OVERVIEW

The Internet and other interactive services are a new medium, and a new array of markets, different from any means of communication that has come before. This new medium raises fundamental questions about the appropriate balance between the needs of the market, of American families, and basic constitutional free speech and privacy guarantees that Americans value so deeply. In order to protect families and children in this open, global network, we should first rely on the entrepreneurial spirit of the interactive services market to build parental empowerment tools, and encourage the industry to work together to ensure that such solutions are widely available. The interactive media market must not be regulated like telegraphs, broadcast radio and television, and telephones, thereby stifling the development of an important new communications medium with burdensome regulations. Rather, we should identify policies that enable the interactive media market to flourish like the personal computer industry, and provide parents the ability to protect their children from inappropriate material that is internationally-available.

In answer to questions posed to the Interactive Working Group by Senator Patrick Leahy earlier this year, this report contains an assessment of:

1. general policy issues at stake in the regulation of content on the National Information Infrastructure;

2. the current state of criminal law regarding obscenity, child pornography, and harassment online;

3. software and services available today that enable parents to restrict their children from access to inappropriate material online;

4. threats to free speech, free press and individual privacy raised by proposed regulation of indecency in interactive media.

http://old.cdt.org/speech/cda/950724iwg_leahy.html
We begin with a brief overview of the contents of the report:

**A. A New Regulatory Model for Interactive Media is needed to Ensure Free Speech and Continued Innovation in the National and International Information Infrastructure.**

The Internet is a global information and communications system which is becoming a critical resource for organizations and individuals around the world. Businesses, schools, libraries, researchers, community groups, and individuals are all coming to rely on the Internet as a vital communications system and information resource. The Internet and other interactive media include electronic mail, the World Wide Web, online discussion groups, and other multimedia information resources. Providers of interactive media services range from large and small online services and bulletin boards, to those who provide services for their own use such as schools, libraries, and large and small businesses.

To ensure the continued growth of the new interactive media market, national policy for the Internet must:

1. preserve the vibrant free market in interactive media, free from regulation of constitutionally-protected communications and information;

2. preserve full constitutional free speech and privacy protections in new interactive media;

3. encourage the industry to work together to develop blocking and filtering technologies that empower parents to restrict their children's access to offensive material;

4. ensure emerging media not be used for criminal activity such as stalking, trafficking in obscenity, and the creation of child pornography.

**B. Currently Available Blocking and Filtering Technology, combined with public education, can empower parents to protect their children from inappropriate material online.**

While the vast majority of content on the Internet is intended for legitimate educational, cultural, political, or entertainment value. Some material on the Internet, however, may not
be appropriate for children. Moreover, much of this material is accessible from the United States but transmitted from other countries, beyond the practical reach of U.S. law. In order to protect children we must rely on powerful new blocking and filtering technology to empower parents to make choices about the material which their children can access.

- Entrepreneurial effort has already produced blocking and filtering products for families and schools: The inherent power of computer software allows the creation of computer programs which enable parents to block material from the reach of their children automatically, without the need for constant parental supervision. Such software can be easily installed by parents, even those who are not computer experts.

- The global and decentralized nature of interactive media requires new approaches to child protection: Censorship of centralized media such as radio and television may be effective at keeping the "seven dirty words" off the airwaves. However, on the Internet, with tens of millions of content creators all over the world, US law, no matter how tough, will never be able to keep offensive material out of the reach of kids.

- Industry-wide initiatives are developing standard label and blocking conventions to increase the effectiveness of blocking: The flexibility of interactive media allows multiple rating systems to co-exist so that individuals and families can chose a rating system that best reflects their own values. No single government- mandated system could be as comprehensive or flexible as voluntary private sector alternatives.

- Individual and parental choice assures full respect for the free speech rights in interactive media: Relying on individuals and parents, not the government, to make choices about the content that they and their families receive assures maximum respect for First Amendment rights of adults to receive and transmit constitutionally- protected material, and allows families, not federal bureaucrats, to determine what information is most consistent with their own moral values.

Any changes in federal law should seek to remove the Hobson's choice faced by all who provide access to the Internet. In order to protect children, legal disincentives facing those who would create 'child safe' areas should be removed.

- Recent case law discourages online providers from screening material that is inappropriate for children: In the recent Stratton Oakmont, Inc. v. Prodigy Services Company, No. 31063/94 (N.Y. Sup. Ct. May 24, 1995) case, Prodigy was found to be a "publisher" of libelous statements made by a subscriber on one of its online bulletin boards. Such added exposure to legal liability is a substantial disincentive to the creation of 'child safe' interactive services.
Neither federal nor state law should punish service providers for creating child-safe services. The marketplace should be free to create a variety of online forums, some that provide only material appropriate for children, and others that are more open and designed for a wider audience.

C. There is No Anarchy in Interactive Media: Vigorous enforcement of current criminal laws will protect all users from obscenity, child pornography, and harassment online.

Law enforcement agencies and some prominent pro-family groups agree current laws already enable prosecutions of online obscenity violations. More vigorous enforcement of existing criminal laws may, however, be necessary. Following this logic, it is unnecessary to amend federal law to prohibit distribution of obscenity by computer, since existing law already criminalizes such conduct, as well as threats and harassment by computer.

- The Department of Justice and American Family Association state that existing laws already criminalize obscenity online.


- Online obscenity and child pornography crimes are being prosecuted around the country: These laws are being enforced, as is evident by numerous prosecutions around the country.

- The Senate-passed legislative proposals fail to add any protections against online stalking and child solicitation: Everyone is concerned about protecting children from threats online and off. Ironically, the Senate-passed Communications Decency Amendment only punishes indecency and obscenity, not stalking or solicitation. Neither prosecutors nor police receive any additional help in the prevention or prosecution of online crimes against children.
D. Bans on indecent communications online are unconstitutional.

