DOCUMENT RESUME

ED 389 334 IR 055 724

TITLE	Cyberporn: Protecting Our Children from the Back Alleys of the Internet. Joint Hearing before the Subcommittee on Basic Research and the Subcommittee on Technology of the Committee on Science. House of Representatives, One Hundred Fourth Congress, First Session.
INSTITUTION	Congress of the U.S., Washington, DC. House Committee on Science.
REPORT NO	ISBN-0-16-047717-4
PUB DATE	26 Jul 95
NOTE	135p.; No. 16.
AVAILABLE FROM	U.S. Government Printing Office, Superintendent of Documents, Congressional Sales Office, Washington, DC 20402.
PUB TYPE	Legal/Legislative/Regulatory Materials (090)
EDRS PRICE	MF01/PC06 Plus Postage.
DESCRIPTORS	*Access to Information; *Child Welfare; Computer Software; Freedom of Information; *Government Role; *Information Dissemination; Law Enforcement; Obscenity; *Parent Attitudes; Parent Responsibility; Parent Role; *Pornography; Sexual Abuse; Telecommunications
IDENTIFIERS	Congress 104th; Cyberspace; *Internet; Offensive Speech

ABSTRACT

This document presents witness testimony and supplemental materials from a Congressional hearing called to address concerns about the Internet becoming a forum through which minors can be exposed to pornographic or otherwise offensive material. It features opening statements by Congressman Steven H. Schiff, chairman of the House Subcommittee on Basic Research, Congresswoman Constance A. Morella, chairman of the House Subcommittee on Technology, as well as Congressmen Pete Geren and Curt Weldon. Testimony is included from two panels of witnesses. The first includes: (1) Anthony M. Rutkowski, Executive Director of the Internet Society; (2) Ann Duvall, President of Surf-Watch Software, Inc.; and (3) Steven Heaton, General Counsel and Secretary of Compuserve; all of whom offer background information on the nature and structure of the Internet and an introduction to screening software and other technologies that can assist parents in restricting access to obscene material on the Internet. The second panel includes: (1) Mike Geraghty; (2) Kevin Manson; and (3) Lee Hollander; who discuss the law enforcement perspective--the extent to which police and courts can restrict the activities of the purveyors of cyberporn, problematic issues in attempting legal regulation of the dissemination of information, and outlets for cyberporn-related grievances. (BEW)

IR

CYBERPORN: PROTECTING OUR CHILDREN FROM THE BACK ALLEYS OF THE INTERNET

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON BASIC RESEARCH

AND THE

SUBCOMMITTEE ON TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

JULY 26, 1995

[No. 16]

Printed for the use of the Committee on Science

U.S. GOVERNMENT PRINTING OFFICE
93-231 (76) WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-047717-4

COMMITTEE ON SCIENCE

ROBERT S. WALKER, Pennsylvania, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
SHERWOOD L. BOEHLERT, New York
HARRIS W. FAWELL, Illinois
CONSTANCE A. MORELLA, Maryland
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
STEVEN H. SCHIFF, New Mexico
JOE BARTON, Texas
KEN CALVERT, California
BILL BAKER, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan**
ZACH WAMP, Tennessee
DAVE WELDON, Florida
LINDSEY O. GRAHAM, South Carolina
MATT SALMON, Arizona
THOMAS M. DAVIS, Virginia
STEVE STOCKMAN, Texas
GIL GUTKNECHT, Minnesota
ANDREA H. SEASTRAND, California
TODD TIAHRT, Kansas
STEVE LARGENT, Oklahoma
VAN HILLEARY, Tennessee
BARBARA CUBIN, Wyoming
MARK ADAM FOLEY, Florida
SUE MYRICK, North Carolina

GEORGE E. BROWN, JR., California RMM*
RALPH M. HALL, Texas
JAMES A. TRAFICANT, JR., Ohio
JAMES A. HAYES, Louisiana
JOHN S. TANNER, Tennessee
PETE GEREN, Texas
TIM ROEMER, Indiana
ROBERT E. (Bud) CRAMER, JR., Alabama
JAMES A. BARCIA, Michigan
PAUL McHALE, Pennsylvania
JANE HARMAN, California
EDDIE BERNICE JOHNSON, Texas
DAVID MINGE, Minnesota
JOHN W. OLVER, Massachusetts
ALCEE L. HASTINGS, Florida
LYNN N. RIVERS, Michigan
KAREN McCARTHY, Missouri
MIKE WARD, Kentucky
ZOE LOFGREN, California
LLOYD DOGGETT, Texas
MICHAEL F. DOYLE, Pennsylvania
SHEILA JACKSON LEE, Texas
WILLIAM P. LUTHER, Minnesota

DAVID D. CLEMENT, *Chief of Staff and Chief Counsel*
BARRY BERINGER, *General Counsel*
TISH SCHWARTZ, *Chief Clerk and Administrator*
ROBERT E. PALMER, *Democratic Staff Director*

SUBCOMMITTEE ON BASIC RESEARCH

STEVEN SCHIFF, New Mexico, *Chairman*

SHERWOOD L. BOEHLERT, New york
JOE BARTON, Texas
BILL BAKER, California
VERNON J. Ehlers, Michigan
GIL GUTKNECHT, Minnesota
CONSTANCE A. MORELLA, Maryland
CURT WELDON, Pennsylvania
ROSCOE G. BARTLETT, Maryland
ZACH WAMP, Tennessee
DAVE WELDON, Florida
LINDSEY O. GRAHAM, South Carolina
VAN HILLEARY, Tennessee
SUE MYRICK, North Carolina

PETE GEREN, Texas
ALCEE L. HASTINGS, Florida
LYNN N. RIVERS, Michigan
LLOYD DOGGETT, Texas
WILLIAM P. LUTHER, Minnesota
JOHN W. OLVER, Massachusetts
ZOE LOFGREN, California
MICHAEL F. DOYLE, Pennsylvania
SHEILA JACKSON LEE, Texas
(Vacancy)
(Vacancy)

---

*Ranking Minority Member
**Vice Chairman

III

SUBCOMMITTEE ON TECHNOLOGY

CONSTANCE A. MORELLA, Maryland, *Chairman*

SUE MYRICK, North Carolina
KEN CALVERT, California
GIL GUTKNECHT, Minnesota
ANDREA H. SEASTRAND, California
TODD TIAHRT, Kansas
BARBARA CUBIN, Wyoming
JOHN S. TANNER, Tennessee
PAUL McHALE, Pennsylvania
EDDIE BERNICE JOHNSON, Texas
KAREN McCARTHY, Missouri
ZOE LOFGREN, California

CONTENTS

WITNESSES

CYBERPORN: PROTECTING OUR CHILDREN FROM THE BACK ALLEYS OF THE INTERNET

WEDNESDAY, JULY 26, 1995

U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE, SUBCOMMITTEE ON BASIC RESEARCH, AND THE SUBCOMMITTEE ON TECHNOLOGY

Washington, D. C.

The subcommittees met at 9:30 a.m. in Room 2318 of the Rayburn House Office Building, the Honorable Robert S. Walker, Chairman of the Committee, Honorable Constance A. Morella, Chairwoman of the Subcommittee on Technology and Honorable Steven H. Schiff, Chairman of the Subcommittee on Basic Research, presiding.

