Policy Analysis

Cato Institute Policy Analysis No. 262: Beyond the Communications Decency Act: Constitutional Lessons of the Internet

November 4, 1996

Solveig Bernstein

Solveig Bernstein is assistant director of telecommunications and technology studies at the Cato Institute.

Executive Summary

On February 8, 1996, the Communications Decency Act was enacted into law. The law criminalizes the use of any computer network to display "indecent" material, unless the content provider uses an "effective" method to restrict access to that material to anyone under the age of 18. But there is no affordable, effective way for nonprofit or low-profit speakers to restrict children's access to such a broad, ill-defined category of material. Thus, the statute effectively bans much speech from the Internet and other networks. The Internet promised the ordinary citizen a low-cost method of reaching an audience beyond immediate family, friends, and neighbors. Legislation like the CDA betrays that hope and is clearly unconstitutional.

No regulation of computer network indecency, however carefully tailored, should pass constitutional scrutiny. First, no legislator has been able to define indecency coherently. Such regulation is inherently unfair, especially as applied to spontaneous, casual speech of the sort that the Internet facilitates between unsophisticated and noncommercial speakers. Second, government cannot legitimately claim that it has any interest in content control, when civil society has solved the perceived problem on its own. Here, private sector solutions include both software filters that parents can use to screen out offensive material and Internet service providers who provide access only to child-safe materials.

Introduction

In speaking of the value of the First Amendment, Supreme Court Justice Louis Brandeis wrote, "The greatest dangers to liberty lurk in the insidious encroachment by men of zeal, well-meaning but without understanding." [1] Now those individuals have blundered into cyberspace. Just as pundits were touting the promise of the information superhighway, the federal government moved to censor it. The advent of federal censorship was deeply mourned by the computer network community. Thousands of people joined in a campaign to protest the new law by blacking out their World Wide Web pages or posting blue ribbons on their Web sites.

Computer network content had, until now, been relatively free of federal censorship. Computer network media such as bulletin boards and the Internet gave many ordinary people their first taste of true freedom of speech--as speakers, not merely as listeners. Having eaten of the forbidden fruit, those who actually use those media realized the loss that censorship would bring.

The voice of the Internet came too late to influence developments in the legislative branch. In June 1995, the Senate voted in favor of an amendment to the Telecommunications Act of 1996 sponsored by Sen. James Exon (D-Neb.). [2] The Exon amendment, which had been added to the Act without hearings and with little discussion among committee

members, would have made it illegal to make any indecent material available on computer networks. [3] The House proffered its own amendment, sponsored by Reps. Christopher Cox (R-Calif.) and Ron Wyden (D-Ore.), to address the issue. That amendment would have encouraged private solutions to the problem of indecency, without restricting free speech.

Rep. Rick White (R-Wash.) tried to craft a compromise between the House and Senate proposals, offering a bill that restricted speech considered "harmful to minors" on computer networks. Under the bill, sexual imagery on private computer networks would be governed by a standard like that usually used for public display of print media. House conferees, however, again with little discussion, substituted broader language regulating "indecent" material. [4] That language ultimately became part of the Communications Decency Act, which was enacted into law along with the Telecommunications Act of 1996.

As enacted, the CDA contains vague, sweeping provisions that prohibit using interactive computer networks knowingly to send or display indecent material to anyone under 18. The ambiguous reach of the law is simultaneously ridiculous and frightening. It is vitally important that Americans understand why.

Computer communications networks, including the linked network of networks that constitutes the Internet, are nothing more than powerful engines of speech. They empower anyone, anywhere, to create any kind of content and to distribute it to anyone, anywhere, who seeks it out. For the ordinary person--the casual artist, the amateur poet, the concerned citizen--computer networks may represent the only low-cost way of immediately reaching an audience beyond friends, relatives, and neighbors. Finally, the ordinary citizen will be not just a listener. He or she can be a speaker as well.

This extraordinary development in the "marketplace of ideas" is directly linked to the low cost to the speaker, in effort and in money, of reaching an audience by computer networks. Anything that adds to the cost directly threatens this embryonic revolution in public discourse. The CDA threatens to add so much to the cost of casual speech over computer networks that it in effect bans much of that speech. The CDA will have a broad, real, observable destructive effect on speech over computer networks, particularly speech by amateur, casual, and not-for-profit speakers.

Recognizing that fact, on June 11, 1996, a panel convened in Philadelphia, consisting of Chief Judge Dolores Sloviter and Judges Ronald Buckwalter and Stewart Dalzell, enjoined the enforcement of the CDA, finding the statute to be unconstitutional on its face. [5] On June 13, 1996, a panel convened in New York, consisting of Chief Judge Jose Cabranes and Judges Leonard Sand and Denise Cote, entered a similar injunction. [6] The matter does not end there, however. The Department of Justice has appealed both decisions to the Supreme Court. Furthermore, legislators may respond to the ruling by enacting new, somewhat different censorship laws, hoping that they will be upheld.

This study will show that government regulation of computer network indecency simply does not make sense, either as a constitutional matter or as a practical one. Government has no legitimate interest in controlling content that users can control themselves.

The question of whether government ought to regulate a narrower category of sexually explicit content identified as obscene is not dealt with here. Regulation of child pornography also raises substantially different issues.

The Amateur Speaker and Computer Network Speech

Even those who have never ventured onto the Internet or other computer networks are probably vaguely aware that those networks have become the repository of vast stores of information. Traditional institutional distributors of speech such as libraries, bookstores, newspapers, and magazines have already begun to move their wares on line. Non-text-based media, such as music stores or movie theaters, are expected to follow. [7] Perhaps most important, computer networks, particularly the Internet, offer the casual, noninstitutional user a unique new opportunity to reach a wide audience for his or her speech; [8] the effect of censorship on such casual speakers and their audiences is the focus of this paper.

The New Speakers

Perhaps the most popular computer speech service is electronic mail (e-mail). This is the equivalent of paper mail in the nonelectronic world, but faster. Unlike paper mail, personalized e-mail communications between persons who have never met one another in "real" space are common.

Discussion groups such as mailing lists have also become important forums for speech by ordinary persons. The two most widely used types of mailing list are the "listserv" and "Majordomo." Users can subscribe to a "listserv" devoted to a discussion of a particular topic; any message posted to the listserv is distributed to other users. Most listservs are not moderated; messages are posted without being reviewed by a human being. Majordomo lists are similar.

Many of the approximately 17,000 (as of the beginning of 1996) newsgroups [9] are unmoderated forums known as "usenet" newsgroups. A substantial subset of these are "alt" (alternative) newsgroups, which tend to be devoted to relatively eccentric, freewheeling discussions. For example, of the Massachusetts Institute of Technology's approximately 9,812 newsgroups, 4,581 are "alt" groups. [10] To set up such a newsgroup, one sends a message to the newsgroup "alt.config." The message is distributed over the thousands of individual administrators of the network of networks that makes up the Internet. [11] Each individual administrator decides whether to instruct its computers to carry the newsgroup. Interested users then can access the newsgroup data at any time. The "alternatives" and all other newsgroups lack any kind of centralized distribution point or administration. The content of messages posted to newsgroups is thus inherently and necessarily difficult to control. [12]

Moderated newsgroups do exist. These are not frequently established by most casual users, as they require access to an independent news server and a lot of spare time to moderate. However, many moderated newsgroups are operated by hobbyists--that is, noninstitutional amateurs as opposed to large commercial or educational institutions.

User forums that do not primarily rely on the Internet as a distribution mechanism include bulletin boards and those provided by commercial online networks such as America Online. A bulletin board is a conference and message exchange system usually devoted to a particular topic and operated from a personal computer with one or more modems connected to it. Users access the service by dialing up on their own modems. There are roughly 50,000 to 70,000 bulletin board services in existence, most based in the United States. [13] Compulink Information Exchange, a United Kingdom bulletin board service, hosts more than 2,600 online conferences addressing topics from architecture to politics. One CIX participant explains, "Each conference is a bit like a club where you can stay in quick and constant touch with a community sharing a particular interest. You can belong to and participate in far more of these virtual clubs than you can in the real world." [14]

Although some bulletin board services restrict access only to certain categories of users, most services do not and cannot screen each individual posted message. The number of messages posted is simply too great. Online services generally control subscriber-contributed content by contract, stipulating in their service contracts with subscribers that some types of speech are not allowed. They also do not, however, screen individual posted messages. Some use software filters that automatically prohibit speech using certain keywords.

Ordinary users may also distribute speech via the Internet by setting up "home pages" on the World Wide Web. They need not purchase their own server and maintain 24-hour-a-day connections over their own phone lines. They can contract with a commercial service to provide them. America Online and CompuServe provide space for home pages and home page software free to members. Other Internet service providers offer noncommercial users Internet access, space for a home page, and Web browser and e-mail software for $20 to $50 per month; software to create Web pages is generally available for less than $150. [15] Prices in this market are falling fast. Space on university servers is often available free to students.