The unique nature of interactive media demands that policy makers carefully evaluate the application of the First Amendment in a new light. Essential to the Court's approval of indecency restrictions in the broadcast media was the fact that listeners had insufficient control over programming to which they were exposed. Any effort to impose similar indecency restrictions on interactive media, however, will not pass constitutional scrutiny given the high degree of user control in this new medium.

- To assure the First Amendment free flow of information and protect individual privacy rights, liability for online service providers must be carefully limited: If online system and service providers are held criminally liable for obscene or indecent material, created by their users, and not intentionally purveyed by the provider, then public service providers and private system operators will be forced to become private censors in order to limit their own legal risk. Just as current law limits the liability of phone companies, mail services, and other carriers for the content of material which the carrier merely transports, online service provider liability should be limited in order to assure the free flow of information on the National Information Infrastructure.

- Ability of users and parents to control the material to which they have access places constitutional limits on the degree to which the government can censor material based on its content: The First Amendment has been interpreted to allow restrictions on indecent speech only if such government restrictions are the "least restrictive means" of protecting children or accomplishing other important government goals. Given that parents are able to protect their children from unwanted material using screening tools, government restrictions are unnecessary and therefore unconstitutional.

- Online service providers should not be forced to become private censors: If online services or individual system operators are held liable for all of their users' communications, the services will be forced to impose stringent censorship rules on their users in order to limit the corporate liability of the service provider. Such rules would only create a chilling effect on users of interactive media.

- There are great constitutional difficulties in defining "indecency": Neither the Congress nor the Supreme Court have ever established a single definition for what constitutes "indecent" material. The FCC has offered different definitions for indecency depending on the communications medium. Embarking on such a process for interactive media would be fraught with Constitutional disputes and challenges in
court. Efforts to ban indecency on dial-a-porn services lead to ten years of constitutional litigation, thus delaying the enforcement of those regulations considerably.

- The Federal Communications Commission should not be given power to regulate content in interactive media: The inherent complexity and constitutional difficulties of regulating indecency would involve the FCC in lengthy and burdensome rulemaking to implement any indecency ban. Such extension of FCC control over new media will create unnecessary bureaucratic intrusions that hinder the development of new interactive media and private sector screening options.

I. Public Policy Reflecting Unique Nature of Interactive Media is Essential to Ensure the Potential of the National Information Infrastructure and Protect Children

The Internet and other interactive communications media are fundamentally decentralized media. Unlike centralized broadcast radio and television services, there are no central control points through which either a single network operator or government censors can control particular content. On the Internet there are literally millions of speakers and publishers. This proliferation of individual speakers stands in sharp contrast to broadcast television or even cable television, where one may count five, ten or perhaps one hundred speakers, each of whom controls a channel. Federal broadcast content regulators can direct their regulations at the operators of a particular channel in order to enforce their regulations. However, content control on the Internet would have to be targeted at each and every one of the millions of US citizens and international users that speak daily online. Any attempt to impose centralized content control in a bureaucratic manner on this fundamentally decentralized medium is bound to stifle the growth of the medium, squander the democratic potential of the Internet, and may even cut the United States off from the growing global information infrastructure.

A. Attempts at "Command and Control" regulation of content online will stifle innovation in interactive media.
As a decentralized medium, the Internet and other interactive services have flourished in a largely unregulated environment. Indeed, recent Congressional decisions to commercialize the Internet has lead to a tremendous increase in the number of users who have access to the Internet and great innovations such as the World Wide Web. Indeed, the innovative, entrepreneurial Internet marketplace has even produced a variety of software and services that help protect children from inappropriate material online. Imposition of content regulations and extension of Federal Communications Commission jurisdiction over standards and technologies would seriously retard the growth of the Internet marketplace. What's more, FCC content control is unlikely to be effective in protecting children.

B. Heavy-handed content regulation will squander the democratic potential of interactive media.

As the popularity and accessibility of the Internet and commercial online services grows, and as the medium becomes easier to use, the political uses of the net have flourished. Political discourse is facilitated by a variety of different communications techniques possible online, including newsgroups, mailing list discussion groups, chat sessions, and a host of electronic publishing capabilities. Any regulation creating criminal penalties for communication of indecent material would have a substantial chilling effect on all who use interactive media. Such a chilling effect would severely inhibit the growth of the Internet as a political forum.

Political groups left, right, and center are using the Internet to communicate, to organize, and to advocate their own views. Advocacy organizations have found World Wide Web services are critical to political education activities, and an increasing number of grass roots and community groups are coming to rely on the Internet to keep in touch with members and constituents. In fact, even some Senators offices are using the World Wide Web to communicate with and solicit feedback from constituents. As a nation we should be encouraging political discourse in this new medium, because of it potential to raise the level of political discussion beyond the sound bite and to involve more citizens in the political process. Encouraging political discourse in interactive media requires that all users are assured that their First Amendment and privacy rights will be respected fully.

Indeed, the Internet and other online services are fast becoming a new public forum for political discourse for American citizens. In order to preserve the freedom and openness of this new political arena, it is critical to avoid creating a chilling effect on individual expression.
II. Parental and User Control Technologies Available Today to Screen Unwanted Content

Overview -- Dealing With Inappropriate Material in Cyberspace Through Technology.

Interactive media such as the Internet and commercial online services such as America Online and Prodigy offer users tremendous control over the information that they and their children receive. Unlike traditional mass media which "assaults" viewers with content, interactive media requires users to seek out information from any number of the millions of available World Wide Web sites, online file archives, and from any of the more than 3000 Usenet newsgroups.