Mr. SCHIFF. I am going to call the Subcommittees to order and kindly ask the witnesses if they would come to the witness table.

[Pause.]

I would like to welcome everyone here today. We are going to be talking about computers and computer interaction, and particularly that aspect of it called "Cyberporn" for short.

I have a brief opening statement that I would like to read for the record, and then I am going to recognize my co-chairs and ranking Democratic Members for brief opening statements.

I will then offer the opportunity for any other Member to be recognized who wishes an opening statement, but I would strongly encourage Members to submit opening statements for the record which, without objection, will be admitted into the record, because as you know there is scheduled at 11:00 o'clock a joint session of Congress to hear the President of Korea.

I am very hopeful that we can complete this hearing by the time we need to recess to go to the joint session so that the witnesses do not need to remain during that period of time.

I can assure everybody that this is a subject we will revisit in the future, and therefore a relatively short hearing does not express disinterest in the subject, but only a conflict of time immediately.

I am calling this hearing to order and want to welcome everyone here today.

For the future, the Subcommittee on Basic Research will be holding hearings over the next several months on High Performance Computing, Internet Security, and several other issues involving computer technology.

Today we are having a joint hearing with the Subcommittee on Technology, chaired by Congresswoman Morella, on the topic of

"Cyberporn: Protecting our Children from the Back Alleys of the Internet."

Today's hearing is extremely relevant to recent stories in the media concerning pornography on the Internet. In Congress, there is an ongoing debate about how to address this issue in the Telecommunications Bill.

As parents get "on line" to provide educational opportunities, interactive capabilities and the whole world of global computers to their children, they have a right to be concerned about the back alleys, the dark streets, and the criminal elements that roam the Internet.

As the parent of two teenagers with many family issues, I believe parents are best able to decide what is important to their family—not the Congress.

I believe it is appropriate that the Committee on Science play a role in the debate by highlighting what industry is doing in developing technology to address this issue.

In the past when minors wanted to see pornography, they had to visit a bookstore, movie theater, or video store and confront a cashier who would hopefully ask for an ID. Sometimes, however, minors were able to get indecent materials but at least there were minimal safeguards making it somewhat more difficult compared to being able to access pornography in the home over a computer modem.

Parents have always been concerned about what effect exposure to violence and sex has on their children. However, in today's modern society with millions of people having access to the Internet, children are much more computer sophisticated than their parents. And I would add, in my house I know that is true.

While most parents just wish they could set the clock on their VCR, today's kids are exploring higher echelon techniques on how to beat The Mario Brothers.

Parents, already concerned over their own lack of knowledge of computers, start seeing cover stories by major magazines discussing pornography on the Internet. They are developing even greater anxiety as they try to understand the depth and the scope of the problem.

As we sit here today, the debate continues as to how readily accessible is pornography on the Internet.

The purpose of this hearing is to hear from the builders of the Information Superhighway, those who supervise the Highway, and those who enforce the laws of the Highway.

But in the end, just as parents teach their children the dangers of real streets and how to cross them, the same will be true of the Information Superhighway. Parents will have to play a role in what their children are learning and doing on the Information Superhighway.

But I want to add, one of the main focuses of this hearing and of the interest of the Science Committee is what technology can be provided to parents that would provide them the opportunity to limit what their children have access to on using computers at home. And specifically, will parents have the technology available to them which is the equivalent of going to the front desk in a hotel

and saying, "please turn off the X-rated movies which are available in my room."

So I think that is the most important aspect of this hearing, and the direction from the Science Committee. In other words. Can we provide parents some help in supervising what their children are seeing?

[The prepared statement of Mr. Schiff follows:]

Honorable Steve Schiff
Hearing--Cyberporn: Protecting our Children from the Back Alleys of the Internet.

I call this hearing to order and want to welcome everyone here today.

For the future, the Subcommittee on Basic Research will be holding hearings over the next several months on High Performance Computing, Internet Security, and several other issues involving computer technology.

Today, we are having a joint hearing with the Subcommittee on Technology, Chaired by Congresswoman Morella, on the topic of Cyberporn: Protecting our Children from the Back Alleys of the Internet.

Today's hearing is extremely relevant to recent stories in the media concerning pornography on the Internet.

In Congress, there is ongoing debate on how to address this issue in the Telecommunications Bill.

As parents get on line, to provide educational opportunities, interactive capabilities, and the whole world of global computers to their children, they have a right to be concerned about the back alleys, the dark streets, and criminal elements that roam the Internet.

As the parent of two teenagers, as with many family issues, I believe parents are best able to decide what is important to their family-- not the Congress.

I believe it is appropriate that the Committee on Science play a role in the debate by highlighting what industry is doing in developing technology to address this issue.

In the past, when minors wanted to see pornography they had to visit a bookstore, movie theater, or video store, and confront a cashier, who would hopefully ask for an ID. Sometimes, however, minors were able to get indecent materials.

But, at least there were minimal safeguards making it somewhat more difficult compared to being able to access pornography in the home over a computer modem.

Parents have always been concerned about what ffect exposure to violence and sex has on their children. However, in today's modern society, with millions of people having access to the Internet, children are much more computer sophisticated than their parents.

While most parents just wish they could set the clock on their VCR, today's kids are exploring higher echelon techniques on how to beat the Mario Brothers.

Parents, already concerned over their own lack of knowledge of computers, start seeing cover stories by major magazines discussing pornography on the Internet. They are developing even greater anxiety as they try to understand the depth and the scope of the problem.

As we sit here today, the debate continues as to how readily accessible is pornography on the Internet?

The purpose of this hearing is to hear from the builders of the Information Superhighway, those who supervise the Highway, and those who enforce the laws of the Highway.

But in the end, just as parents teach their children the dangers of real streets and how to cross them, the same will be true of the Information Superhighway. Parents will have to play a role in what their children are learning and doing on the Information Superhighway.

COMMITTEE ON SCIENCE
SUBCOMMITTEES ON BASIC RESEARCH AND
SUBCOMMITTEE ON TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C. 20515

HEARING CHARTER

CYBERPORN: PROTECTING OUR CHILDREN FROM THE BACK ALLEYS OF THE INTERNET

JULY 26, 1995
2318 RAYBURN HOUSE OFFICE BUILDING
9:30 A.M. TO 1:00 P.M.

I. Purpose of the Hearing

- To provide Members with a background, an overview, and a demonstration of the Internet. This hearing will be the first in a series of hearings regarding the Internet, HPCC and the information highway, and issues affecting its use and implementation.
- To discover the technologies currently available to assist parents in restricting access to pornographic materials on the Internet.
- To receive testimony from law enforcement witnesses regarding the legal concerns and obstacles in banning or prosecuting obscene or pornographic material transmitted through computer on-line services.

II. Background

This hearing is the first in a series of subcommittee hearings focusing on the Internet and issues affecting high performance computing and communications, and the information highway.

The Internet has become the gateway for information, education, and entertainment. As more and more users participate on the Internet, it is also becoming a forum where children have been exposed to obscene and pornographic material.

This access to pornography has greatly disturbed parents, Congress, and the American public. This proliferation of pornographic and obscene materials available on the Internet is one of most difficult issues confronting Internet use.

