis of" race, religion, or another "prohibited ground of discrimination." The Human Rights Act allows for the formation of Human Rights Tribunals to hear

cases alleging violations of its provisions. If a Tribunal finds a defendant guilty, it can, among other remedies, order that defendant to "cease the discriminatory practice."

In 1997, a Human Rights Tribunal convened following a complaint filed by Sabina Citron and the Toronto Mayor's Committee on Community and Race Relations against Holocaust-denier Ernst Zündel and the *Zündelsite*. The complaint alleged that Zündel and the Web site bearing his name telephonically communicates material that discriminates on the grounds of race, religion, and national or ethnic origin, thereby violating Section 13 of the Canadian Human Rights Act. Issues involved in the Tribunal's proceedings include questions about whether the Internet can be considered a telephonic device under Section 13; whether the *Zündelsite* promotes hatred; and whether Zündel controls the *Zündelsite*. The League for Human Rights of B'nai Brith Canada, an affiliate of ADL, has full standing as an intervenor in the case.

Zündel steadfastly denies that he manages the *Zündelsite*, claiming that his compatriot, Ingrid Rimland, who resides in the United States, is solely responsible for it. However, Rimland clearly gets her marching orders directly from Zündel.[37]

The applicability of Section 13 and the jurisdiction of the Tribunal have so far been upheld by a Canadian Federal Court. Computers using the Internet communicate with each other using phone lines; hence, the Internet can be considered a telephonic device.

As of late 1999, the Zündel case had not yet been resolved. Though that case stands alone on Canadian dockets with regard to the prosecution of online hate speech, the Human Rights Act, as well as the Criminal Code, were cited in another high-profile Canadian episode involving online hate, that of Internet Service Provider Bernard Klatt.

In February 1998, British and French police arrested 13 people affiliated with the French neo-Nazi Skinhead group Charlemagne Hammer Skins (CHS). Those arrested were charged with crimes including promoting racial hatred, uttering death threats and desecrating a grave. Central to these charges was the CHS Web site, which contained Holocaust-denial material such as *Did Six Million Really Die?* by Richard Harwood and death threats directed at many prominent French Jews.

At first, the CHS Web site was hosted by America Online's service in France. When that ISP refused to service it further, the group moved its site to the servers at Klatt's Fairview Technology Centre, located in Oliver, British Columbia. There, it joined the sites of numerous other hate groups.

In March 1998, B'nai Brith Canada requested that BC Telecom, the telephone company that services the Fairview Technology Centre, void its contract with Klatt. B'nai Brith asserted that BC Telecom has the right to choose not to do business with those supporting online hate. He explained that, as private enterprises, neither BC Telecom nor Fairview is legally bound by Canadian free speech guarantees, but that both are bound by the Canadian Human Rights Act, specifically Section 13. Though he noted that Section 3 of the Human Rights Act protects owners and operators of telecommunications services from liability, B'nai Brith declared that BC Telecom should be held responsible for the sites on Klatt's servers because it had already received complaints about those sites and was aware of their contents.[38]

BC Telecom hired outside counsel to investigate the hate sites hosted by Klatt. Counsel found that the sites violated Canada's criminal code provisions against hate speech. Nonetheless, BC Telecom refused to stop servicing Klatt. B'nai Brith reiterated its request and filed a complaint with the Canadian Association of Internet Providers (CAIP), of which BC Telecom is a member. The CAIP Code of Conduct holds that its members cannot knowingly host illegal content, and that they must make a reasonable effort to investigate complaints and take appropriate action.

In late April 1998, Klatt sold his Web hosting business to Valley Internet Providers (VIP). While denying the sale was caused by anti-hate protests, the main reason he gave for selling his service involved the negative financial consequences of signing a new contract with BC Telecom. The new contract, which Klatt would have had to sign in order to win an equipment upgrade, contained provisions holding him legally and financially responsible for the sites he hosted. Faced with the fact that he would be forced by Canadian laws to pay for the bigotry of the sites he had been hosting, Klatt chose to shut down his operation.

The sites Klatt housed did not disappear. Some survived and headed South. For instance, the *Freedom Site* moved to an American ISP located in Boca Raton, Florida.