The vast majority of the content available on interactive media is related to normal everyday topics such as politics, sports, consumer information, shopping, to name just a few. In addition, millions of people use the Internet every day to conduct business, socialize, organize political activities, and communicate on issues of interest to them. However, just like in the terrestrial world, there are areas of cyberspace which may contain materials that are not appropriate for children.

Preventing children from successfully gaining access to such material is an important issue which must be addressed. However, because cyberspace is a global network with millions of users, active policing of content by governments, besides the obvious implications for free speech and privacy rights, is simply not a practical or effective solution.

There is a growing market for applications that empower users and parents to control their children's access to inappropriate materials on the Internet and commercial online services. This document provides an extensive (though by no means exhaustive) overview of some of the technologies currently available. All but two of the tools mentioned here are currently available to consumers across the country.

Four categories of technological options are examined here, each provides a slightly different, but equally effective, point of intervention.

1. Commercial Online Services Parental Control Features
The Parental Control Feature of three of the most popular commercial online services (America Online, Prodigy, an Compuserve) are illustrated. These features are embedded in the service and are available to all subscribers of these services at no additional charge.

2. Features for the Home PC and Direct Internet Access

For families that do not subscribe to one of the commercial online services but instead receive direct access to the Internet, there are a variety of products that run right on the home PC (SurfWatch, NET NANNY, and CYBERsitter). Some of these products are also compatible with and can run in addition to the parental control features available on the commercial services.

3. Applications for Schools and Businesses

Schools and corporations can employ server based technologies such as the Netscape Proxy Server and WEBTrack to prevent users from accessing inappropriate content while in the classroom or at the office.

4. Proposals for the Future

In addition to these examples of products currently on the market, there is a innovative proposal being offered by Nathaniel Borenstein and Darren New. KidCode, a proposed Internet protocol, is a voluntary rating system that can prevent children from accessing content that may not be appropriate.

A. Child Protection in Commercial Online Services.

Commercial online services such as America Online, Compuserve, and Prodigy offer technologies that allow parents to block their children's access to certain online forums where children might be exposed to inappropriate content. Other services run filtering software which automatically screens messages posted to public forums that contain language inappropriate to children.

1. America Online Parental Control Features

America Online (AOL), one of the large commercial online service providers, contains a feature which allows parents to prevent their children from accessing interactive discussion forums (a.k.a. "Chat Rooms"). A small minority of these forums, which are areas provided by America Online and are accessible only to
AOL's subscribers, sometimes contain language and other discussion which may not be suitable for children. Parents are empowered to prevent their children from accessing these areas simply by selecting a menu option and entering a password. The block out function cannot be de-activated without the password.

America Online also offers parents the ability to block access to Usenet newsgroups based on keywords, subject matter, or specific newsgroups. For example, parents can configure their system to block access to newsgroups containing the word "sex", or can block access to specific newsgroups such as "alt.sex.binaries.pictures". This mechanism is not exclusive to sexually explicit materials -- the software can be configured to block access to groups based on any keyword. Configuring this system is as simple as clicking a button and describing the keywords or groups to be blocked.

Concerned parents, even if they are less computer literate than their children, have easy access to these control features. AOL provides telephone help, detailed instructions and advice for parents. There is no additional cost for this service, and, like the other parental control features on AOL, the feature cannot be turned off without a password known only to the parent.

Finally, on July 17, 1995, America Online announced that they had entered a partnership with SurfWatch Software (described below). Starting in the fall of 1995 AOL will provide SurfWatch as part of its regular service, preventing children from accessing sites on the Internet known to contain sexually explicit material. SurfWatch will run continuously, unless disabled by the parent, and will provide a further layer of protection for children who use America Online.

2. Prodigy Internet access restrictions

Prodigy runs special screening software that monitors messages posted to public bulletin boards and chat rooms on the Prodigy network, and automatically blocks messages which contain language (such as the "seven dirty words"), and other content deemed inappropriate for children.

Like all the major commercial online services, Prodigy offers users access to the Internet. Prodigy will not provide customers access to the Internet without the authorization by the head of the household (the principal account holder). The authorization is made at the time of the account setup and requires credit card verification. This additional child protection feature is designed to ensure that parents are aware that their child has access to the Internet where Prodigy cannot control the content.
Finally, Prodigy offers parents the ability to monitor which sites their child has visited on the World Wide Web. Each time a site is visited, the Prodigy software records that site in a log which can be displayed at a later time. Parents can keep track of where their children have gone in cyberspace, and can instruct their children not to visit sites which may contain inappropriate materials (based on their own personal values).

3. Compuserve: Internet in a Box for kids

Compuserve another of the large commercial online services, recently announced a partnership with SPRY Inc. (makers of the popular "Internet in a Box") is currently developing two child protection features: Internet In a Box for Kids, and KidNet.

Internet In a Box for Kids contains a program called Crossing Guard, which will allow parents to control their children's access to the by blocking access to sites that may contain inappropriate materials. Crossing Guard will also allow parents to monitor their children's online activities and set timers to control when and how long their children can surf the net.

Parents who purchase Internet In a Box for Kids will automatically become subscribers to KidNet, an electronic community designed specifically for kids. The site will allow members to congregate, chat, exchange information, shop, and play interactive games. All content on KidNet will be closely monitored to ensure that it is appropriate for children. The area will also be designed to offer teachers and adults access to educational sites, school networks and other resources for education and information geared to kids. KidNet will also include a home page builder that will allow kids to develop their own resources.