Before identifying a new role for government, the hearing provides for a discussion of methods already available in the private-sector marketplace to allow users and on-line service providers to control the types of materials coming into homes, schools, and businesses. The hearing also provides Members with a full understanding of solutions already available in the marketplace and those likely to become available before upcoming Congressional consideration of new government regulation or new criminal laws regarding pornography and the Internet.

To address this concern, commercial on-line Internet providers have been developing new technologies to block access to pornography. These efforts include making available screening software, such as SurfWatch, which prevents the computer on which it's loaded from accessing sites on the Internet known to contain sexual content. This software works by matching a potential Internet destination to a proprietary list of forbidden sites. For example, an attempt to browse through a pornographic Web page results in a screen reading "Blocked by SurfWatch."

Distributing obscene material across state lines, even by computer, is already illegal under federal law, and child pornography in particular is vigorously prosecuted. Since this is a new medium, there may be difficulties and peculiarities involved in its prosecution.

III. Witnesses

Panel One witnesses include representatives of the Internet Society, an on-line Internet service, and a software program company. These witnesses will discuss Internet applications and technology solutions to the unregulated availability of pornography on the Internet.

Panel Two witnesses are representatives from law enforcement. They can discuss law enforcement efforts on the Internet and the problems of prosecuting pornography distributed via this technology.

Congressional Research Service • The Library of Congress • Washington, D.C. 20540-7.

Memorandum July 20, 1995

TO : Committee on Science

FROM : Jane Bortnick Griffith
Acting Division Chief
Science Policy Research Division

SUBJECT : **Background Information on the Internet**

As you have requested, we have prepared a short background memorandum on the Internet for the Committee hearings to be held on July 26. This memorandum addresses those issues which you asked us to provide for Members of the Committee.

Emel Gokyigit provided the research and outlined the issues for this memorandum. If you need additional information regarding background information in preparation of your hearing, please do not hesitate to call me at 707-9547 or Emel Gokyigit at 707-0186.

WHAT IS THE INTERNET AND HOW IS IT USED?[1]

The Internet is an international, cooperative computer network of networks which links many types of users, such as governments, schools, libraries corporations, hospitals, individuals, and others. An immense amount of information is available on the Internet -- speeches by world leaders; full texts of books, (e.g., the Bible, Aesop's Fables, Complete Works of William Shakespeare, Son of Tarzan, Great Expectations, Collected Articles of Frederick Douglass, and many others), magazines, and newspaper articles, medical fact sheets; electronic discussion groups; library catalogs; college courses; recipes; games; Supreme Court rulings; legislation; scientific papers; government documents; music lyrics; software; sports schedules; weather reports; resumes; satellite images; and much more.[2]

---

[1]Portions of this memorandum have been taken from CRS Report 94-471, Welcome to Cyberia: An Internet Guide, by Rita Tehan.

[2]U.S. Library of Congress. Congressional Research Service. Welcome to Cyberia: An Internet Guide, by Rita Tehan. CRS Report 94-471. May 12, 1994.

The Internet is based on a common telecommunications protocol, a standard connection that allows many different types of computers and systems to communicate with each other. The Internet is mainly used to send and receive electronic mail (e-mail), to access remote computers, and to transfer files.

Electronic mail allows users to engage in person-to-person communication by sending electronic messages over the network. Each user is given a unique electronic address where he/she can access these messages. E-mail is also used to join subject-based discussion groups that send out notices and postings electronically. Such discussion groups allow individuals with similar interests to share stories and information. Topics vary from dessert recipes to Hungarian politics.

Internet users can also contact and search other Internet-connected computers. Once a connection is established with a remote computer, users can search that remote system as if their computers were directly wired to it. Users can, for example, view texts and images from the Russian Archives or Vatican Exhibits. In addition, file transfer commands allow users to transfer these textual or graphical files back to their home computers for storing or printing.

Information on the Internet can be accessed in several different ways, of which Gopher and the World Wide Web are the most popular. The Gopher software, originally developed at the University of Minnesota, guides users through a series of menus to reach a computer site containing information of interest. The more recently developed World Wide Web is the most rapidly expanding service within the Internet. The Web includes graphics and allows users to link to other information sites by clicking on highlighted words.

WHO OWNS THE INTERNET?

No single organization owns, manages, or controls the Internet. It is a cooperative fusion of independent networks. Member networks may have presidents or CEOs, but there is no single authority for the Internet as a whole. Substantial influence over the Internet's future resides with the Internet Society, which is a voluntary membership organization whose purpose is to promote global information exchange through Internet technology.[3]

HOW DID THE INTERNET DEVELOP?

The existing Internet in the United States began as a program of the Advanced Research Projects Agency (ARPA, later DARPA), in the Department of Defense. The Pentagon needed a military command and control system that would continue to operate in the event of a nuclear war. The original network, ARPANET, was created in the late 1960s. Its purpose was to allow defense contractors, universities, and DOD staff working on defense projects to

---

[3]Tehan, Welcome to Cyberia.

communicate electronically, and to share the computing resources of the few powerful, but geographically separate, computers of the time.[4]

Today, however, the ARPANET has been phased out and the Internet is supported by numerous large and mid-level private and public networks.

WHO PAYS FOR THE INTERNET?

The major costs of running the network are shared by its primary users: universities, national laboratories, high-tech corporations, and governments. Each institution, organization, corporation, or individual with access to the Internet purchases that access through a Network Service Provider offering Internet access in its area.

Universities, government agencies, and other institutions with direct connections via a mid-level network usually absorb the cost of Internet connections in the data processing budget without charging the costs back to the end users. This is why many Internet users refer to Internet as being "free."[5]

HOW DOES ONE GET ACCESS TO THE INTERNET?

As mentioned above, universities, agencies, companies, and organizations usually provide Internet access to their members free of charge. Individual users who do not have organizational access to the Internet must go through commercial Internet service providers. A number of service providers specialize in providing access to the Internet only. Others, such as Compuserve, America Online, and Prodigy, provide access to the Internet in addition to an extensive array of services in their private networks. Such providers are reached through the use of a modem and a local telephone number.

It is important to note that there are a large number of private networks that are not part of the Internet. Access to these, often also through a local phone number, should not be confused with access to the Internet.

HOW MANY PEOPLE USE THE INTERNET?

In January 1995, the Internet served approximately 4.9 million host computers in 90 different countries. As many as several hundred users may have accounts at a single host. Analysts estimate that some 30 million individuals use the Internet worldwide. The Internet is growing rapidly -- 26% in the fourth quarter of 1994 -- with the World Wide Web representing the greatest growth area.[6]

---

[4]Tehan, Welcome to Cyberia.

[5]Tehan, Welcome to Cyberia.

[6]Internet Society Press Release. 6 Feb 1995.

IS THERE AN INTERNET PORNOGRAPHY PROBLEM?

A certain amount of Internet traffic is pornographic, although the exact amount is unknown and, recently, bitterly debated. Pornography is transmitted on the Internet in different ways. Some mailing groups have pornographic themes, varying from mild erotica to bestiality. The World Wide Web contains sites that have pornographic images, again representing a wide range of practices. Although most pornography sent in the form of e-mail is exchanged between consenting partners, unsolicited pornographic text can be transmitted through this channel.[7] Most pornographic sites have titles representative of their content, such as alt.sex.erotica and are easy to recognize.

