Internetiquette: Fact or Fiction?

George B. Trubow (*)

The media is buzzing with discussions of ethics and propriety on the Internet. On a daily basis one may find an item somewhere discussing instances of Internet communications that may constitute sexual harassment, pornography, hate mail, vulgarity, obscenity, profanity, threats, torts such as defamation and the invasion of privacy, crime schemes, infringements of intellectual property, rudeness, or bad taste. Examples of such messages motivate state and federal legislators in the U.S. to propose measures proscribing categories of speech on the Internet and defining new contexts for electronic crime. Indeed, as this article is being written, Congress is hurrying to pass a bill that will criminalize the sending of "indecent" messages to minors. Various groups, professional and otherwise, discuss the establishment of standards for network communications while others protest against any regulation of the Internet so that it remains subject only to "self-regulation" by its users.

Those who urge standards and protocols maintain that "self- regulation" won't work because the tolerant will be victimized by the intolerant and the "bad" will drive the "good" off the national and international information highways. This is denied by those who say that the First Amendment requires electronic speech to be free of regulation and that Internet "community" standards are developing a workable "netiquette" of propriety. I will here discuss some pros and cons of internet regulation, the application of Constitutional and common law to the environment of electronic digital technology, and some premises for a framework for network regulation.

In spite of the First Amendment's prohibition of the government regulation of speech, we all have heard the oft-quoted admonition that one can't yell "fire" in a crowded theater. I don't think users should be allowed to yell "fire" on the Internet, either, because I believe that the Internet -- a global information network -- will not achieve its vaunted potential unless it is a truly "user friendly" environment. Individuals should be able to enter cyberspace reasonably free from harassment or abuse and with confidence that the integrity of their communication will be respected and adequately protected.

Of course, when one goes out into the world there are risks of being offended, exploited or victimized. Society reacts to its environment with varying levels of tolerance or control; if crime appears to be rampant then freedoms become restricted as society responds with defensive measures to control antisocial behavior. We witness that phenomenon regarding cyberspace today in the form of the legislative proposals mentioned earlier. Surely, cyberspace cannot be an Eden absolutely free of offensiveness; neither should it be a sanctuary for those who would prey on others. "Rules of the road" are necessary whether the highway is an Interstate or on the Internet.

Indeed, even those who argue against government regulation of the Internet generally agree that some speech is inappropriate and should be banned, the best example being commercial advertising. Probably the best-known incident involved the law firm of Canter and Siegel (C&S) which posted widely on Usenet newsgroups

advertisements for their services in connection with entering the U.S. greencard lottery. Commercial ads, looked upon as "junk e- mail," are frequently prohibited by "netiquette" from being posted to newsgroups or "chat rooms." The C&S postings were sent to newsgroups irrelevant to immigration matters and the ads were sent to literally thousands of forums and displayed repeatedly, conduct especially abhorred by Internet enthusiasts. As a result, "self- help" measures were employed by system users to "bomb" the C&S account -- send them a torrent of complaint messages that overloaded the C&S service-provider and led to the termination of the C&S account, which nevertheless was then established with another provider.

The point here is that "self-regulation" is considered by the Internet "freedom writers" to be o.k. For instance, an Internet Advertisers Blacklist has been established on which is posted the names and addresses of those who are considered by the list operator to have advertised improperly. Users are invited to punish the violator in a variety of ways, from product/service boycotts to deluging the offender with all sorts of creative communications. The operator of the Blacklist says:

"the Internet is probably as close to an anarchy as we can get. This is good. Therefore, punishing of unwelcome behavior should be done by private individuals, following the same grass roots philosophy that governs the rest of the net."

Though self-help may be an appropriate remedy in limited instances, it is doubtful that rule by "vigilante justice" in cyberspace will be better than it is in any other place. In examining the colorful vocabulary in connection with prohibited behavior and self-help procedures we find such words as "spamming, velveeta and jello," which do not refer to those products, and others such as cancelbot, cancelmoose, flaming, bombs, traps, killfiles, and more. Obviously, there is enough objectionable on the Internet to warrant a special vocabulary for wrongs and remedies. Regarding the latter, the words are suggestive of electronic warfare, which, in microcosm, may be what takes place with some frequency in cyberspace. That doesn't sound like a friendly environment. Internet self-help has other problems.

