TITLE: A Draft of a Legal Policy Paper on how to Deal with the Dissemination of Racist and Holocaust-Denial Information via Electronic Media, particularly the Internet.

http://shamash.nysernet.org/~ajhyman/hate-law/legalp

(version 1.00 March 1995)

ABSTRACT:

Recent news reports have related suggestions that Ernst Zundel and other individuals who question the authenticity of the Holocaust are attempting to gain direct access to the Internet, a global network of computer networks connecting as many as 30 million individuals.[1] Zundel, in particular, has a reputation for allegedly being the world's largest print publisher of Holocaust denial material. This paper will serve to evaluate the legal issues pertaining to the use of the Internet as a medium of communication for Holocaust deniers, in light of the recent reports. Although Zundel's base of operation is Canada, the reports have stated that his access point will be in the United States. The primary legal focus of this paper will thus be American. A follow-up revised study will include Canadian legal issues, including those surrounding international transmission. Finally, the generalist issues discussed herein will have import to those interested in the broader issues of racism and other -isms on the 'net'.

AUTHOR & USAGE:

Avi-Jacob Hyman conducts seminars on the Internet and related computer-mediated communication issues at the Ontario Institute for Studies in Education. He also serves as managing editor of the electronic publication, _Jewish Studies Judaica eJournal_, co-published by the Shamash Project of the New York State Educational Research Network and the H-Net Group at the University of Illinois - Chicago. He is a former managing editor of Canada's largest Anglo-Jewish monthly newspaper. Please send all commentary to the author via e-mail: ajhyman@oise.on.ca

TABLE of CONTENTS:

(1) THE MEDIUM DEFINED:

The Internet is a conglomerate of computer service providers that includes educational institutions, government agencies, private corporations, computer clubs and bulletin boards, and specialty providers, such as CompuServe and an array of public-access organizations (freenets).

Each provider makes available a selected range of software for individuals to use over the Internet. There is no uniformity in which software packages are made available by each provider, but the single most common package would be some form of electronic mail. Various estimates put the number of people with e-mail access at between 10 and 35 million world-wide. In order to better grapple with the legal issues, an initial understanding of Internet software is required within a more generalized perspective.[2] Essentially, Internet software can be broken down into three types:

- Primary Publishing Tools; - Secondary Publishing Tools; - Interactive Communication Tools.

These categories have been specifically chosen because they relate directly to how an individual might make use of the network to spread their message of hate and denial. (a) Primary Publishing Tools: These tools include any software that makes use of electronic mail and individual archiving, whether they are used to distribute information to another individual or to a group of individuals. Within this category are the popular 'listserv'-like discussion group and newsletter software packages; USENET news facilities; localized computer forums; and private World Wide Web home page enablers. The underlying principle behind all of these tools is that they allow an individual entity (which may include more than one person) to create and/or distribute information directly and often without the express knowledge of a system administrator vis-a-vis content. (In other media, a primary publisher might include both the author and publishing company; newspapers; and broadcasters).

(b) Secondary Publishing Tools: As defined within the law, a secondary publisher would be an 'agency' that serves to house and/or redistribute material produced by some other 'agency' (the primary publisher). In other media, booksellers and libraries often fall into the category of secondary publishers, where explicit knowledge of content is not required. From an Internet perspective, centrally controlled software (i.e., controlled by a system operator) such as gopher or World Web archivers, could be considered secondary publishing tools, and make the system administrator who controls them the secondary publisher.

(c) Interactive Communication Tools: This category of tool, which often allows for real-time communication either between individuals or among large groups, can include CHAT, IRC, TALK, MUDs (multi-user dimensions) and so on. These type of tools are most analogous to the telephone system (and its 'party lines'), or to an open space or forum.