A portion of the pornography available in digital form, however, is not on the Internet, but on private bulletin boards that require proof of age and charge fees for membership. This was a source of confusion in the recent debate about the amount of pornography on the Internet.

Analysts and politicians supporting the restrictions on Internet pornography argue that, especially with the introduction of the World Wide Web, finding pornographic text and images is increasingly easier, and that children surfing the Net are likely to come across them, either intentionally or accidentally. Some of this material, they point out, would be considered obscene and therefore illegal in printed form.

Those who oppose restrictions argue that, although some Internet pornography may be classified as obscene, much of the material is just as easily available in book stores, video rental stores, or even libraries. Civil libertarians raise First Amendment concerns about restrictions. In addition, some opponents of restrictions fear that any threat of liability will hurt the development of the Internet.

Although many analysts acknowledge that access to pornography via the Internet is a growing problem, some believe that it can be controlled through technology. Online servers and software companies are developing new technologies to restrict access to pornographic sites. Commercial servers such as Prodigy, Compuserve, and America Online have tried to build safeguards into their systems to catch pornographic material.[8] A new software, Surfwatch, created by a Silicon Valley Firm, blocks access to sites known to contain pornographic material.[9]

---

[7] Steven Levy. No Place for Kids? A Parents' Guide to Sex on the Net. Newsweek, July 3, 1995.

[8] Peter H. Lewis. Helping Children Avoid Mudholes. New York Tines, April 4, 1995, p. c8.

[9] Newsweek, July 3, 1995.

Mr. SCHIFF. I would like to welcome our first panel of witnesses.

Mr. Tony Rutkowski, Executive Director of the Internet Society, who just returned from Sweden, where pornography was addressed as a global issue at the Internet Engineering Task Force Conference. Additionally, he will have a short demonstration on the capabilities of the Internet.

We have Stephen Heaton, General Counsel for CompuServe, the largest on-line provider, who will tell us what they are doing as an industry.

And finally, we have Ms. Ann Duval, president of SurfWatch, a computer software company that has developed technology to assist parents in restricting access to inappropriate material.

Before I recognize the first panel, I would like to recognize the Chairwoman of the Technology Subcommittee who is jointly holding this hearing with my Subcommittee, and the Ranking Members of both Subcommittees.

Mrs. Morella?

Mrs. MORELLA. I want to thank my colleague from New Mexico, the Chairman of the Basic Research Subcommittee, for his leadership on Internet issues and for sharing jurisdiction on this issue so that we can review the technologies that are currently available to assist parents in restricting children's access to pornographic materials on the Internet.

We have heard a lot about it lately. There have been a number of hearings that have been held, and we are going to be focusing on what this technology is that is involved.

I am pleased that we have representatives from computer on-line providers before us this morning. We will also be hearing from law enforcement witnesses on the difficulties which surround the investigation and prosecution of computer crime in general, and specifically, Cyberporn.

The Internet has become the gateway for information, education, and entertainment. It is fast becoming a fixture of our work and personal lives. Yet, as more and more users participate on the Internet, it is also becoming a forum where children have been exposed to obscene and pornographic material.

This access to pornography is greatly disturbing and is one of the most difficult issues confronting Internet use. All we need to do is to review the recent headlines to understand this problem needs to be addressed.

Any one of us, including our children, can pull up on the Internet any time and find a potpourri of images depicting women being abused, being bound, and very explicit sexual acts.

There have been cases of children surfing the Internet to obtain material which they would not legally be able to purchase at a bookstore; of convicted pedophiles soliciting minors for sex; and of children searching what they believe is a Disney bulletin board and inadvertently pulling up pornographic pictures of Disney characters in compromising situations.

Before identifying a new role for government, this morning's hearing provides for a discussion of methods already available in the private-sector marketplace to allow users and on-line service providers to control the types of materials coming into homes, schools, and businesses.

We are being told by the commercial on-line providers that there exists adequate technology to block children's access to pornography, thereby eliminating the need for any Congressional legislation to restrict content and subject matter on the Internet.

So the purpose of this hearing is to have industry inform us of their currently available and developing technologies so that Congress will have a full understanding of solutions available to the marketplace before upcoming consideration of a new government regulation or new criminal laws regarding pornography on the Internet. I do look forward to the testimony of our witnesses this morning.

[The prepared statement of Mrs. Morella follows:]

Opening Statement of
Chairwoman Constance A. Morella

Subcommittee on Basic Research
Subcommittee on Technology

Joint Hearing of the House Science Committee

CYBERPORN: PROTECTING OUR CHILDREN FROM THE BACK ALLEYS OF THE INTERNET

July 26, 1995

I would like to thank my colleague from New Mexico, the Chairman of the Basic Research Subcommittee, for his leadership on Internet issues and for sharing jurisdiction on this issue so that we can review the technologies currently available to assist parents in restricting children's access to pornographic materials on the Internet.

I am pleased that we have representatives from computer on-line providers before us this morning. We will also be hearing from law enforcement witnesses on the difficulties which surround the investigation and prosecution of computer crime in general and, specifically, cyberporn.

The Internet has become the gateway for information, education, and entertainment. It is fast becoming a fixture of our work and personal lives. Yet, as more and more users participate on the Internet, it is also becoming a forum where children have been exposed to obscene and pornographic material.

This access to pornography is greatly disturbing and is one of the most difficult issues confronting Internet use. All we need to do is review the recent headlines to understand this problem needs to be addressed.

Anyone of us, including our children, can pull up on the Internet any time and find a potpourri of images depicting women being abused,

women being bound, and very explicit sexual acts. There have been cases of children surfing the Internet to obtain material which they would not legally be able to purchase at a bookstore; of convicted pedophiles soliciting minors for sex; and of children searching what they believe is a Disney bulletin board and inadvertently pulling up pornographic pictures of Disney characters in compromising situations.

Before identifying a new role for government, this morning's hearing provides for a discussion of methods already available in the private-sector marketplace to allow users and on-line service providers to control the types of materials coming into homes, schools, and businesses. We are being told by the commercial on-line providers that there exists adequate technology to block children's access to pornography, thereby eliminating the need for any Congressional legislation to restrict content and subject matter on the Internet.

The purpose of this hearing is to have industry inform us of their currently available and developing technologies so that Congress will have a full understanding of solutions available to the marketplace before upcoming consideration of new government regulation or new criminal laws regarding pornography on the Internet. I look forward to the testimony of our witnesses this morning.

Mr. SCHIFF. Thank you, Mrs. Morella.

Mr. Geren?

Mr. GEREN. Thank you, Mr. Chairman.

The value of the Internet as an educational resource is enormous. The Internet allows for collaborations and shared learning experiences, provides rural communities with access to teachers in specialized subjects, and provides access to equipment or facilities in remote locations—for example, "virtual" field trips to museums, observatories or science exhibits.

Teachers and parents see the benefits of the technology and have embraced it. Children now have access to these resources both from computers at school and, increasingly, at home.