The most spontaneous form of computer network speech is the chat room, an electronic forum set up to admit a limited number of speakers. Chat rooms may be restricted to a suggested topic or open to any topic. Chats take place in real time and are spontaneous, like a face-to-face chat around a backyard barbecue. Lasting relationships form in chat rooms between "cyberfriends" who have never seen or met each other.

For the ordinary person computer networks are not just a source of information. They are a source of listeners and readers and viewers. They transform the ordinary person into a speaker capable of reaching an audience of millions. Computer networks are nothing less than a vast engine of free speech with the potential to transform the entire "marketplace of ideas."

The New Audience

It is tempting to view the significance of computer networks in the marketplace of ideas only through the lens of analogy. One could say that computer networks have the power to transform the ordinary person into a publisher, a broadcaster, a newspaper editor. When this seems not to capture the full impact of these networks on speakers and speech, one tries to improve upon the imagery by adding that the networks are also like a post office and fax machine and telephone and printing press rolled into one. That comes closer. But that analogy, too, fails to express the extent to which the networks empower audiences as well as speakers.

A speaker who uses computer networks as a soapbox will reach a large number of people. But only the user who employs an Internet search tool actively to seek out the information the speaker provides will receive it; these tools include the directories used with "File Transfer Protocol" (FTP), "Gopher" software, or Web browsers such as Netscape Navigator. [16] So whomever the speaker reaches will usually be a member of a self-selected audience with some interest in the topic. The computer network user can determine what information he will receive by choosing one access service over another. He or she cannot go to any location on the World Wide Web except by affirmatively asking to be taken there. If the user wants, he or she can buy software that will block his or her own or children's access to a wide range of objectionable information. If the user receives an unidentified file attached to an e-mail that might contain a computer virus or something that might prove offensive, he need not download it.

In some ways, this is not new. Someone wandering about the city streets can pick and choose which stores to enter. But the Internet allows the wandering to go thousands of miles further afield. The broadcast audience has always been free to change the channel, turn off the television or, for that matter, get rid of it altogether. On computer networks, as we describe further below, the information filters can be more subtle.

An Age-Old Subject

Because computer networks such as the Internet are decentralized and user-controlled, people can use them to discuss almost any subject that interests them, from antique tools to zoology. People, it seems, also are interested in sex.

As a result, sexually explicit material is available on the Internet, through online services, and on bulletin boards. Some of the material would be considered obscene or to be child pornography; state laws prohibiting distribution or possession of such material already apply to these materials. [17] A greater proportion of the sexually explicit material posted on computer networks is softer stuff. A lot of it (there is no way to measure how much) is posted or traded by amateurs, not by commercial pornographers. Access to most commercial pornographers' material (except for a few "teasers" floated for advertising purposes) has always been restricted because they want payment from their audience; they demand credit card numbers or passwords.

Sexually explicit materials are available on computer networks because people want them to be. Whatever people might say in public, people's private choices show that they are fascinated by sex and enjoy sexually graphic materials. Sometimes we like this taste presented in an exalted artistic or literary form--sometimes not. This fact is aptly illustrated by the link between the spread of VCRs and the growth of the adult video market. In 1979, less than 1 percent of Americans owned a VCR. [18] Recorded tapes were as much as $80; while no one would pay for commonplace fare available on broadcast, people would pay for adult titles. During the early years, pornography made up over half of the recorded tape sales. [19] As the use of VCRs spread from 1987 to 1993, the adult video market grew 90 percent. [20] From 1991 to 1993, the sales and rental volume of adult tapes grew from $1.2 billion to $2.1 billion, an increase of almost 100 percent. [21] It is estimated that the growth has been slowed by prosecution of video store distribution outlets. In Sweden, where there are no such restrictions, 25 percent of video rentals are adult titles. [22]

Likewise, in Italy, 50 percent of video sales are adult titles. One wonders whether VCR technology would have developed so fast and become so affordable if not for the initial spur of the pornography market.

Would-be censors of the Internet and other computer networks therefore face a problem: it is hard to generate sympathy for their cause when in fact it runs counter to what many people privately prefer. *The common rhetorical response has therefore been to lump all sexually explicit material available on computer networks together with child pornography and depictions of torture*. [23] Defenders of the CDA try to conceal the breadth of the law. One defender reassures the public that "indecency laws require the courts to evaluate material in its context, taking into account things like literary value." [24] This is true of laws that regulate obscenity in the print media; it is notably not true of indecency regulations that govern broadcasting, the model for the CDA.

The media have proven susceptible to these rhetorical tactics; the CDA is often described as a law that targets "smut," or "porn," in spite of the fact that its sweep is far broader. As described below, the law also might be applied to discussions of sex or the use of vulgar language that is not intended to be arousing.

Still other distortions have affected the public debate. Some defenders of net censorship, *including the Department of Justice*, still cite Marty Rimm's study of computer network pornography, [25] which is widely believed to be a fraud. [26]

This raises a puzzling point. If the public's real concern is very disturbing material such as child pornography, why did lawmakers not try to craft a law that more narrowly targets this type of material? First, such a law would have been unnecessary; state laws already prohibit this type of material as well as obscenity. Second, lawmakers were influenced strongly by groups that ultimately would prefer to prohibit the distribution of *all* sexually explicit material, to adults or to minors, regardless of whether it is obscene. A representative of one such group stated that "computer pornography should be eradicated, not controlled." [27] The newsletter for the Family Research Council, which has been active in supporting censorship legislation, in one paragraph anticipates the triumph of the forces defending the CDA at the trial in Philadelphia, and in the next goes on to praise a bill that would prohibit the sale of pornography at military facilities. [28] There is a gulf between the goals of those groups and most people's understanding of what government may legitimately do.

The Communications Decency Act

The CDA covers "whoever" knowingly uses an interactive computer service to "send to a specific person or persons under 18" or "display in a manner available to a person under 18" any "comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." [29] The following section explores the meaning of these provisions further, and also delineates defenses most relevant to the casual user.

"Knowing" Violations Interpreted Broadly

One can be convicted under the CDA only of a "knowing" violation of its terms. The question becomes, when does one "know" that one has sent or displayed material to someone under 18? Obviously if one sent material that had been ruled "indecent" (say, George Carlin's "Seven Dirty Words" monologue) over a computer network to one's own child, one would know that one had violated the law.

But suppose one sent material that no agency or court had ever declared was indecent to a stranger who told you that he or she was over 18? One could still be convicted under the law, because courts interpret "know" broadly; one would be convicted because one knew that the stranger might have been lying, and that the material might be ruled indecent. Likewise, one could be convicted for a knowing violation if one merely posted material to a newsgroup or a Web site, knowing that it was possible for children to access the site.

Send or Display Includes All Communications

Plainly, the law's "send *or display*" (emphasis added) language applies to any computer network communication-- e-

mail, an utterance in a chat room, a posting on a home page or a bulletin board, or a newsgroup message. And it applies to any speaker. Commercial pornographers using the Internet as a distribution service are, obviously, covered. So is a casual user sending an e-mail message, posting a message to a bulletin board, typing a statement in a chat room, or creating a home page for the World Wide Web. That much is obvious. [30]

A vast range of communications and communicators are potentially swept within the law's reach. To return to (admittedly inadequate) analogies, it is as if the law regulates phone conversations, faxes, television broadcasts, readings of poetry in coffee houses, private letters, newspaper articles, and works of literature and art, all in one fell swoop.

What Is "Patently Offensive"?

The legislative history explains that the definition of indecent material as "patently offensive" is meant to be the same standard that is applied to radio and television broadcasters. [31] So perhaps we can look to the cases and Federal Communications Commission decisions regulating indecency on the airwaves to find out what the new law means. What we learn is more alarming than helpful: works of considerable literary, scientific, and artistic merit might be "patently offensive." In some contexts, ordinary cuss words might be considered indecent.

Indecency at the FCC. At least three judges of the District of Columbia Circuit Court of Appeals believe that under the Federal Communications Commission's indecency standard, "affected speech could include programs on the AIDS epidemic, abortion, childbirth, or practically any aspect of human sexuality." [32] It is next to impossible to capture the gist of the FCC's rulings without recounting each indecency adjudication in detail. [33] The FCC has never issued general rules describing exactly which factors will result in material's being considered "patently offensive." Indeed, the FCC has admitted that it cannot, explaining that indecency cases are "highly fact-specific and are necessarily made on a case-by-case basis." [34]

In other words, something is indecent if it offends a majority of FCC Commissioners. Works that have offended the FCC include

- social satire such as George Carlin's monologue, "Seven Dirty Words," which makes fun of our attitudes toward common swear words;
- excerpts from radio broadcasts by Howard Stern, a tremendously popular radio and television host;
- the critically acclaimed play "Jerker," which consists mainly of conversation between two gay men with AIDS discussing their sexual fantasies and experiences; and
- the song "Penis Envy," a cheerful account of what a girl would do if she had a penis.

In response to critics, the FCC has protested that its indecency regime leaves speakers with ample alternative ways of expressing their ideas; it only precludes offensive forms of expression. The "Penis Envy" ruling strongly suggests that this is not true; it is difficult to imagine a song about a penis that is worded more politely. The only arguably offensive word in the song is the word "penis." Jonathan Weinberg of Wayne State University Law School finds the ruling a puzzle, and muses that "perhaps someone on the FCC enforcement staff does not like songs about penises. Perhaps songs about penises are not per se indecent, but in this case the singers used the word 'penis' too many times, and in too disrespectful a tone." [35] The most likely explanation seems to be that the FCC objected to the song's core meaning, not to the language chosen to convey that meaning.