(2) SUMMARY of LEGAL ISSUES:

This section will outline six issues in law that will ultimately impact on the dissemination of Holocaust denial material via the Internet. They are: Non-government infringement; Public Forums; Conduct vs. Speech; Lawless Action; Fighting Words; Defamation. This synopsis owes most of its content to two excellent summary publications, one by Cavazos & Morin [3] and the other by Loundy [4]. Please access and read both.

(i) Non-governmental infringement: While every US citizen has First Amendment (FA) rights to free speech, the Constitution only provides this protection against infringement by the government. Nowhere does the Constitution provide protection from infringement by a private person, including, of course a system operator. In citing at least two cases involving the on-line service Prodigy, Cavazos and Morin establish the concept of 'editorial discretion' as a governing principle.

(Interestingly enough, one case involved a heated exchange between Jew-haters and Jews over the authenticity of the Holocaust. In conjunction with the B'nai Brith Anti-Defamation League, Prodigy eventually settled on an editorial policy of not allowing comments that were 'grossly repugnant to community standards'. However, clearly, this policy was not dictated by law).

(ii) Public Forums: Certain interpretations of the FA by some courts have included a ruling that some private places resemble public forums so much that the Constitution protects free speech there by anyone, not just the government. Some commentators have tried to include the entire Internet within that interpretation. However, to date, no court has yet ruled on that. Cavazos and Morin ask whether "CompuServe is any more a public forum than a call-in radio show?" Reference to the underlying concept of 'universal access,' implicit in defining a public forum, will be discussed in the section regarding civil liberties.

(iii) Conduct vs. Speech: Generally speaking, US courts have let governments 'restrict' speech and even punish conspirators for their speech, if the content of the speech relates to the planning or commission of a crime. Furthermore, government can generally restrict speech provided the restrictions are not based on content at all, but only on the time, place or manner of the activity.

(iv) Lawless Action (the Brandenburg Test): Surprisingly to some, speech which advocates illegal, dangerous or violent action is often protected by the FA, unless it meets the two-part Brandenburg Test for a 'clear and present danger'. For part one, the speech must be directed to inciting or producing IMMINENT lawless action, and for part two, the speech must be LIKELY to incite or produce such action. This test has been upheld for speeches at volatile rallies, for example, but one of the biggest current debates in law on the new medium deals specifically with the nature of immediacy and the Internet. An inciteful message transmitted via e-mail, might not meet the IMMINENT standards of the Brandenburg Test.

(v) Fighting Words (the Chaplinsky Test): The FA does not protect speech that will likely provoke acts of violence by the audience (even if the audience is an individual), providing it has the ability to provoke a common person of average intelligence. Although there is no specification for imminence in the Chaplinsky test, some observers have tried to tie it to the exclusion for fighting words. While this test has seldom stood up to challenge, Loundy feels, for example, that if speech provokes an audience to attempt tampering with the speaker's computer or host, it might be grounds for finding in favour of a FA exemption.

(vi) Defamation: A defamation claim (slander if committed via an interactive tool; libel if committed via a publishing tool), may be appropriate, according to Cavazos and Morin, provided 'the defamatory language is discernibly aimed at, or refers to the plaintiff with some degree of specificity - and has a tendency to harm one's reputation by attacking honesty, integrity, or sanity - in a manner that makes the identity of defamed party clear to the audience.' Defamation law is further complicated by a number of case-law exemptions, for example, defamation of a public figure in the context of that figure's job may be protected under the FA.