Unfortunately the Internet is a mixed blessing for children. It has become apparent that objectionable material is also lurking there from which children should be shielded. No one disagrees with this, but the question is, what do we do about it?

Some have advanced proposals that would have the effect of banning all indecent materials on the Internet. This approach may impinge upon First Amendment protections of Free Speech, and is probably unenforceable because of the international reach of the Internet.

Others believe that an open and unregulated Internet is essential for its continued growth and development, and that control of content is unnecessary, because technological means can be placed in the hands of teachers and parents to block access to unsuitable materials.

The basic question for our witnesses is whether technology and existing criminal statutes provide adequate safeguards to protect children who use the Internet.

In particular, is the technology for filtering and blocking unsuitable material readily available, effective, and easy to use, because the kids are usually more computer literate than their parents. I can certainly say that is true in my household. And, are existing laws banning obscenity and child pornography adequate? And can they be enforced effectively in Cyberspace?

I especially invite recommendations for any actions by Congress which are needed to encourage relevant research and development efforts and standards setting processes, or to address any shortcomings in current laws.

Mr. Chairman, I am pleased to join you in welcoming our witnesses this morning and look forward to their testimony.

[The prepared statement of Mr. Geren follows:]

OPENING STATEMENT

HEARING ON CYBERPORN
BY
THE HONORABLE PETE GEREN (D-TX)
RANKING DEMOCRATIC MEMBER
SUBCOMMITTEE ON BASIC RESEARCH

July 26, 1995

THE VALUE OF THE INTERNET AS AN EDUCATIONAL RESOURCE IS ENORMOUS. THE INTERNET ALLOWS FOR COLLABORATIONS AND SHARED LEARNING EXPERIENCES, PROVIDES RURAL COMMUNITIES WITH ACCESS TO TEACHERS IN SPECIALIZED SUBJECTS, AND PROVIDES ACCESS TO EQUIPMENT OR FACILITIES IN REMOTE LOCATIONS -- FOR EXAMPLE, "VIRTUAL" FIELD TRIPS TO MUSEUMS, OBSERVATORIES OR SCIENCE EXHIBITS.

TEACHERS AND PARENTS SEE THE BENEFITS OF THE TECHNOLOGY AND HAVE EMBRACED IT. CHILDREN NOW HAVE ACCESS TO THESE RESOURCES BOTH FROM COMPUTERS AT SCHOOL, AND INCREASINGLY, AT HOME.

UNFORTUNATELY, THE INTERNET IS A MIXED BLESSING FOR CHILDREN. IT HAS BECOME APPARENT THAT OBJECTIONABLE MATERIAL IS ALSO LURKING THERE FROM WHICH CHILDREN SHOULD BE SHIELDED. NO ONE DISAGREES WITH THIS, BUT THE QUESTION IS HOW TO DO IT.

SOME HAVE ADVANCED PROPOSALS THAT WOULD HAVE THE EFFECT OF BANNING ALL INDECENT MATERIALS ON THE INTERNET. THIS APPROACH MAY IMPINGE UPON 1ST AMENDMENT PROTECTIONS OF FREE SPEECH AND IS PROBABLY UNENFORCEABLE BECAUSE OF THE INTERNATIONAL REACH OF THE INTERNET. OTHERS BELIEVE THAT AN OPEN AND UNREGULATED INTERNET IS ESSENTIAL FOR ITS CONTINUED GROWTH AND DEVELOPMENT, AND THAT CONTROL OF CONTENT IS UNNECESSARY BECAUSE TECHNOLOGICAL MEANS CAN BE PLACED IN THE HANDS OF TEACHERS AND PARENTS TO BLOCK ACCESS TO UNSUITABLE MATERIALS.

THE BASIC QUESTION FOR OUR WITNESSES IS WHETHER TECHNOLOGY AND EXISTING CRIMINAL STATUTES PROVIDE ADEQUATE SAFEGUARDS TO PROTECT CHILDREN WHO USE THE INTERNET. IN PARTICULAR, IS THE TECHNOLOGY FOR FILTERING AND BLOCKING UNSUITABLE MATERIAL READILY AVAILABLE, EFFECTIVE, AND EASY TO USE -- BECAUSE THE KIDS ARE USUALLY MORE COMPUTER LITERATE THAN THEIR PARENTS? AND, ARE EXISTING LAWS BANNING OBSCENITY AND CHILD PORNOGRAPHY ADEQUATE AND CAN THEY BE ENFORCED EFFECTIVELY IN CYBERSPACE?

I ESPECIALLY INVITE RECOMMENDATIONS FOR ANY ACTIONS BY CONGRESS WHICH ARE NEEDED TO ENCOURAGE RELEVANT RESEARCH AND DEVELOPMENT

EFFORTS AND STANDARDS SETTING PROCESSES, OR TO ADDRESS ANY SHORTCOMINGS IN CURRENT LAWS.

MR. CHAIRMAN, I AM PLEASED TO JOIN YOU IN WELCOMING OUR WITNESSES THIS MORNING AND LOOK FORWARD TO THEIR TESTIMONY.

Mr. SCHIFF. Thank you, Mr. Geren. Do any other Members seek recognition for an opening statement at this time?

[No response.]

Mr. SCHIFF. Again, written statements will be allowed, without objection, into the record.

[The prepared statement of Mr. Weldon follows:]

July 26, 1995

Joint Hearing
Science Subcommittees on Basic Research and Technology

Statement of Congressman Curt Weldon

As both the father of five and the Chairman of the National Security Subcommittee on Research and Development, I have an interest in the two primary elements of this debate: protecting our children and maximizing the benefits of advancing technology. Just as I have advocated the use of innovative, cutting-edge design to protect our troops from the dangers they may encounter on the battlefield, I feel that we must utilize the latest software design to protect our children as they venture into the front lines of the information age.

I feel that the tremendous information-sharing potential of the Internet will revolutionize communication, education, and even democracy as we know it. It is for this reason that I am now trying to match the enthusiasm that my two youngest have expressed towards computers, and I want to provide to them access to the Internet because of its undisputed educational value. I have also vigorously supported the Global Learning and Observations to Benefit the Environment (GLOBE) program-- an avenue by which many schools have been able to obtain access to the Internet as well as the scientific expertise available on its pages.

The informational empowerment brought about by advancing technology enables individuals to use it as they see fit, and unfortunately, those with deficient codes of decency are equally capable of using it for their own ends. Such is the reason why we must fear our children's exposure to pornographic discussions and graphics, as well as their possible interaction with pedophiles.

As with any powerful tool, if the Internet is used improperly or knowingly abused, the effects can be devastating to innocent others. There is no one more innocent than our children and I would like to keep them that way. Although there may be some doubts as to the extent to which pornography pervades the digital codes of the Internet, I want to have the ability to protect my children from such immoral influences.

I am supportive of the software industry's initiatives to empower parents and enable them to protect their children from the inevitable dangers of the Internet. As a parent, I know that the number one priority is to protect your children from known dangers. Unfortunately, the rampant computer illiteracy of parents renders them helpless as they try to comprehend the Internet and its inherent dangers to children. Filter software packages like "Surfwatch" and the cooperation of the popular servers such as Prodigy, America On Line, and Compuserve, are invaluable to parents with limited computer skills.