The FCC has also *refused* to decide whether certain works would be considered indecent, including James Joyce's book *Ulysses* and the television miniseries *The Singing Detective*. [36] In both cases, the FCC's problem was that it was reluctant to declare artistic or literary merit as a defense to a charge of indecency. But censoring works whose merit was so widely recognized would have proved embarrassing for the agency.

Here, it is instructive to compare the regulation of sexual material in the print media. Some printed works are considered obscene. The Supreme Court has ruled that these may be banned altogether. But a work may be considered obscene only if, taken as a whole, it lacks serious literary, political, artistic, or scientific value. [37] A somewhat

broader category of print works may be regulated by laws that require material that might be considered "harmful to minors" from being displayed in public places. [38] Those laws generally describe the material they cover with particularity. Further, these laws apply only to material that might have "prurient appeal" to minors (that is, that might arouse minors' lust), *and* that would lack literary, artistic, or scientific merit for minors. [39] The laws rarely try to encompass private communications and in most circumstances if so applied would probably be declared unconstitutional; many apply only to commercial displays. [40]

Community Standards. The CDA defines indecency with reference to a "community standard." Which "community" does the law mean? A lot of users think of the online community as a community. Is that what the law means? Does it mean the local community where a message is downloaded? Something else?

Perhaps it means that computer networks are to be brought under a national indecency standard. The legislative history explains that the provisions of the CDA that preempt certain state laws were intended to create a "uniform national standard" of content regulation for computer networks. [41] But this comment apparently does not apply to the indecency definition.

We might think that the CDA establishes a national standard of indecency similar to or identical with the FCC's broadcasting standards. The broadcasting standard is supposed to be a national standard, referring to the tastes of the "average broadcast viewer or listener." [42] Does the legislative history's reference to the broadcast standard mean that computer network indecency will be whatever offends the average broadcast viewer, too? Or that courts are to craft an *analogous* standard, referring to the tastes of the average computer network user? This point is not clear.

By contrast, obscenity in the print media, including material deemed "harmful to minors," depends partly on the tastes of local, not national, communities.

Safe Harbors

The CDA is not a flat ban on all indecent speech. A defense is provided for those who take measures to restrict children's access to indecent material. A person who "has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number" will not be liable under the new law. [43]

The law provides another blocking option. A person who "has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology," will not be liable. [44]

The legislative history explains:

> the word "effective" is given its common meaning and does not require an absolute 100 percent restriction of access to be judged effective. Content selection standards, and other technologies that enable restriction of minors from prohibited communication, which are currently under development, might qualify as reasonable, effective and appropriate access restriction devices if they are effective at preventing minors from exposure to indecent material via the Internet. [45]

This language leaves one to wonder how much less than 100 percent effective a restriction of access may be. The common meaning of the word effective would seem to require something that would keep out most children. In fact, further discussion below will show that it is not technically or economically possible for most amateur, not-for-profit, and small-scale content providers to satisfy this requirement.

The Impact on Forums for Amateur Speakers

As we have seen, the CDA applies to any type of message that can be sent or displayed across computer networks. The

CDA potentially affects any reference to sex or excretory functions, by anyone, using any network function. It applies to casual, noninstitutional, and amateur users as well as to professional pornographers. And it applies, apparently, to an extraordinarily broad, albeit ill-defined, range of content. To see the potential impact of the law on computer network communications, one must understand the operation of the supposed "safe harbors" for indecent speech.

Perhaps the most important forums for amateur speech are newsgroups and mailing lists. Currently, there is simply no way for a speaker who posts a message to an unmoderated newsgroup or list to restrict underage viewers' access to that individual message. Nor, for that matter, is there any way for content providers to block children's access to an entire newsgroup. The CDA thus sounds the death knell for unmoderated newsgroups or lists that discuss sexual issues of any kind. Many would-be participants will keep out of the discussion, fearing that their postings might be considered indecent. Many groups will be unable to maintain the necessary critical mass of contributors.

Furthermore, the CDA penalizes the formation of moderated lists, newsgroups, and bulletin boards--conceivably, the moderator or bulletin board operator might be liable for an unexpected indecent message posted to his newsgroup or on his board. While the CDA provides a defense for those who merely provide access to indecent material, [46] that defense is not available if the access provider controls the network in question, or if the individual "knowingly advertises" the availability of a service that distributes indecent content. [47] Nor is the defense available to persons who own or control a system used to violate the indecency law, such as the servers from which bulletin boards are operated. [48]

Any time anyone sends e-mail containing sexual or excretory references to someone he or she does not know personally, that person now risks conviction under the CDA. There is no practical way for the casual user of e-mail to satisfy the statute's safe harbor requirement that he restrict access to recipients of his e-mail to adults. If Joe wants to send some artwork to someone he met in a chat room, he cannot very well ask the virtual acquaintance for a credit card number. As far as e-mail is concerned, then, the CDA in effect bans a wide range of communications between adults.

The impact of the CDA on amateur home pages should be obvious. Internet users looking for something interesting on a home page sometimes go from page to page for a long time before they find whatever it is they are looking for. No one who expects to hit 20 home pages or so in 15 minutes is going to bother to obtain a personal identification number (PIN) or give a credit card number to access each one. [49] Even a user looking through only a few home pages will simply not be willing to obtain a PIN or give a credit card number to view an amateur page offering only a few photos or other information of unknown quality. Many computer network users are understandably cautious about divulging credit or other information online, since they cannot easily identify with whom they are dealing at the other end of the transaction; even if they could, they know the network itself is vulnerable to hackers. [50] The CDA forces authors of amateur home pages to choose between keeping silent or losing their audience.

Amateur speakers who do decide to restrict access to their Web sites by requiring a credit card number or PIN access will find the means to do so are not available to them. Providers of credit card services may be unwilling to serve amateur or small-scale Web sites. According to the testimony of the government's expert witness in the American Civil Liberty Union's lawsuit against the CDA, credit card verification agencies probably would not process a card verification request unless it accompanied a commercial transaction. [51] If they did, they would charge a fee (about $.60 to $1 per verification) that most amateur content providers could not afford. [52] The credit card verification companies' reluctance to deal with amateur operators will also affect implementation of any PIN-based access system, because the easiest way for an operator to determine an applicant's eligibility for an adult PIN is to ask for a credit card number. Third-party age verification services such as those used by sites offering pornography charge users or content providers for their services. [53] The CDA thus implies that, for the most part, only large-scale, commercial, or institutional enterprises will offer content that is covered by the Act.

Credit card or PIN-based access systems, then, will not work at all for newsgroups or e-mail. In addition, they are both overly cumbersome and economically infeasible for the vast majority of chat rooms or Web sites, particularly those that provide information for free, on a not-for-profit basis, or on small commercial sites. In theory, the Act allows other "good faith" and "effective" defenses. But no such alternatives exist. Thus, following the enactment of the CDA into

law, some amateur Web sites simply shut down. Other amateur sites were still up and running; they attempted to comply with the Act by "honor system" methods of restricting children's access. Such methods include layers of click-through warnings, or requiring those accessing the site to declare their age.

Unfortunately, such labeling almost certainly does not satisfy the CDA's requirement that restricting access to children be done using an "effective" method. While the legislative history does not require 100 percent effectiveness, warning labels are unlikely to divert more than a handful of honest, uncurious children.

Other amateurs or small-scale enterprises have tried to comply with the Act by registering their sites with various organizations that rate Web sites' content. [54] Parents can purchase software, further discussed below, that prevents children from accessing sites with certain ratings. However, site registration would not restrict access for those children whose parents have not purchased such blocking software. Registration alone, too, will run afoul of the CDA's "effectiveness" requirement. [55] Ironically, a Web site author could be prosecuted for allowing site access to a child whose parents believe that he or she is mature enough to handle the information in question.

Theoretically, operators of chat rooms could restrict access up front by requiring a credit card number or PIN, segregating chat rooms into adults-only and public. But it is common for would-be participants in chats to go from room to room in search of a conversation that interests them, sometimes ranging through 20 rooms before they find one they like. No one will do this who must run a gauntlet of PIN or credit card requests. The populations of the adults-only rooms will be extremely low, since few adults will be willing to risk divulging their credit card numbers or go to the trouble of obtaining an adult PIN to access the chat rooms. And, whenever participants in a chat are in a room that does not restrict access, the CDA requires them to self-censor. The application of the CDA to chat rooms will thus preclude a vast number of interchanges between adults.

The CDA and the Constitution

The framers of the Constitution intended our government to have only those powers enumerated in the Constitution. The Constitution does not authorize Congress to regulate the content of speech. The original purpose of the commerce clause, which regulates interstate commerce, was to prevent impediments to the free flow of interstate commerce, not to empower censorship. [56] The First Amendment underscores this, stipulating that "Congress shall make no law...abridging the freedom of speech, or of the press." Under this constitutional structure, could anyone seriously believe that the CDA does not violate the Constitution?