(3) REGARDING CIVIL LIBERTIES

No other organization better represents the cause for complete civil liberties in this new communication age than the Electronic Frontier Foundation (EFF). The EFF was founded in July of 1990 to ensure that common carriage principles are upheld in the information age, mainly by promoting the protection of what they see as Constitutional rights and the creation of a National Public Network policy. [5] The EFF's virtual library contains dozens of articles and policy papers that speak to the various issues discussed herein, and no article speaks as eloquently on EFF's position than their own response paper to the National Telecommunications and Information Administration 'Notice of Inquiry: Request for Comments on the Role of Telecommunications in Hate Crimes,' issued in 1993.[6] In their response, the EFF's staff attorney, Shari Steele writes, "_Instead of any government initiated scheme to control constitutionally-protected, even if noxious, speech in this new medium, government policy ought to promote broader access to the medium as the most appropriate response._". "_It is important that the speech that takes place over computer networks is given the same First Amendment protection as all other speech,_" added Steele. According to the EFF, "_computer bulletin board systems and networks are accessible to anyone with a computer and a modem. And if users of a BBS do not like something another user has posted, the users have available to them the same medium that delivered the noxious speech to refute it._". While perhaps admirably ideal, the EFF ideology is fundamentally flawed. Not only does it assume, from an ethical perspective, that all speech is equally valid, it also makes some very serious practical errors in its application.

Networks are NOT universally accessible to everyone. Their existence and usage is class, sex, and age-based, and any principle, such as the EFF's, which seeks to prevent action against wrongful acts in speech because of some erroneous perception that network access is universal, is classist, sexist and ageist. It costs money to have a computer and a modem, and it costs even more money to get an Internet account, clearly placing those with economic hardships at a disadvantage. Furthermore, current statistical analysis puts the ratio of men to women on the Internet at over 3 to 1, and certainly not on an equal footing.[7] And finally, and most importantly for combating Holocaust denial, older citizens of our world are far less likely to become Internet users - and they represent the key segment of our society who are still in a position to give first-hand rebuttal to the deniers. In citing the earlier mentioned Prodigy case, EFF's Steele writes, "_The discussion on Prodigy turned out to be a rather fair exchange, with both sides of the issue explaining their viewpoints, and each side being given the opportunity to

learn more about the other._". However, this was not a debate about government fiscal policy or about who has a better baseball team. The promotion of hate against any group cannot be viewed as "fair exchange of viewpoints," in a democratic society. On the other hand, Sen. James Exon's proposed bill to extend the 1934 Communications Decency Act to cover the Internet (which may very well be law by the time you read this article), is an ill-informed and sweeping blanket of law that shows how law-makers have neglected to study how the network really works. When conceived as a single type of medium, the Internet is unregulatable, and the bill will ultimately be shown to be unconstitutional if the net retains its current manifestation. However, when conceived as a series of overlapping software applications, the Internet becomes much more regulatable under current legislation, particularly when the law is applied to the message and not the medium. Of course, if the EFF should have its way - true universal access for everyone, then the laws of common carriage could be more strictly applied. In an ironic twist, so long as the Internet remains in the hands of many private operators, users are more likely to be protected from government interference. Going truly public gives the government the authority to step in and regulate the Internet.

(4) PROBABLE SCENARIOS

It is very important to understand that 'internetting' or 'surfing the net' is not one activity. When a Holocaust denier 'buys' an Internet account, s/he may gain access, through their provider, to a range of different tools that allows them to carry on different types of activity. The legal ramifications of each kind of activity are different. Loundy states this most clearly when he writes: "_ Liability for illegal activities in Cyberspace is affected by how the particular computer information service is viewed. Some services allow one entity to deliver its message to a large number of receivers. In this regard the service acts like a publisher. However, other services are more like common carriers than publishers. Networks just pass data from one computer to another - they do not gather or edit data. Still other services are more akin to broadcasting than common carriage. This similarity exists because computer services can be provided by sending data over airwaves. Computer services can also be used to allow many entities to deliver their messages simul-taneously to many other entities in a public debate-style setting. In this way, computer information systems are likened to traditional public forums, such as street corners or community bulletin boards. None of these analogies is especially useful taken individually. Each is accurate in describing some situations, but lacking in describing others. There is a tendency to look at a service and give it a label, and then regulate it based on its label. This labeling works well in some instances; but, when a service has a number of communication options, one analogy is insufficient. To regulate computer information systems properly, lawyers, judges and juries need to understand computer information systems and how they work._". Let us assume, for the moment, that a Holocaust denier achieves ('buys') full Internet access from a commercial provider who extends to that denier the full range of tools. That denier could create public e-mail discussion groups and private e-mail discussion groups; could join and contribute to someone else's discussion group; could create an electronic publication and distribute it via e-mail; could contribute to USENET from their account; could set up a personal World Wide Web homepage; could contribute material to the system's gopher and web spaces; could use their account to