As in Germany with T-Online, hate speech laws in Canada have counteracted online hate by influencing the behavior of ISPs such as the Fairview Technology Centre. However, it may be difficult to use these laws to prosecute many of the hate sites themselves due to jurisdictional issues. Sites such as the *Zündelsite* and the *Freedom Site* can, and do, find homes in the United States, where they are protected by the First Amendment.

VII. International Regulation of Online Hate

International organizations such as the European Union and the United Nations have also tried to balance free speech rights with the restriction of hate speech. These organizations too have pondered the regulatory difficulties created by bigots housing their sites on servers in other nations and questioned the liability of Internet Service Providers.

The European Union

The European Union (EU), composed of 15 European nations, maintains that "everyone has the right to freedom of expression." However, the exercise of that right "carries with it duties and responsibilities" and may be subject to such "formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society," including laws restricting hate speech.

The European Convention for the Protection of Human Rights and Fundamental Freedom (ECHR) states that member nations' legislatures may enact exceptions to freedom of expression only where certain conditions exist. Laws establishing the exceptions to freedom of speech must be clear and precise; those exceptions must correspond to an imperative social need; and they must entail a legitimate goal, such as "national security, crime prevention, the protection of morality or the protection of the reputation or rights of others."[39] Presumably, member states believe that their hate speech laws meet these conditions.

On January 25, 1999, the EU adopted a four-year, 25-million Euro (U.S. $26.4 million) "action plan" on "promoting safer use of the Internet by combating illegal and harmful content," including "racist and xenophobic ideas." The promotion of industry self-regulation and content monitoring, as well as the development of filtering tools and rating systems, are central to the plan.

The plan asks groups of ISPs to institute "codes of conduct" that regulate online hate and other objectionable material. It proposes a system of "quality-site labels" to help Internet users identify the ISPs that adhere to such codes. With regard to content monitoring, the plan calls for the establishment of a "European network of centres (known as hot-lines) which allow users to report content which they come across in the course of their use of the Internet and which they consider to be illegal."

The EU recognizes that "where certain acts are punishable under the criminal law of one Member State, but not in another, practical difficulties of enforcing the law may arise."[40] For example, German regulations against Holocaust denial might not be enforceable against Holocaust deniers based in England, though these deniers' Web sites might be easily accessible by German Web users. In the "action plan," the "responsibility for prosecuting and punishing those responsible for illegal content" remains with each member nation's law enforcement authorities. Of course, enforcement in a nation outside of the EU, such as the United States, would be even more difficult, if not impossible.

In addition to "codes of conduct" and "hot-lines," the "action plan" encourages industry to provide filtering tools and rating systems to Internet users. In the course of the plan's four-year term, the EU hopes to demonstrate both "the potential and the limitations" of filtering and rating systems "in a real world environment," with the objective of encouraging the establishment of European systems and familiarizing users with their use.

INCORE (Internet Content Rating for Europe), a group of European organizations working to create a generic filtering and rating system for European Internet users, has received funding from the European Commission under the "action plan." In September 1999, INCORE and the Bertelsmann Foundation brought together experts in Munich for an Internet Content Summit. At this meeting, the Bertelsmann Foundation released its "Memorandum on Self-Regulation of Internet Content," which reflected the EU "action plan." Most significantly, the "Memorandum" argued in favor of self-labeling of all Internet content so that third parties can filter that content.

The architects of the plan believe that even objectionable sites will rate themselves once major Internet companies rate their own sites and promote the system, making its use commonplace for Internet users. However, some civil libertarians believe that the Bertelsmann system will be used by repressive governments to effectively control their populations' Net experience.

The United Nations

The United Nations (UN), which has 185 member states, convened a seminar to discuss regulating online hate in November 1997 in Geneva, Switzerland. The seminar focused on Internet hate in light of the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), described as "the international community's primary legal instrument for combating racial hatred and discrimination."

The ICERD, which entered into force on January 4, 1969, stipulates in Article 4 that nations ratifying the convention are required to "declare an offence punishable by law" the dissemination of ideas "based on racial superiority or hatred." Additionally, the convention requires these nations to "declare illegal and prohibit" all organizations and organized activities that "promote and incite racial discrimination."