In an extraordinary departure from enumerated powers analysis, the Supreme Court has permitted nonobscene sexual speech to be regulated, if the law is the least restrictive means of serving a compelling government interest. [57] The Supreme Court has also upheld laws requiring broadcasters to broadcast indecent material only late at night, [58] and a law restricting material that is considered obscene because it is "harmful to minors" from being sold to minors. [59] Under these precedents, the lower courts have upheld laws requiring customers to obtain an adult PIN or use a credit card number to access telephone dial-a-porn. [60] The Supreme Court, however, did rule that a total ban on indecent dial-a-porn was unconstitutional. [61]

To a certain extent, proponents of the CDA tried to bring it within these First Amendment precedents. They did not, however, try very hard. At the time of this writing, therefore, most experts predict that the CDA will be ruled unconstitutional under existing precedents; [62] the district judges' decisions in Philadelphia and New York bear this out.

Vagueness. If no one can understand what a law means, he or she cannot know whether he or she is complying with it or not. This simply is not fair. Vague laws also invite tremendous impact on politically unpopular speech; under a statute that permits "a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections," [63] prosecution will be arbitrary. So will judgments. Uncertain whether and when a vague law applies, a speaker may choose not to speak at all. [64] The Supreme Court has explained that a "person of ordinary intelligence" should be able to know what is prohibited. [65]

The legislative history suggests that interpretation of computer network indecency must follow the pattern established by regulators of broadcast indecency. Here again, the FCC declines to lay down any general rule describing what will not be considered "patently offensive" and therefore indecent. Professor Weinberg explains that the FCC's indecency rulings "are not susceptible to clear-cut rules; they are based on 'context' which in turn depends on a 'host of variables.'" [66]

Professor Weinberg concludes that such ad hoc rulings cannot satisfy established First Amendment vagueness doctrine. [67] A law cannot be said to be clear if its interpretation depends on factors not mentioned in the law itself, such that one never knows until years after the transmission in question whether one has violated the law or not. In spite of this, the Supreme Court refused to rule on a vagueness challenge to the FCC's broadcast indecency regime; the District of Columbia Circuit has, strangely, interpreted this to mean that the FCC's regime is not too vague. [68]

But it is unlikely that the courts' reluctance to recognize the vagueness problems with regulation of broadcast indecency will determine the outcome of a vagueness challenge to the CDA. For the first time, the courts will have to consider the effect of the law on amateur speakers, ordinary persons rather than powerful commercial enterprises. Thus, although the panel convened in New York did not find the plaintiff likely to succeed on his vagueness challenge, [69] its members were perhaps unduly influenced by the Supreme Court's recent rejection of a vagueness challenge to a statute regulating cable television [70]--yet another situation in which the Court was able to duck the question of the impact of the statute on the ordinary user. Finally, precedents aside, it is clear that the scope of material covered by the CDA is unclear. No court should refuse to recognize the problem.

In declaring the CDA to be unconstitutional, Chief Judge Sloviter agreed with Judge Buckwalter that the statute was unconstitutionally vague, especially as it was unclear whether the question of what was "patently offensive" would be determined with reference to national or community standards. [71]

Overbreadth. Supporters of the CDA have been quick to assure the public that the CDA does not differ substantially from measures regulating sexual content in other media, including broadcasting and the print media. [72] Such claims are misleading.

It is true that the Supreme Court has ruled that a statute punishing the sale of material that is "harmful to minors" is constitutional. But the Supreme Court also explained that that category of material closely tracked what would be considered obscene. [73] The category of "indecency" is much, much broader. In the words of the Supreme Court, "the normal definition of the term indecent merely refers to nonconformance with accepted standards of morality." [74] This means that it is now illegal to distribute text over the Internet that any child could legally see by walking into a library or bookstore and pulling a book off the shelf. A prime example is the George Carlin "Seven Dirty Words" monologue, which the FCC ruled was indecent in the *Pacifica* case. The monologue is appended to the text of the Supreme Court's opinion in *Pacifica* and is available without restriction in many libraries. The ACLU apparently has violated the CDA, however, by posting the text of the monologue to its Web site without restricting children's access to the site.

Also significant is the CDA's lack of exceptions for works of literary or artistic merit. In defending the CDA, the Department of Justice argued that prosecutors could be trusted not to apply the Act to such works. Judge Sloviter of the Philadelphia court correctly dismissed this argument, saying that "the bottom line is that the First Amendment should not be interpreted to require us to entrust the protection it affords to the judgment of prosecutors. Prosecutors come and go.... The First Amendment remains to give protection to future generations as well." [75]

Finally, the statute's affirmative defenses are almost entirely useless for most amateur content providers. For the panel of New York judges, that fact made the statute fatally overbroad. [76]

Why Indecency on Computer Networks Should Not Be Censored

One can be certain, however, that the censors will not give up. If the CDA ultimately is declared unconstitutional, the censors will try to craft new legislation along similar lines.

Possible Alternatives to the CDA

Legislation somewhat less broad than the CDA would cover only material that is "harmful to minors." *This option would essentially still ban much amateur speech because of the technical and economic difficulties of restricting access*. More sophisticated plans have also been suggested.

Use of site rating labels could be added to the available defenses (which would in effect make labeling of sexually explicit sites mandatory) to ease this problem somewhat. Labels can be used to rate newsgroups, Web sites, and content posted on online networks. Eugene Volokh of the University of California Los Angeles Law School has suggested that governments could require all content providers to rate their own sites. [77] Parents could then buy software filters that would reject adult-rated content.

In defending the CDA, the Department of Justice crafted a similar argument. Under one proposal supported by the Department of Justice, all "indecent" materials would be tagged "L18," for "not less than 18." At the first CDA hearing in Philadelphia, the Department of Justice explained that computer network users would be registered as "adults" or "minors," and that information would be encoded in their online personas. Network servers (the computers on which content is stored) would be customized to deny minors access to Web sites tagged "L18." [78] The proposal would require all Internet service providers to reprogram a substantial number of their servers. The CDA does not require Internet service providers to undertake any such project; generally, only those that control content are liable under the law. Thus, the argument that the L18/server scheme could alleviate the burdens of the CDA on speakers was essentially absurd, as Judge Sloviter noted. [79] Additionally, courts have recognized that advanced speaker registration requirements stifle the spontaneity of free expression. [80] And advanced registration would threaten the existence of electronic forums operated for the benefit of those most anxious to protect their identity, such as victims of sexual abuse. [81] Finally, the suggestion that servers be restructured is eerily reminiscent of the Singapore government's insistence that Internet communications be routed through "proxy servers" to facilitate intensive political censorship.

By the second CDA hearing, the government had apparently abandoned the server/registration approach to tagging, and explained that the tags could work with filtering software controlled by the end user. But that would not satisfy the CDA's effectiveness requirement, as Judge Cabranes noted, because many parents do not use filtering software; the Department of Justice's assertions at the hearing that it would not prosecute labeled sites were not binding on any prosecutor. [82] As a defense of the CDA, both incarnations of the L18 scheme failed. But they might suggest a direction for future legislative efforts.

Any form of mandatory labeling, however, is objectionable for several reasons. First, it is compelled speech, which should not be constitutionally permissible. [83] It would place an extraordinary burden on entities with large collections of works, such as libraries. [84] It would be oppressive to expect such labels to be applied to casual or intimate speech, such as statements in chat rooms, private e-mail, or individual newsgroup or bulletin board postings. For spontaneous computer speech, *mandatory tagging would be the equivalent of requiring the labeling of conversations around a backyard barbecue*.

Second, mandatory labeling as unsophisticated as the L18 scheme proposed by the Department of Justice would prevent older children from accessing information about reproduction, art, and other topics, or from contributing to discussions of those topics. Minors, too, have free speech rights. Sixteen-year-olds should not be restricted to viewing what is fit for six-year-olds.

Third, because there is so much content on computer networks, the only practically feasible kind of universal labeling scheme would require content providers to rate their own material. A substantial number of amateur or casual speakers would, out of an excess of caution or as an act of civil disobedience, deliberately give their sites a more or less restrictive label than the law requires. Libraries might be forced to slap an "adult" label on their entire collection, because they could not afford to rate all their content. There are so many thousands of communications traveling over computer networks every day that only a very small proportion of the labels would be checked by third parties. Thus, ironically, a mandatory labeling regime is more likely than voluntary labeling to be substantially inaccurate and

unhelpful to parents. Under the market-driven voluntary systems that will work with the new rating standards known as PICS (Platform for Internet Content Selection), unrated sites can be blocked automatically by filter software; a greater proportion of those fewer sites that are rated can be checked by private ratings groups. Only voluntary rating would be consistently undertaken with care.