access someone else's mud; could set up their own MUD on their system; could use their account to 'e-mail-bomb' or 'spam' other people's accounts; or even 'hack' into other people's accounts. Let me say, at the outset, blood-relatives of mine were murdered by the Nazi killing machine for no reason other than that they were Jewish, and it is not my intention here to give deniers a free hand in spreading their hate. I am seeking to address the issues in a practical and rational way. However, if a denier sticks strictly to denial, or to questioning the authenticity of certain facts, then there is little legal recourse for removing that denier's access. Having said that, there is little recourse a denier can have if their provider chooses to 'kick' them off their system, because, despite the best efforts of organizations like EFF to assert otherwise, the Internet is NOT a public forum, and individual providers certainly are not public institutions subject to provisions of the FA. For all the 'net' rhetoric that occurs daily about 'freedom of speech', there is no such thing via the Internet when it involves the 'editorial prerogative' of a provider.

That, of course, leaves much to the discretion of the provider, and a sympathetic provider may be hard to convince to 'kick off' the denier. However, since the Internet is primarily a hierarchical domain structure, recalcitrant providers might find themselves without a network connection should they develop a reputation of inappropriate behaviour. (There is no doubt that, in part, the origin of Acceptable Use Policies (AUPs) arose as a result of the desire of main hub providers to create responsible service sub-providers 'down the line'. For example: The Domain Administrator's Guide of the Network Information Center (NIC) of the Defense Data Network (DDN) says: "_the Domain Administrator must be aware of the behavior of the hosts in his domain, and take prompt action on reports of problems, such as protocol violations or other serious misbehavior. The administrator of a domain must be a responsible person who has the authority to either enforce these actions himself or delegate them to someone else._"[8] (in other words, even on the Internet, the buck does stop). Legal ramifications enter the picture when a denier 'crosses' the line and commits some violation of the law. When a denier advocates lawless action while using an interactive tool; if a denier emotes fighting words using any type of tool; or if a denier defames using any kind of tool - then the denier would be subject to legal action in the courts. Furthermore, if a system operator knowingly gives a denier access to any system-wide tool which is then used to commit a transgression, then the system operator is also liable.

Thus, if a denier sets up a personal home page that advocates violence against Jews and claims that there is a Jewish economic conspiracy, it would be the denier that can be charged and lose the protection of the FA. However, if a system operator constructs a listserv list for a denier, called 'How to Kill Jews,' then both the denier and the sysop could be liable. If a sysop is informed that a particular denier regularly uses their e-mail to 'spam' groups with hate literature, then the sysop would likewise be co-liable, once a warning has been issued. For example, a Canadian univeristy was the site of an 'e-mail attack' by a Jew-hater over the Internet. For many reasons, the user violated a signed agreement and lost their priveleges. While the university concluded that was enough, clearly under tort law alone, they could have taken more action if they had chosen to.

(5) CONCLUDING COMMENTS:

A few months back, a representative of the Simon Weisenthal Centre was on the radio in Toronto discussing Internet regulations. It was the representative's assertion that the Internet should be regulated in the same way as broadcast media. The rationale for regulating broadcast media was the lack of 'bandwidth' available to every user (or in lay terms, not everyone had access to a radio station). This does not apply to the Internet, even though access is NOT universal. Furthermore, the domain structure of the Internet means that the Internet is somewhat self-regulating. While the action of some providers is to cut off access by their users to certain 'newsgroups,' for example, (misdirected, since it targets the medium and not the message sender), the problem for the SWC representative was that the self-imposed regulations did not appear to be sufficient to combat Holocaust denial. Clearly then, the solution lies not in over-regulating, but in education, at the provider level. As the BB-ADL did with Prodigy's managers, so must anti-denial forces do across the Internet - i.e. - educate providers as to what are acceptable 'community standards,' regarding the Holocaust, and racism in general.[9]