Freedom of speech is also recognized in international law. Article 19 of the Universal Declaration of Human Rights provided that "Everyone has the right to freedom of opinion and expression." However, similar to the European Convention for the Protection of Human Rights and Fundamental Freedom, Article 29 of the Universal Declaration deems these rights subject to limitations determined by laws made "for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society." These principles were rearticulated and enshrined in international law when the International Covenant on Civil and Political Rights (ICCPR) entered into force on March 23, 1976.

In March 1993, the UN Committee for the Eradication of Racial Discrimination (CERD) reminded parties to the ICERD that Article 4 was of a "mandatory nature" and that they had the obligation "not only to enact laws to criminalize racial discrimination but also to ensure that the laws were effectively enforced by national tribunals and other State institutions." Additionally, at least one member of the CERD believes that "declarations of interpretation" of the ICERD by participating nations have "no legal effect on the obligations under the Convention of the States that made them."[41]

Despite the insistence of UN officials on the legality and binding force of the ICERD, when it comes to the Internet, inherent problems of implementation remain. Those at the UN seminar wondered:

> Would there be cyber courts, cyber judges and cyber sleuths? Who would be sentenced? Would it simply be the person responsible for sending the message, or would it also be the service providers? If the service providers were also prosecuted and sentenced, would they be accomplices, or something else?[42]

These issues posed further difficulties when the UN seminar attendees took the United States into consideration. Though the ICERD may be legal under the ICCPR's allowance for laws that restrict free speech, it is not consistent with U.S. free speech considerations.

When the U.S. signed the ICERD on September 28, 1966, it noted that "nothing in the Convention shall be deemed to require or to authorize legislation or other action" by the U.S. that is "incompatible" with the U.S. Constitution. When it ratified the ICERD on October 21, 1994, the U.S. Senate stated the following:

> The Constitution and laws of the United States contain extensive protections of individual freedom of speech, expression and association. Accordingly, the United States does not accept any obligation under this Convention, in particular under articles 4 and 7, to restrict those rights, through the adoption of legislation or any other measures, to the extent that they are protected by the Constitution and laws of the United States.[43]

Participants in the UN seminar understood that "the regulation of racist speech was held to violate" U.S. free speech rights. The case of the United States was described by one attendee as "sui generis" because the First Amendment guaranteed "virtually absolute freedom of speech." Significantly, those at the U.N. seminar recognized that "national laws prohibiting racist propaganda on the Internet could not pursue criminals to countries such as the United States, where the prohibited speech was protected under the Constitution."[44]

---

1 Certain limited categories of speech are considered unprotected, and not subject to this high standard. As the Supreme Court noted in the case of *Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942), "There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem." The Court gave examples of such categories of speech, including, "the obscene, the profane, the libelous and the insulting or 'fighting words'.... " The government may regulate these categories of speech through *content-based* restrictions. Several lawsuits have already been filed challenging the use of such types of speech online.

2 *Black's Law Dictionary*, Abridged Fifth Edition, by Henry Campbell Black, West Publishing Company, St. Paul, Minnesota, 1983, pg. 769

3 "Legal Aspects of Government-Sponsored Prohibitions Against Racist Propaganda on the Internet: The U.S. Perspective" by Philip Reitinger, United States Department of Justice, presented at the Seminar on the Role of the Internet with regard to the provisions of the International Convention on the Elimination of All forms of Racial Discrimination, November 1997

4 Id.

5 395 U.S. 444 (1969)

6 *U.S. v. Richard Machado*, Exhibit 1, filed August 19, 1997

7 United States Code, Title 47, Section 230

8 *Doe v. America Online Inc*., State of Florida Circuit Court for the 5th Judicial Circuit, Case No. CL 97-631AE, decided June 26, 1997

9 "In Drudge Case, AOL Finds Shelter in Decency Act," by Jeri Clausing, *The New York Times on the Web*, April 24, 1998

10 "Echoes of the Railroad Age in AOL Decision," by Carl S. Kaplan, *The New York Times* on the Web, July 3, 1998

11 *Zeran v. America Online Inc*., U.S. 4th Circuit Court of Appeals, Case No. 97-1523 (Nov. 12, 1997)

12 *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, New York Supreme Court, Case No. WL-323710 (May 24, 1995)

13 "Hate on the Internet," by Karen R. Mock and Lisa Armony, *Speaking About Rights*, Volume XIII, No. 2, 1998

14 Three types of Internet services based in the U.S., all of which can legally be regarded as "Internet Service Providers," generally provide space for users' Web pages. Web-based Web page hosting services such as Tripod provide this space free of charge but do not provide a connection to the Web, which users must already possess. Unlike these free Web-based hosting services, Internet Service Providers (ISPs) in the classic sense, or Internet access providers, charge their customers, often providing them with a dial-up connection to the Internet, an E-mail account, access to Usenet newsgroups and Internet Relay Chat, and space for building a Web page. Finally, some services, such as America Online (AOL), give users everything that access providers offer plus access to their own, proprietary networks.