The Fallacy Motivating the Search for CDA Alternatives

Proposing any legislative alternative to the CDA makes a fundamental error: such proposals *assume that government has constitutional authority to regulate nonobscene sexually explicit computer network speech*. Judge Dalzell identified this as the central issue at the hearings concerning the constitutionality of the CDA, stating that:

> from the Supreme Court's many decisions regulating different media differently, I conclude that we cannot simply assume that the Government has the power to regulate protected speech over the Internet....Rather, we must decide the validity of the underlying assumption as well, to wit, whether the Government has the power to regulate protected speech at all. [85]

The analysis below shows that this assumption is not valid. Even if we assume that the precedents that allow the government to regulate nonobscene sexual speech on other media are correct, these precedents do not supply any convincing rationale for regulation of computer networks. Communication over computer networks does not raise entirely new constitutional issues. But it raises two particularly important issues in such a way that they cannot be avoided.

First, computer networks empower millions of ordinary citizens to become speakers. As censorship laws are enforced, the court's failure to coherently define categories of forbidden talk about sex will look more and more obviously unjust and arbitrary.

Second, the power of the private sector to offer alternatives to censorship erodes arguments that government has any legitimate interest in this problem. Without a constitutionally cognizable interest in imposing the regulation, government cannot act.

These are both sound reasons to believe that indecency (or its cousin, material that is "harmful to minors") on computer networks cannot constitutionally be regulated at all. First Amendment jurisprudence must evolve to address these issues or become divorced from the reality of the marketplace of ideas.

Defining Forbidden Speech

Unwilling to rule that government simply may not censor any speech, the Supreme Court has struggled to distinguish between speech about sex that may be censored, and speech that may not be. Early on, the Court decided that obscene speech was not entitled to First Amendment protection. But what was obscene? The Court's attempts to define this category coherently have important implications for regulation of indecency or material that is "harmful to minors" on computer networks.

This is not because obscenity and indecency are the same thing. Whatever is obscene is almost certainly indecent; a wide range of material that is indecent is not obscene. But our judgments about what is obscene and what is indecent are closely tied to subjective moral judgments. If the Court cannot define one category coherently, it is unlikely to make much headway with the other. Nor is it likely to make headway with the in-between category of "harmful to minors."

For years, the Supreme Court struggled to create a national definition of obscenity. It failed. At bottom, the question of what is "obscene" is a matter of taste. No power in the world can convert a subjective question into an objective one, even by abstracting from the myriad subjective tastes of members of a national community. Under the "national" approach, ultimately, a work was obscene if it offended enough Justices of the Supreme Court. This was evidenced by hilarious yet deeply troubling statements such as that of Justice Potter Stewart, who, in attempting to define hard-core pornography declared, "I know it when I see it." [86] In 1963, Chief Justice Earl Warren stated, "I believe there is no

[87]

provable 'national standard.'" ___ Still later, in abandoning the national standard, the Court explained:

> it is neither realistic nor constitutionally sound to read the First Amendment as requiring that the people of Maine or Mississippi accept public depiction of conduct found tolerable in Las Vegas, or New York City. People in different states vary in their tastes and attitudes, and this diversity is not to be strangled by the absolutism of imposed uniformity. [88]

Similarly, the FCC has failed to craft a coherent national standard of broadcast indecency. According to the FCC, broadcast indecency is to be judged according to the tastes of the "average broadcast viewer." But who is this "average" viewer? In a country with local standards as diverse as those of San Francisco or Iowa, there can be no such animal. The national standard boils down to what offends the FCC.

Insofar as interpreters of the CDA are directed by the legislative history to craft a national indecency standard, they will be no more successful than the FCC. The early print media precedents are no more helpful. It is possible for any court to string together words in an important sounding way, crafting phrases such as "prurient interest," or a mythical national consensus, and claim to have created a uniform definition of indecency. What it will have done, in effect, is to impose its tastes on the rest of the nation.

Nor can the Court resolve the problem by referring to a hypothetical "average" computer network user. A First Amendment that protected only "average" speech would provide little or no protection at all to unpopular minorities. Part of the reason that computer networks are special is that they empower an extraordinary range of speakers from diverse communities. The tastes of the "average" user are thus not only hard to identify, but should be of no relevance.

If there cannot be a national standard for forbidden speech about sex on computer networks, can there be local standards? The Supreme Court allowed states to adopt community standards to alleviate the embarrassment of its failure to craft a national obscenity standard for the print media. [89] The question of what was obscene was largely left to local juries. [90]

But some members of the Court long resisted adopting a local community standard, for good reason. Justice William Brennan argued that the local community standard could not serve as a constitutional standard:

> We do not see how any "local" definition of the "community" could properly be employed in delineating the area of expression that is protected by the Federal Constitution....It would be a hardy person who would sell a book or exhibit a film anywhere in the land after this Court had sustained the judgment of one "community" holding it to be outside the constitutional protection. [91]

His fear was that an adverse judgment in a few restrictive local communities would chill the national distribution of speech.

The Supreme Court has since flatly refused to recognize the constitutional dimensions of this problem. In one case, the Court considered a dial-a-porn operator's argument that Congress could not force it to tailor its messages to the least restrictive community, because such a requirement in effect created a national standard of obscenity. The Court explained, "While Sable [the operator] may be forced to incur some costs in developing and implementing a system for screening the locale of incoming calls, there is no constitutional impediment to enacting a law which may impose such costs on a medium electing to provide these messages." [92]

Computer networks will raise this issue again, this time with a vengeance. The impact of the law will be felt, not by the narrow, unpopular community of professional pornographers, but by ordinary citizens able to reach a wide audience for the first time. The local standard will not suffice in any country that takes free speech seriously.

If the national standard is inherently incoherent, and the local standard inherently unfair, what is the Court to do? The answer is that the Court should admit that government, especially the federal government, has no place regulating the display of sexual imagery in cyberspace, especially if it is neither obscene nor categorized as child pornography. If it cannot be done consistent with the Constitution, it should not be done.

But will this mean that the United States' children are to be exposed to a never-ending stream of sexually explicit images? It will not mean that at all. And the dispute surrounding the constitutionality of the CDA is the perfect opportunity for the Court to make this clear.

Market Alternatives Erode the Government Interest

The Supreme Court's indecency jurisprudence requires that a statute choose the least restrictive means to serve a compelling state interest. The Court's accumulated indecency cases, however, do not make clear what that interest is. It is either government's interest in helping parents protect their children, or an independent interest of government in protecting the children themselves. [93] The analysis below shows that the latter interest cannot be viewed as constitutionally compelling. And, where computer networks are concerned, parents are capable of taking care of their own children. With computer networks, government's interest falls away.

An Interest in Helping Parents. The Supreme Court has described the government's interest in regulating indecency as an interest in helping parents supervise their children--not in protecting children from indecency when their parents believe the materials in question would do their children no harm:

> Constitutional interpretation has consistently recognized that the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society.... The legislature could properly conclude that parents and others, teachers for example, who have this primary responsibility for children's well-being are entitled to the support of laws designed to aid discharge of that responsibility...*the prohibition against sales to minors does not bar parents who so desire from purchasing the magazines for their children* [emphasis added]. [94]

It is not rational to argue, however, that government can have a compelling interest in helping concerned parents when concerned parents do not need help. Government should not be able to argue that it has a compelling solution to a problem that has effective private solutions.

Computer networks offer an excellent private solution to parents who want to protect their children from indecency, but who do not want to deny access to online services altogether. As with any media, parents can control their child's access to computerized indecency by exercising a little sense. Some parents, for example, do not allow their children access to online services in the privacy of their own rooms; access is available only by means of a computer in the family room, where anyone walking by can see what is on the screen.

Technology is available to supplement parental supervision. Software is available to parents who want to restrict their children's access to indecent material online. The cost of filtering software is about $30 to $50--about the cost of a computer game, and not nearly as much as the computer itself.

Some filters block sites identified as undesirable (the "exclusive" approach). If such software operated only by blocking lists of sites actually visited and rated "bad," it would allow all unrated sites through. Thus, products such as CyberSitter, [95] CyberPatrol, [96] and SurfWatch also restrict the type of Web searches that a child can perform and restrict visits to unrated content by watching for words and phrases typical of sexually explicit material. One government witness during the CDA trial testified that he had been able to find sites that SurfWatch did not block. But he admitted during cross-examination that SurfWatch had been turned off during the searches he used to find those sites, and that SurfWatch would not have allowed him to perform those searches. [97] Developers of filters that take the exclusive approach defend it on the grounds that undesirable sites are rare. Nigel Spicer, president of Microsystems, Inc., explains that "it's more effective to monitor the 1 percent of sites that are inappropriate." [98]

Other software avoids the problem of unrated sites by allowing access only to rated sites (the "inclusive" approach). For example, users of CyberPatrol may opt to allow access only to the "CyberYES" list, which contains about 10,000 sites. [99] SafeSurf, a voluntary rating organization, includes 50,000 child-friendly sites in its Cyber-Playground. [100]

These software solutions are in relatively early stages of development. But they are already effective and affordable.