Legally, then, there may not be any 'pre-preemptive' recourse to shutting down denial on the net. Legal alternatives appear to be only 'after-the-fact' recourses once a denier or racist commits a transgression of the law. That means monitoring and response, and that means that, like the deniers themselves, organizations like the ADL (or League for Human Rights in Canada), and the SWC must get fully on the net - providing easy access opportunities for Interneters to report violations of the law, as well as anti-denial material. And it means expanding such programs as the video-taping of Holocaust survivor testimony to include the development of multi-media materials for use over the Internet. One individual, Ken McVay, of British Columbia has started such a service with the assistance of many volunteers; however, the organized Jewish community must come up to speed in assisting his efforts, and working with him.

Traditional approaches and attitudes do not apply here. The SWC approach, for example, was misdirected, since it assumed an analogy to broadcast media. This is wrong. The closest analogy that applies is the regular post system. Anyone who chooses to, can walk up to a post box, spend the money, and mail a letter. We do not seek to prohibit people from buying stamps, or from even mailing letters, but should that letter contain something illegal, the full weight of society's laws come to bear on that person - and, generally, not on the postal system. Finally, to the issue of 'cross-border' transmission and the international flavor of the Internet. Every post, every file starts somewhere. Legal prosecution should be handled in the jurisdiction where a racist has the account, and should be treated as a 'foreigner' if that person is making a cross-border connection to access that account. FA protection should apply to US citizens only.

(6) REFERENCES: ----------

[1] There is a great debate regarding the actual number of people using the Internet, which is beyond the scope of this paper. For a place to start, please refer to the Internet Society.

[2] For further, more detailed reading regarding Internet software tools, try Jim Carroll and Rick Broadhead's _Canadian Internet Handbook_ (Scarborough: Prentice Hall, 1995) (Actually, for American readers, if you can get your hands on a copy of this book, I recommend it highly).

[3] Cavazos, Edward, and Morin, Gavino. _Cyberspace and the Law: Your Rights and Duties in the On-line World_. (Cambridge: The MIT Press) 1994. - Edward Cavazos (polekat@well.sf.ca.us); Gavino Morin (gmorin@bga.com)

[4] Loundy, David. _E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability_ in Albany Law Journal of Science and Technology 3(1). Revised version accessed from the archives of the Electronic Frontier Foundation (eff.org). -David Loundy (david@home.interaccess.com)

[5] The complete EFF story can be accessed from their gopher, eff.org.

[6] The National Telecommunications and Information Administration 'Notice of Inquiry: Request for Comments on the Role of Telecommunications in Hate Crimes (Docket No. 930349-3049)' and the EFF response can be retrieved from the EFF gopher.

[7] See note 1 regarding Internet usage information. While the focus of this article is not on gender, clearly, the disproportionate use of the Internet by men is indicative of a larger societal problem in providing educational opportunities to women.

[8] Stahl, M. _NIC Domain Administrators Guide_, (Network Working Group, SRI International, 1987). Located as file RFC 1032 in the InterNIC gopher at host rs2.internic.net

[9] The Buffalo Freenet's AUP, for example reads, in part, '_In exchange for the use of the Buffalo Free-Net Community Computer System, I understand and agree to the following: (1) That the use of the Free-Net is a privilege which may be revoked by the administration of the system for abusive conduct. Such conduct would include, but not be limited to the placing of unlawful information on the system and the use of obscene, abusive, or otherwise objectionable language in either public or, upon registration of complaint, private messages. The staff of the Buffalo Free-Net will be the sole arbiter of what constitutes obscene, abusive, or objectionable language. _' (source: gopher host: kilburn.keene.edu)