15 " GeoCities Personal Home Page and Chat and Forum Content Guidelines," from the GeoCities Web site, retrieved December 1998

16 "Angelfire Rules and Regulations," from the *Angelfire* Web site, retrieved December 1998

17 "Alert Form," from the *Prodigy Internet Personal Web Pages* Web site, retrieved December 1998

18 "Profile," from the *America Online* Web site, retrieved January 2000

19 *Nationalist Observer* E-mail magazine, "Racial Reader's Forum," July 15, 1998

20 Statement by Northwestern University President Henry S. Bienen regarding Associate Professor Arthur Butz and his Web page, Northwestern University Web site, retrieved January 1999

21 "Disclaimer," from the Washington State University Web site, retrieved January 1999

22 "UIUC Computing and Networking Policies," August 15, 1997, from the University of Illinois Web site, retrieved January 1999

23 "Office of Information Technologies Acceptable Use Policy," University of Massachusetts at Amherst Web site, retrieved January 1999

24 United States Code, Title 47, Section 230

25 *Board of Education v. Pico*, 457 U.S. 853 (1982)

26 "Complaint for Injunction Relief," *Kathleen R. v. City of Livermore*, filed May 28, 1998

27 "The 1998 National Survey of U.S. Public Library Outlet Internet Connectivity: Summary Results," American Library Association Office for Information Technology Policy, American Library Association Web site, retrieved December 1998

28 "Neo-Nazi Gets Two Years in Prison for Denying Holocaust," Associated Press, December 3, 1999

29 "Freedom of Speech and Recent Legal Controversies in Germany," *German Information Center* Web site, under the auspices of the German Foreign Ministry, retrieved December 1998

30 Act on the Utilization of Teleservices, German Federal Law Gazette, 1997 I 1870, translated by Janet Barton

31 "Germany's Internet Angst," by David Hudson, *Wired News*, June 11, 1998

32 *Right-wing Extremist Activities in Internet, Federal Office for Protection of the Constitution* Web site, retrieved October 1998

33 "Australian jailed for spreading Nazi propaganda," *The Age*, November 11, 1999

34 "$5,000 wins early release for Holocaust sceptic," *Sydney Morning Herald*, November 13, 1999

35 "No Repentance from the Revisionist," *Sydney Morning Herald*, November 13, 1999

36 For assistance in preparing this section, ADL would like to acknowledge Dr. Karen Mock, National Director of the League for Human Rights of B'nai Brith Canada.

37 "Hate on the Internet," by Karen R. Mock and Lisa Armony, *Speaking About Rights*, Vol. XIII No. 2, 1998

38 Letter from David Matas, B'nai Brith Canada, to Michael Belec, Senior Counsel, BC Telecom, March 23, 1998

39 "Report on the Commission Communication on illegal and harmful content on the Internet," Committee on Civil Liberties and Internal Affairs, March 20, 1997, from the European Parliament Web site, retrieved January 1998

40 "Illegal and harmful content on the Internet, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions," form the Information Market Europe Web site, retrieved January 1999.

41 "Report of the Expert Seminar on the Role of the Internet in the Light of the Provisions of the International Convention on the Elimination of All Forms of Racial Discrimination," from the United Nations High Commissioner for Human Rights Web site, retrieved January 1999

42 Id.

43 International Convention for the Elimination of All Forms of Racial Discrimination, "Status of Ratifications," from the United Nations High Commissioner for Human Rights Web site, retrieved January 1999

44 "Report of the Expert Seminar on the Role of the Internet in the Light of the Provisions of the International Convention on the Elimination of All Forms of Racial Discrimination," from the United Nations High Commissioner for Human Rights Web site, retrieved January 1999