The product will begin shipping in the Fall of 1995. Information is currently available at the Compuserve/Spry Home Page: http://www.spry.com

B. Parental Empowerment Applications for the Home PC and Direct Internet Access.

Although many parents subscribe to commercial online services such as those mentioned above, access to the global information highway is not limited to commercial online services. Many parents, educational institutions, and corporations choose to access the directly through an Internet Access Provider. Unlike commercial online services, access providers generally do not provide any of their own content. Because of this, parental control features must be initiated on the Home PC.

There are a variety of software developers working on parental control features for this
market. Some of these applications can be used in conjunction with commercial online services, over and above the parental control features provided by commercial services, while others are designed specifically for direct access.

1. 'Surf Watch'

Surf Watch Software is designed to provide parental control for families who do not subscribe to commercial online services. SurfWatch allows parents to block their children's access to Usenet newsgroups, World Wide Web sites, gopher and file archives (ftp sites) which are known to contain sexually explicit material. When activated with a private password held only by a parent, Surf Watch completely prevents any user from accessing these areas. The program is launched when the computer is started up, and operates when the parent is not present.

SurfWatch employs a group of professional "net.surfers" to find out and log sites on the where sexually explicit material is located. Sites are reviewed by a group of concerned parents and educators to determine the nature of the content, and those sites which meet specific criteria are added to a list which is embedded in the program.

SurfWatch software resides on the home PC. When activated, the program cross-checks every attempt to access Usenet newsgroups, world wide web, gopher, and ftp sites. Sites which are included on the list are blocked automatically. Because the new sites are constantly appearing on the net, SurfWatch provides a subscription service that automatically updates the list of sites to be blocked, without any intervention required from the user. Subscribers can receive updates as frequently as they choose.

Surf Watch Software maintains the list of sites the program will block, and will make custom lists available if requested. SurfWatch will also soon provide users the ability to add an delete sites to their own custom lists Both Windows and Macintosh versions are available now for under $50.00.

SurfWatch is available now for under $50.00. Information on SurfWatch is available on the world wide web: http://www.surfwatch.com/

2. NET NANNY

NET NANNY, developed by Net Nanny Ltd. of Vancouver BC Canada, is designed to prevent children from accessing areas on the Internet that a parent deems
inappropriate, prevent children from giving their name, address, telephone number, credit card, or other personal information to strangers via email or chat rooms, and can log off an online service or shut down the computer when the child attempts any of these activities.

The program contains a dictionary in which the parent can enter the names of sites known to contain sexually explicit or other material (e.g., the Usenet newsgroup alt.sex hierarchy, or the web site http://www.playboy.com). Parents may also enter phrases such as "what's your name?", "what's your phone number", "where do you live", or "are your parents home". If anyone attempts to ask these questions, NET NANNY will automatically log off the network or shut down the computer.

NET NANNY can also be configured to block access to files on the PC's hard drive, floppy drive and CD-ROM, to prevent a child from accessing and altering the parent's financial records, work related files, and programs and files intended only for adults.

Finally, the program keeps a log of all activity that occurs on the computer, allowing parents to monitor their children's use of the computer. By using this feature, parents can determine if their children are using the computer to access inappropriate material, and can then augment the Dictionary to prevent further access.

NET NANNY is compatible with commercial online services and direct Internet access providers. The program is launched when the computer is started up, and operates when the parent is not present.

Net Nanny is available for Windows users for $49.95. More information can be found on the World Wide Web: http://www.netnanny.com/netnanny

3.'CYBERsitter'

CYBERsitter, developed by Solid Oak Software in Santa Barbara California, allows parents to monitor their children's computer activity and can prevent a child from downloading image, sound, and video files. It will also prevent children from accessing files on the home PC hard drive such as financial information, business related files, CD-ROM titles, and anything else a parent determines their children should not have access to. The program is launched when the computer is started up, and operates when the parent is not present.

CYBERsitter keeps a log of all activity on the computer, including access to the, commercial online services, and local files on the hard drive, CD-ROMs and floppy
disks, enabling parents to monitor their children's use of the computer.

CYBERsitter is available for $29.95. More information, and a free demonstration version of the product (for Windows) is available on the world wide web:
http://www.solidaok.com/~solidoak

C. Solutions in the Schools and Businesses -- Server Based Applications.

In addition to the commercial online services and home access environments, many schools (from k-12 to universities) and corporations are beginning to provide access to the Internet. Many of these organizations are becoming increasingly concerned about the availability of not only sexually explicit materials, but also games, sports information, gambling sites, and other areas which may not be appropriate for access during school and work hours.

Products such as the Netscape Proxy Server and WEBTrack provide schools and businesses the ability to block specific sites from access by all users on the network, and to track an monitor use of the Internet.

1. Netscape Proxy Server

The Netscape Proxy Server, developed by Netscape Communications Corporation (the developer of the popular World Wide Web browser), allows schools and business to block access to specific sites on the Internet, individual computers (IP addresses) and other information. The Server operates in the background and does not require teachers or employees to have sophisticated programming knowledge or configure any feature. The systems administrator is responsible for operating the server and for maintaining the list of sites to be blocked.

The Server can be configured to block access to specified World Wide Web, file archives (ftp), and Gopher sites on the for users on the network on which the server is deployed. In other words, a school or business which runs the Netscape proxy server can prevent students or employees from accessing sites known to contain sexually explicit materials, information about drugs, gambling, sports, games, and anything else determined to be inappropriate for users on the network.

2. WEBTrack

WEBTrack, developed by Webster Network Strategies in Naples Florida, allows businesses to block access to certain pre-determined sites on the Internet. The product
gives businesses the capability to restrict access to 15 categories of World Wide Web, Gopher, and ftp sites (including sexually explicit material, games, gambling, job search information, drugs, online merchandising, sports, humor, and others), while allowing full access to a wide variety of resources. The product is designed to promote the use of the Internet for business purposes while restricting recreational use.