Obscenity has always been difficult to define. The community standards that have developed and been recognized by the courts are tenuous enough, and the wonders of interactive media transmitted across state lines further complicates this issue. What is acceptable in Times Square may is certainly offensive to most of my constituents. The advent of the Internet makes the simultaneous display of material in both of these venues possible, having a very different response by each audience. Through the empowerment of the

family, the foundation of any community, we can keep obscene material out of our homes.

I support government involvement in the Internet, but only to the extent of enhancing its interactivity with the people. I have established an e-mail address as an additional communication line to my constituents, and I fully support House efforts to make our activities known and available to the people via the Internet. Such is the proper role of government in the Internet, and not as a heavy-handed body attempting the impossible task of policing the international Internet. It is unfortunate that with all of the promise of the Internet, we must focus upon the development of such a negative aspect. However, it is important for the government to make the people aware of the existing dangers, and ensure that the tools for combating these threats are readily available.

I will continue my involvement in the Internet as both a father and a Congressman, and I believe that through both the initiatives of industry and the responsible role of the family, we can neutralize the negative aspects of the Internet, leaving only its tremendous positive potential.

Mr. SCHIFF. One more item here before I go to the witnesses. That is, if you have never seen a Congressional hearing before, our comings and goings may be a bit disconcerting. The fact of the matter is, there are a number of matters happening at the same time oftentimes in the Congress, and in fact, I have another hearing to attend a little bit later and I will be turning the Chair over to Mrs. Morella in a little bit myself.

But what I want to let you know is that the main purpose of a hearing is the record of the hearing that is being made by the Court Reporter. In due course, all of the testimony that is being made today will be made available to all Members of Congress. So the intent of what the hearing is all about is accomplished, and I want to make sure that everybody realizes that.

We have just been joined by the Chairman of the Science Committee, Congressman Walker. Congressman Walker, do you desire to make any opening statement?

The CHAIRMAN. No, thank you.

Mr. SCHIFF. With that, I understand that we are beginning, Mr. Rutkowski, with you with a demonstration. So if I can ask someone to dim the lights, we can proceed.

[Computer visuals are shown:]

STATEMENT OF MR. TONY RUTKOWSKI, EXECUTIVE DIRECTOR, INTERNET SOCIETY, RESTON, VIRGINIA

Mr. RUTKOWSKI. Good morning. I would like to express my thanks to the Chairs of this hearing, the Subcommittee, and the staff for their positive contributions in dealing with the subject, the excellent preparations, and my opportunity to assist you here.

I am Executive Director of the Internet Society. However, I am not speaking on behalf of the Society, which is a nonprofit international organization for coordinating and educating for the Internet, and with members in more than 125 countries, it doesn't normally intervene in formal domestic proceedings. Rather, I am here as an engineering, legal, business, and public policy expert well known in the field.

In addition, I suppose we are a "power user family" with an Internet local network in our home, to which my wife and young children and I have access from our respective rooms—we haven't yet figured a way to provide our dog Sasha with a machine. My wife also publishes the leading K-12 newsletter for schools, actually.

At the request of the Subcommittees' staff, I have assembled the latest information on four topics:

What is the Internet and what is it not?

What are the Internet's directions and resulting implications?

How is it actually used?

What recent developments are occurring which allow reader selectivity in accessing materials?

To help the Subcommittee appreciate the global scale and power of the Internet, I am showing the slides which accompany my remarks from an Internet-based World Wide Web server, which is also providing the information to the public worldwide, a copy of my written submission with built-in slides and links to the many subjects mentioned. Millions of people from nearly 100 countries

have potential access. This took but a few hours to accomplish and can be hosted on machines as small as this little one kilogram notebook computer that I usually carry around with me on trips.

The basic idea is you can go literally anywhere in the world with something this small, plug it into the Internet and actually be a service provider of information. But what is the Internet and what is it not?

Admittedly, computer networking is about as mystifying to most people as gazing at the cosmos. Perhaps that is why it is convenient to lump it all under the term "Cyberspace." However, the basics are pretty simple.

The Internet can be visualized as 7 million computers of all kinds seamlessly connected around the world in a big cloud of 60,000 largely private networks. It allows any one of the computers to share information or resources with any other, just like we are doing here now.

It runs over virtually every kind of underlying telecommunications medium known to humankind. Sometimes it is said that the Internet runs over everything except wet string.

However, there are other kinds of services and networks in Cyberspace that are not the Internet. This includes the On-Line providers, Bulletin Board Service providers, and a wide variety of other computer networks.

Increasingly, many of these other entities have gateways to the Internet so that things like E-Mail can go between them. However, these services and networks are not the Internet.

This is particularly relevant to the subject matter before the Committee. Any cursory survey of popular computer magazines today makes it clear that a significant amount of the potentially offending material is on separate DBS systems dialed up over the telephone, or even on CD-ROMs distributed through the postal system and not the Internet. What are the features and implications here?

The most basic one is that it is highly distributed, largely in private hands, with about half located outside the United States.

The data is also broken into separate packets and routed automatically through thousands of potential paths by a self-managing intelligent agglomeration of networks distributed around the globe. It is collectively maintained by the hundreds of access providers and literally the millions of users.

Governmental regulation of the Internet in conventional terms is probably not possible and fraught with enormously complex international effects and difficulties.

Certainly making Internet service providers responsible for the content of traffic would be utterly vicarious since they are simply passing someone's digital bits from one point to the other.

On the other hand, the Internet in the final analysis is a transparent communications medium and the entire panoply of criminal and civil law still apply to activities of end users to control the egregious conduct of the few. And I believe that is what is going to be visited in the second panel. What are the directions of the Internet?

Well, it is certainly growing. For the past decade the growth has been exponential, doubling every year. By the year 2000, 120 mil-

lion computers are likely to be Internet-connected. This is occurring also in every region of the world, modulated by factors such as government policies, available capital, open competitive markets, and computer skills.

The Internet has developed and grown as a very large scale, bottom-up infrastructure capturing the enormous energy and creativity of grassroots institutional individual initiative and investment.

It has been aided also by long-standing Telcom and trade policies that have eschewed any Internet regulation and pursued telecommunications policies that ensured access to telecommunication facilities and pushed down prices of leased and access lines.

The Internet's growth trends seem destined to continue with dramatic increases in PCs and workstations, service providers, low-cost networking hardware, and all the things that go into making the Internet grow worldwide.

The Internet has, in the final analysis, become the ultimate global engine for collaboration, education, research, development, information sharing, now marketing, sales, and correspondence—an important point, especially between dispersed family members and friends. How is the Internet used?

I think there is a lot of misinformation here. It is possible on a service level to measure what occurs on major trunks of the Internet, and we have provided as a graphic a snapshot of the February, 1995, traffic on the principal backbone and shows quite graphically how all those Terabytes are being used.

The biggest single use is a gaggle of more than one thousand largely special or experimental services. After this, transferring files—primarily software—is the largest use. Increasingly small portions consist of World Wide Web browsing, Newsnet, E-mail, remote computer access, gopher browsing, name lookup, and interactive chat.

Only a minuscule part of this overall traffic could consist of possibly objectionable material primarily from a few World Wide Web sites and NewsNet topic groups. Recent purported data to the contrary has been subsequently shown to be misleading and inaccurate.