As the technology advances, they will become even more so. Children might attempt to evade the controls, for example, by booting the computer from a floppy diskette and attempting to access the Internet directly without triggering the filtering software. Or a child might attempt to defeat the software by deleting files from config.sys. Gordon Ross explains that Net Nanny works at the operating systems level, monitoring the status of all files on the system. If a child attempts to use either evasion method, Net Nanny can shut down the computer or simply notify parents of the evasion attempts. [101] CyberSitter [102] has similar features. CyberPatrol prevents children from accessing the Internet after booting the computer from a floppy by monitoring all activity at the computer's communications port, and also shuts down the system in response to attempts to disable CyberPatrol's files, which upon installation are hidden throughout the operating system. [103] Some devices, such as CyberSitter, also have the ability to report to parents which sites the child has visited.

PICS, an industry group, has created a technical platform for encoding ratings of online content, including Web sites, newsgroup content, audio and video files, FTP sites, and individual images within a document. [104] The PICS standard enables Web browsers such as Netscape or Microsoft's Internet Explorer to read a line of code attached to Web sites, which can be used to classify the site according to a variety of ratings systems. [105] PICS is backed by the most important developers of access software, including Netscape, IBM, MCI, SurfWatch, Microsoft, Compuserve, Prodigy, AT&T, and SafeSurf. The PICS standard went from the drawing board to marketplace reality in only eight months, showing the rapid response of markets to parents' concerns. [106] All software filters and Internet browsers are expected to work with the PICS system. [107] Because browsers and filters can be set to automatically reject unrated sites, rating is encouraged. Britain's Science and Technology Minister Ian Taylor has said that PICS appears to be a solution to that government's request for the industry to self-regulate. [108] Table 1 gives an overview of some software filters that will work with PICS.

The software ratings systems that PICS enables are far more responsive to parents' concerns than any statutory solution. One rating system (RSACi), developed by PICS in cooperation with the Recreational Software Advisory Council (RSAC), [109] classifies content according to levels of nudity, sex, language, and violence. [110] Content providers seeking an RSACi label must complete a questionnaire on RSACi's Web site, detailing the "level, nature, and intensity of sex, nudity, violence, or offensive language (vulgar or hate motivated)" in the content. A rating is then automatically assigned based on the responses; the labels are encoded to prevent tampering. [116] SafeSurf's rating system employs nine categories, helping parents to restrict exposure to profanity, heterosexual themes, homosexual themes,violence, gambling, intolerance, drug use glorification, and other adult themes.

Table 1
Selected Software Filters

Product	Price	Functions
Net Nanny Trove Investment PC only	$39.95 Free Updates	Real-time monitoring of Web sites, newgroups, FTP, Internet Relay Chat (IRC), and e-mail for keywords. Users can add terms to keyword dictionary, which is keyword updated bimonthly. Also allows users to opt between exclusive or inclusive lists. Users can add or subtract sites from lists. Will be PICS compatible and work with SafeSurf and RSACi ratings. Can block child from revealing information such as names or credit card numbers. Estimated 150,000 to 200,000 copies distributed worldwide. [111]
		Exclusive blocking only. Logs Internet activity, controlling access to Web,

CyberSitter Solid Oak Software PC only	$39.95 Free updates	newsgroups, IRC, and e-mail. Lets parents block, block and alert, or alert when certain sites are accessed, including SafeSurf or RSACi "bad site" lists. Lists can be customized. Restricts searches using context-sensitive phrase filtering. PICS compatible. Over 100,000 copies distributed. [112]
Specs NewView Mac & PC	$39.95	Inclusive (access to sites rated safe by NewView), per year semiexclusive, or exclusive limits on Web, IRC, NewView newsgroups, Telnet, FTP, and e-mail. Inclusive setting offers kids' directory of 150,000 sites, about 1 million Internet pages. Semiexclusive offers the directory, and uses dictionary to check unrated sites. Very new pure exclusive setting blocks 2,000 sites. Allows parental override. Winter release to be PICS compatible, log use, tell parents of attempts to circumvent. [113]
SurfWatch	Sells for about $20.00; updates $5.95 a month;some ISPs offer free	Exclusive blocking of Web, chat, newsgroups, and FTP sites. September release will add inclusive blocking; "safe" lists offered in partnership with rating services will range from 3,000 to 50,000 sites. Fall release will be PICS compatible, add the ability to add or delete sites from lists. [114]
CyberPatrol Microsystems Mac & PC	$29.95 with 3 months of updates; further 6-month updates $19.95; free edition	Exclusive blocking of CyberNOT or SafeSurf list, or inclusive access to CyberYES list. Optional keyword blocking. Updates downloaded automatically every seven days. Screens Web sites, IRC, and newsgroups. Sites can be added or reinstated manually. Can restrict time spent online. PICS compatible. Can stop child from revealing name, address, credit card numbers in chat rooms. Separate settings for up to 10 different children.
InterGO InterGO Communications Inc.	$49.95	Inclusive or exclusive. Can be set to access only SafeSurf's "white" list. Or, older users are sent to Web listing of 3,500 sites rated by age group; parents can add sites as "bookmarks." KinderGuard Web , crawlers search content of unrated sites, block "adults only" (about 25,000 sites as of August 5, 1996, updated weekly). Parents can override ratings, rate unrated sites. Fall release will be PICS compatible. [115]

Some might argue that software solutions are not as effective as a statute that cordons off or bans indecent network speech. In fact, these devices are substantially more effective. Note that censorship laws passed in the United States do not apply to sexually explicit material posted in foreign jurisdictions. Currently, about 30 percent of indecent material on the Internet originates in foreign jurisdictions; [117] obviously, there is nothing to stop this proportion from growing rapidly in response to developments in the United States. The statutory solution therefore is no real solution at all.

One potential weakness of some blocking software is that it might fail to block access to misrated sites (sites accidentally or deliberately rated "safe" that are not). First, at this stage, misrating is largely a theoretical problem. It remains to be seen what solutions civil society would devise should this become a serious problem; under a government of enumerated powers with no authority to regulate speech, the market must be given a chance to operate. It would be highly inappropriate for government to become involved in deciding whether any highly subjective, value-laden private rating system had been applied correctly in a particular case.

Second, the problem is likely to occur only with blocking systems that rely on *unchecked* self-rating, without offering any kind of backup. Systems that rely on third parties to rate sites, [118] or to create and supervise a child-safe environment of the type described, have mechanisms in place for evicting miscreants. SafeSurf reviews the ratings of about 300 to 500 sites a day, [119] and plans to block sites that deliberately violate the system. [120] RSAC plans to do spot checks of sites that use RSACi to ensure that sites are correctly labeled, and is in discussions with a company to monitor the labels. [121]

Most important, the government's interest in occasional problems with misrating, unrated sites, or software that can be defeated by a few enterprising children cannot possibly be compelling. It is hard to imagine any child being permanently harmed by a few encounters with misrated indecency, any more than by sneaking a peek at *Playboy* in a neighbor's garage.

Additionally, parents who are not satisfied that software filters are at present sufficiently sophisticated and effective have other options. Child-safe environments also have been created by major online service providers. Compuserve offers a kids' version of WOW!, which lets parents screen their kids' incoming e-mail, has no chat or shopping features, and restricts Web access to sites approved by WOW!'s staff. [122] America Online provides filters that allow parents to restrict children to Kids Only areas that are supervised by adults, allows parents to block all chat rooms, selected chat rooms, instant messages (a sort of instant e-mail), and newsgroups. Prodigy lets users restrict children by limiting access to certain newsgroups, chat rooms, and the Web. Yahooligans! will permit access only to Internet areas rated "safe." [123] Microsoft Network's service automatically restricts access to adult areas except to users who have submitted an electronic form requesting access; Microsoft then checks to see if the account is subscribed to someone over 18. Bess, an Internet service provider for families and schools, automatically blocks sites that are not suitable for children. The list of blocked sites is updated daily and blocked automatically, with no need for action on the part of users. [124]

The federal government's interest in restricting indecent speech on interactive computer networks cannot be "compelling" if there is a purely private way to effectively solve the problem. Finding a compelling interest in regulation of indecent speech on interactive computer networks makes no sense, when private solutions are widely available and effective, and rapidly becoming more so.

An Independent Interest in Protecting Children? Perhaps government could claim a compelling interest in protecting unsupervised children, children whose parents do not purchase or use filtering software? Justice Stephen Breyer, writing for the plurality in *Denver Area Educational Telecommunications Consortium v. FCC*, a case involving the constitutionality of restrictions on the transmission of indecent material over cable television, restates that protection of children is a compelling or at least important interest, and suggests, without further analysis, that such interest allows the federal government to intervene to protect children of "inattentive" parents. [125]

There are substantial reasons to believe that protecting children from a danger that the childrens' parents do not recognize as particularly grave should not amount to a compelling interest. As pointed out above, filtering software is

affordable to anyone who can afford a computer system. Nonsupervising parents have implicitly decided that exposure to material of a sexual nature probably will not harm their children enough to bother with.*If the parents do not find the interest sufficiently compelling to take action, there is no reason to think that government should*.

Indeed, there may be parents who believe that their children should be exposed to materials that might be considered indecent, including information about disease prevention, birth control, reproduction, works of literature and art, and so on. Government's claim of an independent interest in restricting indecency *contradicts* government's claim of an interest in helping parents control their children's education. [126]

If government did have an independent compelling interest in keeping children from viewing all sexually explicit or vulgar material, it could pass a law that parents must lock all the indecent materials in their home (*Playboy*, romance novels, *Lady Chatterley's Lover*) in special safes to ensure that their children never access it. Or that parents must use software filters to prevent teenagers from using the Internet to read about sex.