In a scheme of "punishment by private individuals," who defines what is "unwelcome behavior" on the global "information superhighways," and by what process? Who governs the administration of penalties? When and how has the offender been sufficiently punished? I reject romantic notions of retribution at the "O.K. Corral" as out of place in today's "electronic frontier." Clearly, I'm skeptical about the reality or the reliability of "Internetiquette" and favor some regulation so that cyberspace and the Internet can be a comfortable environment for business and commerce, government communications, education, sharing information and just plain socializing. I suggest the following notions as being basic to a "user friendly" cyberspace.

1. Rules of the road must be established at a national level and coordinated internationally. Alleged violations of law by messages initiated in one state and downloaded in another demonstrate the need to develop a rational scheme of rules and jurisdiction. The prosecution for pornography in Tennessee of the Thomases, EBB operators in California, illustrates a problem in trying to apply "community standards" in borderless cyberspace. The recent litigation involving the Church of Scientology, wherein U.S. copyrights were allegedly infringed in the U.S. with the help of an Internet re-mailer in Finland, emphasizes the international scope of cyberspace regulation. Governments must make these rules and monitor their application because global cyberspace cannot be workable merely as a collection of private domains privately ruled.

2. Anonymous non-traceable communications must not be allowed on the Internet. Whether one argues for "self-regulation" or for rules established by government, neither regime can be implemented if transgressors

are immune from sanction and they will be if they cannot be identified. In the U.S., the current state of the law suggests that anonymity might be protected, however.

The question of anonymity in communications has been before the U.S. Supreme Court a number of times, most recently with respect to anonymous political leaflets. In McIntyre v. Ohio Elections Commission, 1995 WL 227810 (U.S.S.Ct.), the Ohio Supreme Court had upheld as constitutional a state statute which, for the purpose of identifying those who distributed misleading or libelous material, prohibited the distribution of anonymous literature designed to influence the voters in an election.

The U.S. Supreme Court reversed, thus invalidating the statutory provision that campaign literature must contain the name and address of the person or campaign official issuing the material. Holding that First Amendment speech was involved, the Court said that Ohio had not met the heavy burden required for imposing limits on protected speech. The case dealt with leaflets that were distributed at a public meeting and, though not dealing with the vastly different forum of the Internet, nevertheless will have implications regarding anonymity in cyberspace.

The McIntyre case was decided soon after the Supreme Court of California upheld its own state statute requiring political candidates and their election committees to identify themselves in mass mailings sent to prospective voters. In Griset v. Fair Political Practices Commission, 35 Cal.Rptr.2d 659 (Cal. 1994), the court held that the purpose of the statute -- to inform the electorate and prevent corruption of the political process -- was compelling and because it did not regulate the content or quantity of speech the First Amendment was not violated. It would appear that McIntyre is contrary to Griset though the latter resonates with me.

In any event, both cases are "technology neutral" and seemingly would apply to communications in any medium. As to the Internet, there is no way to automatically distinguish between messages entitled to First Amendment protection and those that are not. Accordingly, if anonymity is allowed for political speech on the Internet then presumably any communication could be anonymous unless monitoring of all communications was undertaken to distinguish message content -- probably an insurmountable burden.

It is important to distinguish between anonymity and traceability regarding Internet traffic. Messages travel the Internet with headings that identify their source, even though the sender may be using a "screen name" alias. Though a message might be anonymous to the recipient, the system operator at the source of the message could probably identify the author. An e-mail remailer, however, could agree to be a go-between, stripping identifiers and forwarding a message so that the sender remains anonymous -- and untraceable, if the re-mailer agrees to keep the secret.

It is possible to achieve both anonymity and accountability. Though messages might be sent anonymously through re-mailers, they could be required to divulge the source of any message when an injured party can show cause. Surely, none would argue that the identity of one who commits intentional criminal acts on the Internet should be shielded. Likewise, there is no reason to protect one who intentionally commits torts, violates intellectual property rights, steals money or breaches other legal duties through use of electronic communications.

To reach a fair balance between anonymity and accountability, however, will take regulatory authority and schemes not currently available on the Internet; that's a big item on the planning agenda for the further development of a national and global information highway. Regarding the impact of McIntyre in that respect, three limiting factors are worthy of note: (1) the case specifically involved election leaflets, (2) the distinction

between anonymity and traceability was not considered, and (3) Justice Ginsburg noted, in her concurring opinion, that "We do not...hold that the State may not in other, larger circumstances, require the speaker to disclose its interest by disclosing its identity."