On July 17, 1995, Webster Network Strategies announced that it would provide its software free to K-12 schools, ensuring that all of America's children who access the Internet from the classroom will not be able to stumble upon inappropriate material.

WEBTrack also allows corporate systems administrators to monitor employee use of the network in order to determine if an employee is using the to access materials which violate stated corporate policy.

WEBTrack is available for most major network servers, and costs approximately $7,500. Updates of the site list are available on a subscription basis for $1,500 per year.

D. Future Applications and Protocol Solutions.

1. Information Highway Parental Empowerment Group

A consortium assembled by Microsoft, Netscape Communications, and Progressive Networks recently announced plans to develop technical standards to enable voluntary rating of a variety of content available through the Internet and other online services. These standards would enable content creators to voluntarily label their own content so that individuals and families can block the material, if they chose. In addition, the Information Highway Parental Empowerment Group (IHPEG) will create standards to allow "third-party" rating of content online. Much as TV Guide rates TV shows on broadcast television, IHPEG would enable multiple third-party rating of content available online.

2. KidCode

Among the more innovative of proposals on the drawing boards is KidCode, currently being developed by Nathaniel Borenstein and Darren New. KidCode, a proposal for an Internet protocol designed to block access to sites based on a common voluntary
rating system, is in the early stages of development, but would be compatible with all of the parental control applications currently on the market.

KidCode is a proposed convention for labeling World Wide Web and other sites on the Internet as containing material which may not be suitable for children. There are an infinite number of possible categories (e.g., sexually explicit material, violent material, drug related material, etc.).

Content providers and individuals who create web 'Home Pages' could voluntarily incorporate a standardized KidCode tag in the address of the site. Browser applications would be configured to read these tags and determine if the content on the site is appropriate for the viewing.

In addition, KidCode can accommodate third party ratings, age verification, and other factors. Finally, because KidCode is a voluntary rating system that may not be employed by every content provider on the, it can be configured to block access to sites that do not contain KidCode tags. In other words, if a site chooses not to use KidCode, a child using a KidCode enabled program would not be able to access that site regardless of the content it contains.

The Borenstein-New KidCode proposal is still in the early stages of development and has not yet been deployed. Further information can be obtained automatically by sending email to.

**Prospects for the future**

The products described here represent only a fraction of what is currently available to empower parents to protect their children from inappropriate material on the Internet. Moreover, these are only the beginning, as the industry is committed to developing more and better solutions, and the open nature of the Internet provides a wealth of possibilities for parental empowerment tools that may not yet have been imagined.

The availability of material on the Internet which may be inappropriate for children is a serious issue and one of `legitimate concern, However, because the Internet is a global network with millions of users, top-down, command and control content restrictions simply cannot effectively control the availability of such materials. The only effective way to protect children from inappropriate material on the Internet is to encourage the continued development and deployment of tools that empower parents to control their children's online activities based on their own individual tastes and preferences. The products described here provide parents these tools, and can do so without the need for burdensome legislation.
or government imposed content restrictions.

III. Prosecution of Obscenity, Child Pornography, and Other Violations of Criminal Law in Interactive Media Proceeding Under Current Law

As the Internet and other interactive media become more fully integrated into the fabric of our society it is sad, but not surprising, that criminal behavior begins to appear online. Already cases of consumer fraud and theft of intellectual property have been reported and prosecuted. Traffickers in obscenity and child pornography, too, have begun to use the Internet to facilitate their criminal behavior. Notwithstanding the recent appearance of crime online, cyberspace is not left in a state of anarchy. Federal criminal laws against transportation of obscenity, child pornography, and harassment have all been used successfully to prosecute criminal behavior online.

More vigorous enforcement of existing criminal laws may be necessary, but law enforcement agencies and some prominent pro-family groups agree current laws already enable prosecutions of online obscenity violations. The Justice Department has repeatedly stated that there are no gaps in current federal criminal laws prohibiting the distribution by computer of obscenity and child pornography. Following this logic, it is unnecessary to amend federal law to prohibit distribution of obscenity by computer, since existing law already criminalizes such conduct, as well as threats made by computer.

A. There is no anarchy in cyberspace: Federal and state criminal laws already are used to prosecute criminal conduct in interactive media.

Tough obscenity, child pornography and harassment laws are already in the federal criminal code. Under existing Federal law trafficking in obscenity (18 U.S.C. §§1462, 1464, 1466), child pornography (18 U.S.C. §2252), harassment (18 U.S.C. §875(c)), illegal solicitation or luring of minors (18 U.S.C. §2423(b)), and threatening to injure someone (18 U.S.C. §875(c)) have already been successfully applied to punish conduct on computer networks. Notwithstanding all of the concern in the popular media and the United States Senate about this issue, all indications are that these and other laws fully cover all serious criminal behavior that may be perpetrated in cyberspace.

The Department of Justice and the American Family Association agree that existing laws already criminalize obscenity online. The American Family Association, a prominent pro-family, anti-pornography group lead by a former federal prosecutor from the Reagan and
Bush administrations wrote to Chairman Thomas Bliley:

"[T]he federal criminal code currently prohibits distribution of both child pornography and obscenity by computer."

In a communication to Senator Leahy, the Justice Department agrees with this assessment:

"[W]e have applied current law to this emerging problem. . . . The Department's Criminal Division has, indeed, successfully prosecuted violations of federal child pornography and obscenity laws which were perpetrated with computer technology."

Thus, while more enforcement resources may or may not be required, no case has been made that any new criminal laws are needed in this area.