Imagine police searching through private residences to enforce this law. The reaction would be public outrage. In short, when it comes down to it, there is *nothing* compelling about government's alleged interest in protecting children from indecency. In this context, we recognize that parents have the right and responsibility to make decisions about such matters for themselves.

So why do we pretend that the interest becomes compelling when the burden of complying with the law is placed on someone other than the parents? We pretend it because we place the burden of complying with the law on unpopular speakers--pornographers, purveyors of smut.

The application of indecency laws to computer networks will throw the issue into stark relief. First, under the CDA, it is possible that parents and teachers could be prosecuted for allowing children in their charge to use computers to access material that the parents believe the child is mature enough to handle. Second, the easy availability of private solutions for parents who are concerned about indecency makes it obvious that the CDA is nothing but a convenience for parents who will not take the trouble to supervise their children--not a compelling problem that the government must step in to solve.

Private solutions might not always be available to solve "indecency problems." On public property, for example, which everyone must access from time to time, one faces more difficult questions. But computer networks are not public parks. They are sophisticated user-controlled private spaces. And private solutions clearly should be part of the constitutional analysis.

Conclusion

The new regime of indecency regulation for computer networks affects anyone, anywhere. Interactive computer service providers have been compared to bookstores, the postal service, broadcasters, publishers, and to a telephone service. No single one of those comparisons or analogies can begin to capture what an interactive computer service can do. Interactive computer services are all of those things put together. A law that censors those services, therefore, is equivalent to a law that censors newspapers, the mail, television and radio service, libraries, bookstores, and telephone and fax calls, all put together.

In fact, however, the CDA is much worse. Computer networks have special qualities of their own that are not captured by analogy to any other medium. In some respects, network exchanges resemble the sorts of exchanges people might have with one another in face-to-face meetings. Conversations among strangers in chat rooms are completely unlike the traditional point-to-point communication in a telephone call, where one would be unlikely to converse with a total stranger for no particular reason, and much more like the casual mingling that one would see in a real-life social gathering. This new censorship law marks an extraordinary extension of "decency" regulation to casual encounters.

However, at the same time, computer technology empowers the speaker's audience to reject and filter unacceptable information. Indeed, user controls are proving the only effective and fair means of controlling distribution of information content.

Courts facing constitutional challenges to the CDA and its successors have a choice. They can ignore the real burdens that any indecency regulation would place upon spontaneous Internet speech. They can ignore the fact that the government is claiming an interest in helping parents solve a problem that parents need no help to solve. Courts that take this route will doom the First Amendment to irrelevance.

Any court prepared to recognize the reality of what computer networks offer speakers and listeners will realize an amazing opportunity to step forward and restore the First Amendment. Parents, not the government, could and should choose what information they and their children will distribute and receive. We can only hope that the courts will recognize this opportunity and take it.

Footnotes

[1]. Olmstead v. United States, 277 U.S. 438, 479 (1928).

[2]. Fred W. Weingarten, "Debate over Indecency on the Net Reveals Deep Divisions," Computer Magazine (February 1996) pp. 68, 73.

[3]. Robert Corn-Revere, "New Age Comstockery: Exon vs. the Internet," Cato Institute Policy Analysis No. 232 (June 28, 1995).

[4]. Weingarten, pp. 68, 73.

[5]. ACLU v. Reno, 929 F. Supp. 824, 825 (E.D. Pa. 1996).

[6]. Shea v. Reno, Civil Action No. 96-Q9767 (July 29, 1996).

[7]. Eugene Volokh, "Cheap Speech and What It Will Do," 104 Yale Law Journal 1805 (1995): 1819.

[8]. See further discussion in ACLU v. Reno, 929 F. Supp. at 843.

[9]. Mary Meeker and Chris DePuy, The Internet Report (New York: HarperBusiness, 1996), pp. 4-7.

[10]. Declan McCullagh, interview with author, August 6, 1996.

[11]. David Post, "Flame On: The State of Nature and the First Internet War," Reason (April 1996) pp. 28, 31.

[12]. See Shea v. Reno, at 14-17.

[13]. Meeker and DePuy, pp. 3-12.

[14]. John Kavanagh and Roger Sinclair, "Kicks," Financial Times Guide: A-Z of the Internet, 1996, p. 19.

[15]. Mary K. Williams, "No Place Like Home; PC 'Pages' Let You Roll Out New Welcome Mat," Chicago Tribune, April 11, 1996, p. C1.

[16]. Shea v. Reno, at 17-19.

[17]. See United States v. Thomas, 74 F.3d 701, 704-05 (6th Cir. 1995).

[18]. Mitch Ratcliffe, "Reach Out and Entertain Someone; Telephone Companies Take an Interest in Tinseltown," Digital Media (January 2, 1995) p. 7.

[19]. Stewart Brand, Media Lab (New York: Viking, 1987) p. 28.

[20]. Ratcliffe, p. 7.

[21]. Ibid.

[22]. Ibid.

[23]. See, e.g., Cathleen A. Cleaver, "Cyberspace Cleanup or Censorship," Washington Times, February 11, 1996, p. B1; William F. Buckley Jr., "Tangled Web for Obscenity Enforcers," Washington Times, March 1, 1996, p. A17; Arianna Huffington, "Internet Evils Beyond the Indecency Limits," Washington Times, March 16, 1996, p. C3.

[24]. Cleaver, p. B1.

[25]. Defendant's Opposition to Plaintiff's Motion for a Temporary Restraining Order, ACLU v. Reno, Civil Action No. 96-963, February 14, 1996, n. 7.

[26]. For discussions of Rimm's work, see Jonathan Wallace and Mark Mangan, Sex, Laws and Cyber-Space: Freedom and Censorship on the Frontiers of the Online Revolution (New York: Henry Holt & Co., 1996), pp. 125-153, and Charles Platt, Anarchy Online (New York: Black Sheep Books, 1996). See also <http://www.me.titech.ac.jp80/=@=:www.2000.ogsm.vanderbilt.edu/cyberporn.debate.cgi>. (August 1996); Declan McCullagh, "The Case of the Two Cybersex Studies," <http://www.cybernothing.org/jdfalk/media-coverage/archive/msg02626.html>. (August 1996).

[27]. Patrick A. Trueman, "Porn on the Internet, Here and Abroad," Washington Times, January 18, 1996, A19.

[28]. Family Research Council, "Smut: Out-of-Line Online," Washington Watch, February 26, 1996, p. 1.

[29]. Telecommunications Act of 1996, 47 U.S.C. §223(d).

[30]. The law's preemption provisions also are significant to the ordinary user. The law protects commercial and noncommercial institutions, such as libraries, from more restrictive state laws. Ibid., at 47 U.S.C. §223. But, very significantly, the law does not preempt more strict state laws of individuals publishing or distributing content as individuals.

[31]. Joint Explanatory Statement of the Committee of Conference, in Peter W. Huber, Michael K. Kellogg, and John Thorne, Special Report: The Telecommunications Act of 1996 (Boston: Little, Brown & Co., 1996), p. 385.

[32]. Alliance for Community Media v. FCC, 56 F.3d 105, 129 (D.C. Cir. 1995)(Wald, J., dissenting).

[33]. See., e.g., Jonathan Weinberg, "Vagueness and Indecency," Villanova Sports & Entertainment Law Journal 221 (1996).

[34]. Sagittarius Broadcasting Corp., 7 FCC Rcd. 6873, 6874 (1992).

[35]. Weinberg, p. 230.

[36]. Corn-Revere, pp. 12-15.

[37]. Miller v. California, 413 U.S. 93 (1973).

[38]. Ginsberg v. New York, 390 U.S. 629 (1968).

[39]. See Georgia Code §16-12-103.

[40]. Fla. Stat. Ann. §847.0125 (display for sale); Kan. Stat. Ann. §21-430c(a)(1)(commercial establishments); La. Rev. Stat. §14-91.11(a)(display at newsstand or other commercial establishment open to persons under seventeen); Minn. Stat. Ann. §617.293, subd. 2(a)(commercial display); N.M. Stat. §30-37-2.1 (retail establishments); N.C. Stat §14-190.14 (commercial establishments); Tenn. Code Ann. §19-17-914(a)(display for sale or rent); Okla. Stat. Ann.

§§1040.75, 1040.76 (all displays).

[41]. Huber, Kellogg, and Thorne, p. 389.

[42]. Infinity Broadcasting Corp., 3 FCC Rcd. 930, 933 (1987).

[43]. Telecommunications Act of 1996, 47 U.S.C. §223(e)(5)(B).

[44]. Ibid., at §223(e)(5)(A).

[45]. Huber, Kellogg, and Thorne, p. 389.

[46]. Telecommunications Act of 1996, 47 U.S.C. §223(e)(1).

[47]. Ibid., at §223(e)(2).

[48]. Ibid., at §223(e)(3).