3. New legal constructs must be developed to deal with the digital electronic environment. Platitudes such as "pouring old wine into new bottles" or "building bridges" will never adequately address the legal and policy questions presented by the new information and communications technology. There is little likelihood that anyone can overstate or adequately predict the total impact that the new technologies will have on individuals, society and governments. The principles of the common law system, shaped in past centuries to deal with past problems, cannot resolve the issues of rights, duties and due process that confront us today in cyberspace. What worked in 1066 (remember, the Battle of Hastings is the final victory of the Norman Conquest as well as the starting point of our "modern" common law) should not dictate our rules in 1996; no legal system can bridge that gap. A few examples can illustrate some of the difficulties:

How should the First Amendment be applied in cyberspace? Past regulation of electronic media (i.e., radio and television) was based on the scarcity of frequencies to distribute those resources, whereas the "print" press was unregulated because anyone could print a paper and communicate with the polity. Today, newspapers are disappearing while the electronic media expands its scope well beyond any dimension that could have been predicted in 1976, let alone 1776. "Scarcity" is not a rationale for First Amendment theory in today's multi-media environment; acknowledging the reality of abundance and the resulting need to classify and sort the overload of available information might save us from drowning in data.

What are the duties and legal liabilities of the network service providers? An example of the conundrum is the recent New York state court case suggesting that Prodigy could be liable for the transgressions of its clients because it tried to enhance the quality of its system by monitoring and screening communications. Though that case was settled before trial and thus sets no precedent, nevertheless it illustrates the "wrongheadedness" of the common law applied in cyberspace. That lower court decisions can be defended on the basis of the common law analysis of who is a "publisher," but that misses the point. Instead of imposing liability of a provider who tries to help, liability ought to be assessed on those who do nothing to "self-regulate" while some immunity should be afforded to those who do.

What happens to intellectual property (patent, copyright) protection in cyberspace? The "freedom writers" often argue that it should disappear (literally, "free" speech); those who spend time and energy to create new tools and techniques want some return for their investment. The rules for statutory protection of "hardcopyright" falter markedly in the digital environment. We need NEW law here, not old bottles.

How will individuals guard their interests with respect to the circulation of personal information about them in the realm of cyberspace? Historically, the question of control of "personal information" was determined on the basis of "ownership." In common law terms, whomever owned the medium upon which information was recorded was regarded as the "owner" of that information, a rule that worked reasonably well with "hard copy." That just doesn't make any sense in today's electronic digital world. Instead, a duty of care in the use of information pertaining to a specific individual makes sense. However one has managed to collect information, s/he ought not be permitted to harm someone through its use -- whether one prepares a dossier from "public" data bases or from the careful examination and sifting of an individual's private transactions.

4. Encryption can provide a means for making cyberspace "user friendly." With respect to pornography, for instance, adult-only EBBs that clearly announce their content and require careful screening, pre-registration

and encryption of messages could assure that only informed adults can visit protected sites. Likewise with respect to "chat rooms" that tolerate vulgarity and insult in their communications; verbal "mud-wrestling" in cyberspace could be available to those who choose it. Here, of course, security in communications is essential and the technology can provide reasonable levels of protection. No system is fool-proof forever, but perfection is not practicality and the perfect ought not be made the enemy of the best.

5. The same rules ought not apply to every mode of communication. What's o.k. for land mail may not work for e-mail. It often seems to be the case that the "freedom writers" think that e-mail communications must meet every need and solve every problem. That's partially a result of "building bridges;" lawyers like to analogize a principle regarding a letter in a paper envelope to an electronic message. Land mail, telephones, telegraph, and other communication devices are not going to cease simply because of electronic information networks. Just as we had different rules, in the old days, for print and electronic media, we must have different regimes today. If we try to put all the eggs into one basket, we may end up with a basket of broken eggs.

Cybernews Volume 2, numéro 1 (printemps 1996)

(*) George B. Trubow, Professor of Law Director, Center for Informatics Law The John Marshall Law School 315 S. Plymouth Ct. Chicago, IL 60604-3907
Fax: 312-427-8307; Voice: 312-987-1445
7trubow@jmls.edu

 ISSN 1201-7302