The overwhelming use encompasses collaboration, communication, and development activities of importance to every component of society. Indeed, with the recent emergency of secure financial transaction techniques, coupled with the more than 70,000 commercial domains now registered, the Internet is certainly poised to emerge as a major backbone of the global economy.

Until recently, the Internet was the province of researchers, educators, and product developers. It revolutionized how people think and work together, and how information is shared. This all occurred because the technology and style is open. Everyone cooperated to operate and constantly developed a vast high performance network and shares resources.

However, as we have entered a new phase of widescale public Internet growth and access, this openness has resulted in sharing and distribution of some materials that people find objectionable—especially where children are involved.

Even though this represents a very small part of Internet use, and such materials are generally available even more readily

through other means, and more effective parental supervision would minimize access, it does pose a concern and a challenge to the Internet development community.

The IETF, The Internet Engineering Task Force standards organization, held a special session in Stockholm last Wednesday, in fact, to discuss for the first time approaches to dealing with this children access concern through the development of reader selectivity techniques.

It took steps to establish a new working group to develop necessary standards. Several dozen experts from around the world explored a variety of different options and some interesting new test bed tools were demonstrated.

I would point out to the Committee, by the way, one of the most interesting of the tools actually is being developed by the Los Alamos National Labs' Application Center, which I believe may be a part of your funding. I think it is an excellent example of how science funding has actually added useful tools in this area.

Considerable work is also being pursued in the World Wide Web Consortium standards organization by a variety of software vendors and in research labs.

Potential problems were raised such as the need for effective authentication and fraud prevention, as well as the abuse of the filtering tools by governments and groups that may define "objectionable" in political, cultural, and religious terms.

The Subcommittee should be aware that there are four broad categories of tools and many different options within each, and additional details can be found in my written testimony.

Some of the other witnesses here today will discuss some of the initial tools that are available on the market. The most sophisticated of these under development would allow fine granularity in tailoring reader criteria and subject matter, and even support multiple third-party rating services so that people could select favorite social, religious, or even political rating services as the basis for their filtering material.

In summary, I conclude by reiterating that the global growth and evolution of the Internet are occurring at hyper speed. As problems have arisen, the Internet development community has responded with effective solutions.

Objectionable materials in fact constitute a very minor part of the real Internet environment. Access to and distribution of such materials can be addressed with existing laws, emerging reader selectivity solutions, and effective industry action.

Legislative and regulatory approaches attempting to deal with such a complex global and dynamic network environment are unneeded, unlikely to be effective, and may engender adverse international consequences if multiple jurisdictions around the world all embark on such initiatives.

Almost two decades ago worldwide cooperation, collaboration, and ultimately the global economy were threatened by misguided attempts to regulate the free flow of information.

Subsequently, the Internet emerged to demonstrate that an open global information network unregulated by government and institutions is an extraordinarily valuable and positive asset for everyone.

The Subcommittee and Congress should be concerned that the near-term focus on children's access to information does not result in long-term adverse effects that impact an open global society.

Thank you.

[The prepared statement of Mr. Rutkowski follows:]

93-231 95 – 2

The Global Internet

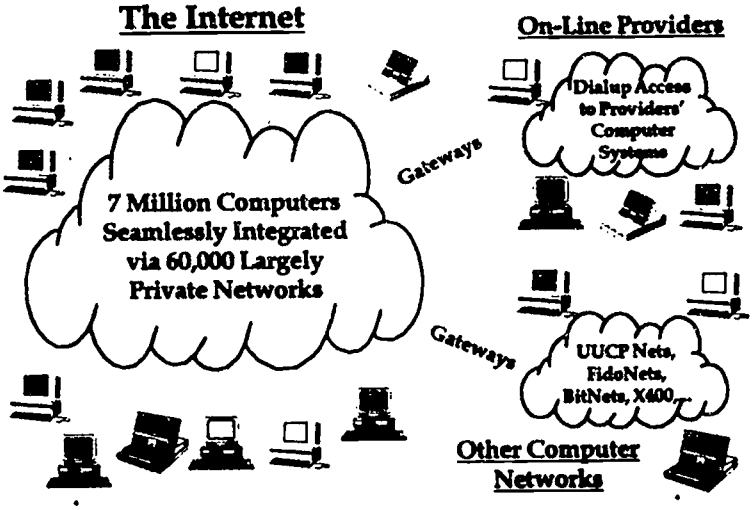
and New Developments in Reader Selectivity Tools

U.S. House of Representatives
Committee on Science
Hearing on 26 July 1995
Washington DC USA

Anthony M. Rutkowski
Executive Director
Internet Society*
Reston VA USA

* Statements are not presented as those of the Society - an international educational organization

What is the Internet? and Not



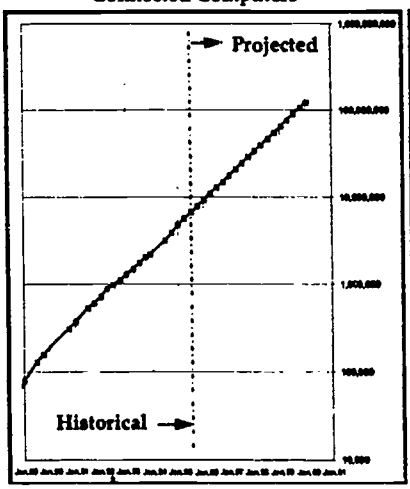
Internet Features - Implications

- Highly distributed throughout the world in largely private hands
- Fostered by government non-regulatory policies
- Operates over every kind of infrastructure: local networks, telephone, ISDN, CATV, wireless, cellular, private and common carrier fiber, satellite, submarine cables, and wetstring (not)
- Traffic dynamically routed

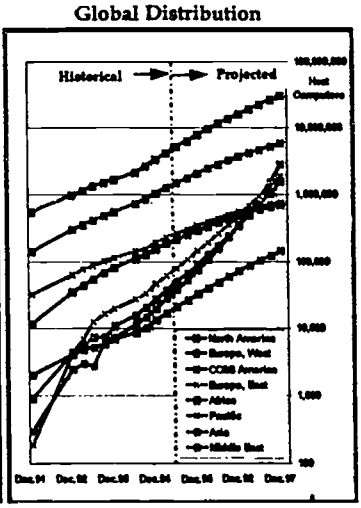
- Difficult to regulate by government dictate or consonant with longstanding deregulation policies
- Significant international effects and complexities
- Criminal and civil law already applies to end user behavior
- Not possible for network operators to be aware of content

Internet Growth Trends

Connected Computers



Global Distribution

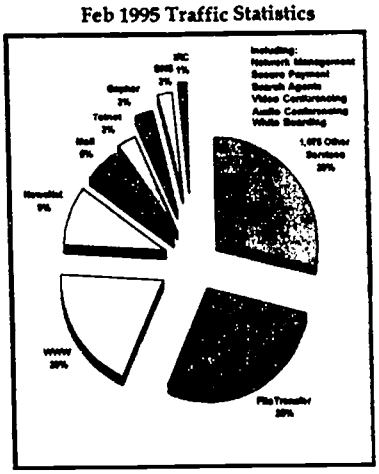


Internet Global Growth Drivers

- Computers diffusing faster than any previous communication technology
- Internet plug-and-play being built into all computers
- Internet built into local, home, and enterprise networks
- Global trade and telecom liberalization
- Internet access by hundreds of providers via every possible medium
- Simple user interfaces
- Constant neat new tools
- High performance at low cost
- Ultimate global engine for collaboration, education, research, development, information sharing, marketing, sales, and correspondance
- People enjoy networking with others

How is it used?