[49]. ACLU v. Reno, 929 F. Supp. at 846. "Credit card verification would significantly delay the retrieval of information on the Internet. Dr. Daniel Olsen, the expert testifying for the Government, agreed that even 'a minute is [an] absolutely unreasonable [delay]....People would not put up with a minute.'"

[50]. Indeed, the Internet is so apt to leak information that verification of a credit card number over the Internet is not now technically possible. Ibid.

[51]. Ibid.

[52]. Ibid.; Shea v. Reno, at 30.

[53]. ACLU v. Reno, 929 F. Supp. 846; see Shea v. Reno, at 31.

[54]. See Will Rodger, "Adult Sites Seek Ratings to Show 'Good Faith,'" Interactive Week (March 11, 1996) p. 12.

[55]. Shea v. Reno, at 57.

[56]. Roger Pilon, "A Modest Proposal on 'Must-Carry,' the 1992 Cable Act, and Regulation Generally: Go Back to Basics," 17 Hastings Communications and Entertainment Law Journal 41 (1994).

[57]. Sable Communications of California, Inc. v. FCC, 492 U.S. 115, 126 (1988).

[58]. FCC v. Pacifica Foundation, 438 U.S. 727 (1977).

[59]. Ginsberg, 390 U.S. 629.

[60]. See Dial Information Services Corporation of New York v. Thornburgh, 938 F.2d 1535 (2nd Cir. 1991).

[61]. Sable Communications, 492 U.S. at 125-126.

[62]. See Eugene Volokh, "Freedom of Speech in Cyberspace from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harassment, and Sex," University of Chicago Legal Forum, forthcoming (1996).

[63]. Smith v. Goguen, 415 U.S. 466, 575 (1974).

[64]. Grayned v. City of Rockford, 408 U.S. 104, 108-09 (1972); Connally v. General Construction Co., 269 U.S. 382, 391 (1926); Baggett v. Bullitt, 377 U.S. 260, 372 (1964).

[65]. Grayned, 408 U.S. at 108; Smith v. Goguen, 415 U.S. at 572.

[66]. Weinberg, p. 227.

[67]. "Ordinary First Amendment law limits government regulators to black-letter determinations, in which results turn mechanically on a limited number of easily ascertainable facts." Weinberg, p. 228.

[68]. See Action for Children's Television, 852 F.2d 1332, 1338-39 (1988); Pacifica Foundation, 438 U.S. at 726.

[69]. Shea v. Reno, at 35-43.

[70]. Denver Area Educational Telecommunications Consortium v. FCC, 64 U.S.L.W. 4706 (June 25, 1996).

[71]. ACLU v. Reno, 929 F. Supp. at 846.

[72]. See, e.g., Cleaver, p. B1 ("There is nothing novel about this new law"); Buckley, p. A17.

[73]. Ginsberg, 390 U.S. at 643.

[74]. Pacifica Foundation, 438 U.S. at 726, 740.

[75]. ACLU v. Reno, 929 F. Supp. at 846.

[76]. Shea v. Reno, at 43-58.

[77]. Volokh, "Freedom of Speech in Cyberspace."

[78]. Declan McCullagh, "CDA Court Challenge, Update #6," April 11, 1996, <http://www.eff.org/pub/Legal/cases/EFF_ACLU_v_DOJ/mccullagh.041196.update>. (August 1996).

[79]. She explained that "tagging alone does nothing to prevent children from accessing potentially indecent material, because it depends on the cooperation of third parties to block the material on which the tags are embedded. Yet these third parties, over which the content providers have no control, are not subject to the CDA.... The government's tagging proposal is purely hypothetical and offers no currently operative defense to Internet content providers." ACLU v. Reno, 929 F. Supp. at 856.

[80]. Rosen v. Port of Portland, 641 F.2d 1243, 1249 (1981) (ruling that requirement that speakers wishing to exercise First Amendment rights in port facilities must register one day in advance violates Constitution).

[81]. One Internet service provider's representative explained his concerns as follows: We provide free anonymous access to the net to sexual abuse survivors. We don't even know who they are, nor do we care--a lot of them are hiding out...and to try and identify them would be an enormous breach of their trust, as they are depending on us for their anonymity... some of them are under the age of 18.... Sure, we could trace each and every one of them back to their providers, and find out who they are, but I'm not going to do it, and I'm perfectly willing to go to jail to protect their identities. My integrity is worth a whole hell of a lot more than any government law. Declan McCullagh, "CDA Court Challenge, Update #6."

[82]. Shea v. Reno, at 14-17.

[83]. Riley v. National Federation of the Blind, 487 U.S. 781 (1988) (state could not require charity solicitors to detail how much money went to professional fundraisers).

[84]. ACLU v. Reno, 929 F. Supp. at 856.

[85]. ACLU v. Reno, 929 F. Supp. at 846.

[86]. Jacobellis v. Ohio, 378 U.S. 184, at 197 (1963) (Stewart, J., concurring).

[87]. Jacobellis, 378 U.S. at 193 (Warren, C.J., dissenting).

[88]. Miller, 413 U.S. at 32-33.

[89]. The basic guidelines for the trier of fact must be (a) whether "the average person, applying contemporary community standards" would find the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

[90]. Miller, 413 U.S. at 30 ("The adversary system, with lay jurors as the usual ultimate fact-finders in criminal prosecutions, has historically permitted triers of fact to draw on the standards of their community, guided always by limiting instructions on the law").

[91]. Jacobellis, 378 U.S. at 193.

[92]. Sable Communications, 492 U.S. at 125-126.

[93]. Alliance for Community Media v. FCC, 56 F.3d at 137.

[94]. Ginsberg, 390 U.S. at 639.

[95]. Mark Kantor, vice president, marketing, Solid Oak Software, interview with the author, August 2, 1996.

[96]. Susan Getgood, marketing/advertising manager, Microsystems Software, Inc., interview with the author, August 2, 1996.

[97]. Letter from Jay Friedland, vice president of marketing, SurfWatch, <http://www.slate.com/Email/Current/Email.asp>. August 1996.

[98]. "Choices Face Those Controlling Access," New Media Age, May 14, 1996, p. 12.

[99]. Interview with Getgood.

[100]. Ray Soular, SafeSurf, interview with the author, August 8, 1996.

[101]. Gordon Ross, president and chief executive officer, Trove Investment, Inc., interview with the author, August 2, 1996.

[102]. Interview with Kantor.

[103]. Interview with Getgood.

[104]. Robert Uhlig, "Connected: Net Porn Filter Strips XXX Files," The Daily Telegraph, May 21, 1996, p. 4.

[105]. Stephen Lynch, "The Rating Game," Orange County Register, March 31, 1996, p. K9.

[106]. "PICS Ready to Go Worldwide as Practical Alternative to Global Censorship of Net," EDP Weekly (March 25, 1996) p. 1.

[107]. See "SurfWatch AT&T WorldNet's Parental Control Software," Newsbytes (March 15, 1996); "Microsoft Internet Explorer 3.0 Beta Now Available," PR Newswire (May 29, 1996); "Choices Face Those Controlling Access," New Media Age (May 14, 1996) p. 12; "PICS Ready to Go Worldwide as Practical Alternative to Global Censorship of Net," p. 1.

[108]. Uhlig, p. 4.

[109]. RSAC was founded in response to public dismay about violent video games. It developed a rating system to label game titles according to levels of violence and sex. "Choices Face Those Controlling Access," p. 12.

[110]. Uhlig, p. 4.

[111]. Interview with Ross.

[112]. Interview with Kantor.

[113]. Kristine Conness, marketing program manager, NewView, Inc., interview with the author, August 5, 1996.

[114]. E-mail from Jay Friedland, Spyglass Inc., to author, August 11, 1996.

[115]. Lana Brian, InterGO Communications, Inc., interview with the author, August 5, 1996.

[116]. "Choices Face Those Controlling Access," p. 12.

[117]. Shea v. Reno, at 25.

[118]. Microsoft's CyberNOT list, for example, is generated by a five-person team of online patrollers, rather than by trusting the negative sites to identify themselves. See Jim O'Brien, "Teach Your Children and Save Money: Don't Get Snowed by Pricey Online Chaperone Software," Computer Shopper (January 1996) p. 667.

[119]. Lynch, p. K9.

[120]. O'Brien, p. 667.

[121]. Uhlig, p. 4.

[122]. Thomas Mace and Rick Ayre, "WOW! From Compuserve," PC Magazine (June 11, 1996) p. 140.

[123]. "Livingston, Yahoo! Partner to Make Internet Kid-Safe; Yahooligans! Is First Application of ChoiceNet Technology," Business Wire (May 6, 1996); "Livingston's Server-Based 'ChoiceNet' Technology Offers Customizable Control Over Internet Access," Business Wire (April 1, 1996).

[124]. See <http://www.vtw.or/pubs/ipcfaq>. (August 1996).

[125]. Denver Area Educational Telecommunications Consortium, 64 U.S.L.W. at 4713, 4714.

[126]. See Action for Children's Television v. FCC, 58 F.3d 654, 672 (D.C. Cir. 1995)(Edwards, C.J., dissenting).