B. Violations of obscenity, child pornography, and other criminal law online are being prosecuted.

Even as the Congress rushes to enact new criminal laws, online obscenity and child pornography crimes online are being prosecuted around the country under existing law. According to the Justice Department:

"The Criminal Division's Child Exploitation and Obscenity Section is aggressively investigating and prosecuting the distribution of child pornography and obscenity through computer networks, and the use of computers to locate minors for the purpose of sexual exploitation."

To the extent that any obstacles arise, Congress should examine whether there is a need for additional training and resources for enforcement. The Justice Department, the agency responsible for investigating and prosecuting these crimes, sees no urgent need for legislation and instead has urged -- prior to any congressional action -- "in-depth analysis" of the "number of complex legal and policy issues" raised by the need to protect children while respecting the First Amendment and privacy rights of computer users. The precise constitutional parameters, for example, of criminal obscenity laws and the application of community standards doctrine to interactive media are currently being decided by the courts. If Congressional investigation determines that there are actual gaps in current law, it may, then, be appropriate to investigate modernization or clarification of existing law.

Ironically, the Communications Decency Act as passed by the United States Senate as part of the telecommunications reform bill, fails to add any protections against online stalking and child solicitation. Everyone is concerned about protecting children from threats online
and off. The Senate-passed Communications Decency Act, however, only punishes indecency and obscenity, not stalking or solicitation. It offers no help to prosecutors or police in prevention of prosecution of online crimes against children.

IV. Censorship of Indecent Communications In Interactive Media Suffers Fundamental Constitutional Infirmity

Indecency restrictions have the acknowledged important purpose of protecting minors from access to controversial and inappropriate sexually explicit material. However, such restrictions, especially if imposed on new interactive media, would be subject to serious constitutional challenge. This section of the report will demonstrate five key constitutional points:

1. Censorship of indecent communications prohibited: General bans on indecent material are unconstitutional.

2. Impermissibly intrusive means of achieving legitimate goal: First Amendment jurisprudence requires that restrictions on speech adopt the "least restrictive means" available for achieving a compelling purpose. Due to the availability of programs such as Surf Watch and the parental control features on America Online and other commercial services, blanket indecency restrictions are clearly not the "least restrictive means", and are unconstitutional on their face.

3. Invasion of privacy: By criminalizing the content of private, non-obscene messages, the Act would force an invasion of the realm of private electronic communications and end the individual's ability to control the content of information he or she chooses to access in private.

4. Creation of private censors: Holding service providers criminally-liable for the content of all messages that they carry will force providers to become private censors and prescreen all communications traveling across their system.

Most importantly, statist, bureaucratic command and control regulation of indecent material online fails to take advantage of the empowering aspects of new interactive media, which can allow parents and other users to exercise control over the information that to which they and their children have access.

Legislating about new interactive media requires a careful understanding of the unique
attributes of this new medium. First and foremost, interactive media enable users (including parents) to exercise choice over the information to which they and their children have access. In sharp contrast to older media, government content regulation is simply not necessary in order to shield children from possibly inappropriate information. Furthermore, given the heavily fact-based determination required to justify regulation of indecency, legislative findings based on open hearings and a public record are essential before any legislation could pass constitutional muster.

Indecency restrictions for interactive media would enshrine in statute a sharp distinction between the print medium and new interactive media. For example, though an individual is allowed to go into a bookstore and buy a sexually-explicit magazine or a "lewd" work of art, one would not be able to access the identical information over the Internet. Both the interactive media and the print media are arenas in which individuals and organizations exercise core First Amendment free speech rights. Before Congress elects to diminish the First Amendment protections available in this new medium, we believe that careful, public consideration is required.

A. General prohibitions against indecent communications are unconstitutional.

A general prohibition against indecent communications in interactive media would violate the First Amendment to the Constitution of the United States. The principle that each person should decide for him or herself the "ideas and beliefs deserving of expression, consideration and adherence" lies at the heart of the First Amendment. Turner Broadcasting v. FCC, 114 U.S. 2445 (1994) This principle has been interpreted to mean that individuals should be able to speak freely and frankly about issues of their choosing, without fear of reprisal because many people may not agree with or appreciate the nature and content of their messages. At the same time, the Supreme Court has recognized that despite this fundamental guarantee, there are certain kinds of speech that fall into a category of unprotected speech -- obscenity is one such category, indecency is not.

Because of the difficulty in defining obscenity in the context of the First Amendment, it took numerous attempts for the Supreme Court to find five justices to agree on defining principles. Finally, in 1973 the Supreme Court in Miller v. California, established the definition of obscenity and the narrow area of sexually explicit speech that is unprotected by the Constitution. Since that time, the definition has not been expanded or changed.

By contrast, indecent speech which may include important political views, even if crudely stated, is protected by the First Amendment. As such, government cannot enact a ban on such speech without illustrating a compelling governmental interest, and any restrictions on
such speech must be accomplished in the least restrictive manner.

B. Restrictions on indecent communications are unconstitutional for failure to adopt least restrictive means.

1. Censorship of indecent, but not obscene, communications for the purpose of protecting minors must employ the least restrictive means available to accomplish their goal.

Indecent communications are protected by the First Amendment, unlike obscenity which is altogether unprotected. Sable Communications of California v. FCC, 492 US 115; 109 S.Ct. 2829; 106 L.Ed. 2d 93 (1989). Indecent communications, which do not rise to the level of obscenity, can only be limited in order to serve a compelling state purpose and must be done using the least restrictive means possible. Id. at 125. The Sable court found that the protection of minors from access to indecent material is a compelling state purpose, but that "it is not enough that the Government's ends are compelling; the means must be carefully tailored to achieve those ends." Id.

As a threshold matter, the Sable court found that the constitutional basis for upholding indecency regulations in broadcast media articulated in Pacifica Foundation v. FCC, 438 US 726, 98 S.Ct. 3026, 57 L.Ed. 2d 1073 (1978), were inapplicable in any other media besides over-the-air broadcasting. 492 U.S. at 127. Pacifica upheld the FCC content regulation based on the dual finding that 1) radio was a "uniquely pervasive medium" that intruded (dirty words and all) into peoples homes, and 2) the only way to protect children from exposure to objectionable content was to keep it off the air altogether. Sable rejects this finding of "pervasiveness" as "emphatically narrow" and irrelevant to other media such as telephone audiotext services. 492 U.S. at 127.

Thus, the Sable "least restrictive means" standard became the test by which all regulations on access to indecent, but constitutional-protected, material were judged. Nearly ten years of litigation along with adjustment of the statute and regulation were required before the current statute was found constitutional under this standard. See Dial Information Services v. Thornburg, 938 F.2d 1535 (2d Cir., 1991)(finding FCC regulations implementing § 223(b) constitutional). During the course of the dispute over the application of § 223 to audiotext services, courts considered and rejected a number of means by which carriers were required to shield minors from access to indecent information. First, time channeling rules, requiring that services only be accessible during hours when children were asleep, were found to violate the First Amendment because they had the effect of denying access to adults as well as
children. Carlin Communications v. FCC, 749 F.2d 113, 121 (2d Cir. 1984) (Carlin I). Next, the courts rejected a requirement that carriers provide access to indecent services only once customers entered access codes or passwords, which were to be issued after verification that the customer was over 18. Carlin Communications v. FCC, 787 F.2d 846 (2d Cir. 1986)(Carlin II).

The finding of the Dial court, approving the constitutionality of § 223 and associated regulations depended on the legislative determination that the telephone company blocking of service pending age verification or use of a credit card are the only means to enable parents to restrict their children from access to indecent audiotext services.

2. Background on dial-a-porn rules:

As was the case for broadcast indecency restrictions considered in Pacifica, the dial-a-porn restrictions were only found constitutional because of the uniquely intrusive and uncontrollable nature of the audiotext services. A key legislative motivation for imposing these rules during the 1980s was that indecent information available through audiotext services in the telephone system were openly available to children in such a way that it was difficult for parents to control access by their children. The views of Congressman Bliley recounts the prevailing view of the need for the legislation: "It constitutes an attractive nuisance in every home in America where children are present. There is no completely effective way to prevent children from being exposed to "indecent" or "obscene" dial-a-porn so long as it is lawfully and commercially marketed. . . ." Bliley continues:

"Telephones are precisely like radio and television because of their easy accessibility to children and the virtual impossibility for parents to monitor their use . . . . [D]ial-a-porn is presently in the home whether the homeowner wants it or not. Today one cannot have telephone service in the privacy of one's family environment without being required to [have] dial-a-porn with it. Families with children must give up telephone service to be "left alone" from exposure of their children to this intruder."

The current statute and Federal Communications Commission regulations promulgated thereunder were found constitutional after nearly ten years of litigation and efforts by Congress and the Commission to bring the statute within constitutionally acceptable bounds. Indecency restrictions applied to interactive media would require a wholesale review of the constitutionality as applied to new media such as online services and the Internet. Interactive media operates in such a different manner, that the constitutional issues must be considered afresh given the new factual
backdrop. Mere extension of the current dial-a-porn rules to new media would be found unconstitutional in interactive media given the standards set out by the courts reviewing the § 223 rules as they applied to older telephone technology.

3. Reliance on government censorship to restrict access to indecency fails to take into account the fact that interactive media offers parents a much greater degree of control then broadcast services or 900 number services.

Indecency restrictions in interactive media would presumably be motivated by the same goal of protecting minors as the existing statute. However, the means adopted for achieving the goal are impermissible under the First Amendment because they are not the least restrictive means of accomplishing the legitimate government purpose. Interactive media is materially different from analog telephone and audiotext technology in that it offers users the ability to exercise control over precisely what information one accesses. Given the dramatic difference between telephone technology and interactive services such as the Internet and other interactive media, we believe that blocking by the carrier as demanded by § 223 would not meet the "least restrictive means" test. Just as the Sable court found broadcast indecency regulations inapplicable to the telephone system because of differences in the medium, regulations designed for audiotext services in the telephone system are constitutionally inapplicable to new interactive media. Indeed, indecency restrictions on material transport by US Mail have also been struck down by the Supreme Court precisely because "the receipt of mail is far less intrusive and uncontrollable" than broadcast information that was the subject of the Pacifica case.

Technologies already exist that enable users to access certain information based on a variety of characteristics, or, to exclude certain types of information from access. With such filtering technology, users, instead of the government or network operators, can exercise control over the information content that they receive in an interactive network environment. User control could be exercised in two ways. First, one could screen out all messages or programs based on information in the header. If a parent wanted to prevent a child from seeing a particular movie or from participating in a particular online discussion group, then the computer or other information appliance used by the child could be set by the parent to screen out the objectionable content. Such features can often be protected with passwords which would be assigned, for example, by the responsible adults in the house. Second, the same systems can be used to enable blocking of content based on third-party rating systems.

Given the flexibility of interactive technology, we need not rely on just one rating
system. In fact, a single rating system or a single set of filters would merely replace a single government censor with a single private censor, with no real gain for the free flow of information. Properly implemented, interactive media can accommodate multiple filtering systems, giving users and parents the opportunity to select and block information based on a true diversity of criteria. The national Parent Teachers Association or different religious organizations could set up rating systems which would be available on the network to those who desired them. Rather than relying on the judgment of the government, or of the service provider, viewers can limit access to content based on the judgment of a group whose values they share.

Interactive media can enable individuals and parents to prevent themselves or their children from using their PCs or TVs (in particular, their children) from accessing certain kinds of content. With such control mechanisms within the practical reach of parents, the governmental purpose generally cited for indecency regulations -- the protection of children -- could be accomplished without government content restrictions. In particular, the reasoning of Pacifica (unsought intrusion of the indecent message into homes) and Sable (inability of parents to exercise control) would no longer justify most content regulation in new interactive media.

C. Forcing online service providers to become private censors impairs First Amendment values by restricting the free flow of information.

Holding carriers responsible for the content of all information and communication on their systems is a grave policy error which will restrict the free flow of information and is contrary to First Amendment and personal privacy values. If service providers are held liable for all of the content on their networks, then they will be forced to attempt to screen all content before it is allowed to enter the system. In many cases, this would be simply impossible. But even where it is possible, such prescreening can severely limit the diversity and free flow of information in the online world. To be sure, some system operators will want to offer services that prescreen content. However, if all systems were forced to do so, the usefulness of digital media as communication and information dissemination systems would be drastically limited. Where possible, we must avoid legal structures that force those who merely carry messages to screen their content.

Relying on user control is a real alternative to the draconian approach now being considered and sure to be proposed again and again. A media environment in which parents -- or anyone else who has particular preferences about the content of information to which he or she is exposed -- would give users the control that courts have determined they lack in the mass media, without involving the government in content control which we believe would
not survive appropriate First Amendment scrutiny in this new medium.

D. Banning private, sexually-explicit communications violates constitutional privacy rights.

Regulation of private, indecent communications between individuals raises constitutional privacy concerns. The Supreme Court has made clear that absolute restrictions on indecency cannot pass constitutional muster under the Fourth Amendment's guarantee of personal privacy. Though the Court has explicitly recognized that while the government may have an interest in protecting in public, Paris Adult Theater I v. Slaton, 413 U.S. 49 (1973) or in a place that caters to the public, Schad v. Mt Ephraim, 452 U.S. 61 (1981); California v. LaRue, 409 U.S. 109 (1972). it does not have a right to ban information maintained in private. Stanley v. Georgia, 394 U.S. 557 (1969). "If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his house, what books he may read or what films he may watch." Id. at 598. If enacted, the Senate-passed Communications Decency Act would empower federal authorities to intrude on the private communications and information used by individuals, in clear violation of Stanley.

As reflected in passage of the Video Privacy and Library Protection Act of 1988 (protecting records of video rentals), and the Electronic Communications Privacy Act (ECPA) of 1986 (18 U.S.C § 2510), Congress has long recognized the privacy interest in information that we read and otherwise use. A number of surveys have confirmed that Americans care deeply about their privacy. In a 1983 analysis of their survey results, Louis Harris & Associates concluded:

Particularly striking is the pervasiveness of support for tough new [privacy protection] ground rules governing computers and other information technology . . . . This support permeates all subgroups in society and represents a mandate for initiatives in public policy. (L. Harris, The Road after 1984: A Nationwide Survey of the Public and its Leader on the New Technology and its Consequences for American Life, December, 1983).

Enforcement of indecency restrictions by online service providers would require that online service providers violate the privacy rights, and statutory protections established by the Electronic Communications Privacy Act, in order to assure that criminal violations do not occur. ECPA established that users of online communications systems have a substantial privacy interest in the communications that they transmit over computer networks. ECPA also set out clear conditions under which law enforcement agencies, and, in narrow cases, system operators, could access these private communications. Holding system operators
liable would presume a dramatic change in the privacy protected established in ECPA, thereby forcing service providers and system operators to invade the privacy of user communications. While there may be some justification for regulation of communication and information made public, there must be no intrusion on private or closed group communications unless there is evidence of criminal wrongdoing.

E. Constitutional alternatives to the Communications Decency Act censorship regime.

Alternative means of achieving the goal of protecting minors from access to material considered inappropriate by their parents would include:

- Maximum reliance on technology to empower parents: Interactive media offers parents and other users the ability to filter certain kinds of content. Instead of relying on government censorship, or even government-imposed rating systems, parents should be able to block the delivery of certain information to their children.

- Clear protection for constitutionally-permissible speech: Any alternative legislation must provide affirmative protection for constitutionally-permissible speech, even if it is lewd or filthy. Controversial speech must be treated separately than that which is clearly obscene and unprotected.

- Emphasis on enforcement of existing statutes: Federal and state law already prohibits transportation of obscenity, child pornography, as well as, in many instances threats, stalking and harassment. To the extent that there are obstacles to enforcing these laws in the new on-line environment, Congress should examine whether or not more resources for enforcement are required, including training for law enforcement in interactive services and cooperative efforts with the industry.

The regulation of speech, commerce, and privacy rights in new interactive communications systems raises many difficult issues of public policy and constitutional law. Before proceeding with legislation, Congress must provide the opportunity for public hearings to identify clearly the problems that exist, and to identify solutions that are appropriate to the new technology. Failure to do so will result in ineffective policy, years of constitutional litigation, and a disastrous chilling effect on the development and growth of a very promising new communications medium.

NOTES

Disclaimer: This report represents general principles discussed by the Interactive Working Group. The report is not a specific policy statement on behalf of the group or of any
individual organization.

This report was written by: Jill Lesser, People for the American Way Ronald Plessner, Piper and Marbury Daniel J. Weitzner, Center for Democracy and Technology

and edited by: The Center for Democracy and Technology, with detailed comments from a number of working group members.

The Center For Democracy And Technology

1634 Eye Street NW, Suite 1100

Washington, DC 20006

(v) +1.202.637.9800 (f) +1.202.637.0968

For more information,

write webmaster@cdt.org