Feb 1995 Traffic Statistics



- Information Sharing
- Global Collaboration
- Distance Education
- Software Distribution
- Scientific Research
- Product Development
- Public Services
- Marketing
- Sales
- Customer Support
- Professional Development
- Correspondance
- Entertainment

Content Problems

- Widescale public Internet growth and access has inevitably resulted in sharing and distribution of some *objectionable* materials
- It represents a very small part of Internet use
- Such materials are generally available even more readily though other means
- Effective techniques and tools are being rapidly devised by the Innovative Internet development engineers to enable reader selectivity of Internet based materials
- However, the techniques and tools themselves may be abused as different governments and groups define *objectionable* in political, cultural, and religious terms
- The Internet development community is deeply concerned that such abuse could significantly diminish the spirit of open global communication across all boundaries that has marked the Internet

Enabling Reader Selectivity

- **Standards and development activities**
  - Internet Engineering Task Force, Stockholm, July 1995
  - World Wide Web Consortium, Cambridge MA
  - Vendor products and research programmes
- **Scope of activity**
  - WWW only
  - Multiple services
- **Additional uses**
  - Efficient information discovery
  - Copyright enforcement
- **Effectiveness**
  - Some tools can be defeated
  - Authentication techniques will help
- **Fraud potential**
  - Authentication of labels will require enlightened national encryption policies
  - National trademark agencies may need to certify rating organizations
- **Abuse potential**
  - Political, religious and cultural controls
  - Use to purposely select objectionable material

Reader Selectivity Techniques and Tools

- **Host Access Control**
  - Two alternatives: exclude access to known objectionable material, or allow access only to acceptable material
  - Features: Poor granularity and hard to maintain, but quickly implemented
  - Examples: Surfwatch, caching proxies
- **Information filtering using source labels**
  - Features: fine granularity, easy to maintain, but relies on the source
  - Examples: First Virtual/Nathanial Borenstein KidCode, initiatives from WWW Consortium
- **Information filtering using ratings from third party**
  - Features: Fine granularity, allows multiple specialized groups to enter ratings business, but difficult to maintain
  - Examples: Los Alamos National Labs has Sun Hot Java based prototype; Dirk-Willem van Gulik implementation in Europe
- **Other alternatives**
  - Bandwidth and machine saturation
  - Industry/provider code of conduct and enforcement
  - Password accounts
  - Credit card access
  - Material encryption

Summary

- The global growth and evolution of the Internet are occurring at hyper speed
- As problems have arisen, the Internet development community has responded with effective solutions
- Objectionable materials in fact constitute a very minor part of the Internet environment
- Access to and distribution of such materials can be addressed with existing laws, emerging reader selectivity solutions, and Internet industry action
- Legislative and regulatory approachs attempting to deal with such a complex, global and dynamic network environment are unneeded, unlikely to be effective, and may engender adverse international effects

Before the

U.S. House of Representatives
Committee on Science

In the matter of	)
	)
The Internet	)
and the	)
Management of	)
Objectionable Materials	)

Hearing on 26 July 1995

Testimony of Anthony M. Rutkowski

Although I am presently Executive Director of the Internet Society, I am not here representing the Society or its views. My remarks are those of an expert witness with more than 30 years experience in many facets of the telecommunication and computer networking industries in the private sector, U.S. government, intergovernment, and academia, domestically and internationally, with an education in both engineering and law. (See Annex 1) The Society is the principal international organization for cooperation and education in the Internet global community, with more than 6000 individual members in 125 countries, and 120 organizations. As an international organization, it doesn't intervene in domestic proceedings.

My purpose in this hearing is to provide the Committee with current basic information in five areas:

- What the Internet is - and is not
- What are the basic trends and drivers of the Internet
- How is it used
- How content problems are being addressed
- Some of the long range problems posed by potential government action

A set of graphics accompany this testimony, and both can be found on the Internet at http://www.isoc.org/rutkowski/hr_hearing.html

Preface

At the outset, it is important to emphasize that the Internet over its entire existence was devised and evolved as a global open medium for researchers, professionals, educators, business, and the public sector to share information and collaborate, to understand and help each other, to effect a global economy. The Internet has been a bubbling cauldron of ideas, innovation, and fast-paced development since its inception. More than just a technology or an electronic medium, it is a vast global "mind meld" where the principal assets are people working and thinking together. It is the principal example not only of what is termed Global Information Infrastructure, but also what Wall Street financier-philanthropist George Soros has called The Open Society.

This openness and dynamism free from the fetters of governmental regulation has been enormously successful by any measure. It has markedly enhanced science worldwide - with estimates

that 70% of all the scientists who have ever lived are now accessible via the Internet. As a marketplace, internet products and services now produce revenues approaching US$6 billion.

The robust open market and institutional freedom of the Internet have incented its thousands of developers not only to devise new tools, but also to fix problems - rapidly and effectively. New efforts are now underway to fix the current problem of an Internet being used by a comparative handful out of the tens of millions of users - some with malicious intent - to disseminate materials that others may find objectionable, particularly for children. The solutions are in the form of elegant new reader selectivity techniques and tools that can allow individuals or custodians to preselect available information based on labels or third party ratings.

However, like many tools, there is a dark side with long-term implications. The actions of a comparative few abusers of the Internet and the surrounding hype have the potential of diminishing the long-term global openness of the medium, as regimes and institutions define "objectionable" in narrow political, cultural, or religious terms. Scientific research, worldwide open society and international human rights are potentially losers in the process. This should equally concern Congress.

What the Internet is, and is not

Most people who are not initiated into today's ultra-tech, jargon-filled environment understandably find the Internet as mystifying as the cosmos. Perhaps that's why it all disappears under the convenient rubric of *Cyberspace*. The terms are not the same.

The Internet consists of approximately 7 million computers seamlessly integrated using a common technology via 60,000 largely private networks. A little less than half of those computers and networks exist outside the USA - spread among 100 different countries. There are currently several hundred commercial firms worldwide that specialize in providing interconnection into the global internet. This agglomeration of millions of computers is a direct descendent from the original Internet assembled by the U.S. DOD in the late 70's and early 80's, and allows any one computer to have immediate and direct (but controlled) access to any other connected computer, its information, and certain processes. What those computers and their users can accomplish is limited only by the kind of computer applications on the machines.

The Internet's key features are very significant. It is highly distributed throughout the world, and the computers and networks are overwhelmingly in hands of literally millions of individuals, companies, and institutions. It was fostered by decades of government policies - domestically and internationally - that left computer networking wholly to a highly competitive marketplace and individual initiative, and is referred to as "bottom-up infrastructure." It operates over virtually every kind of underlying means, including: local networks (LANs), telephone lines, ISDN, CATV, wireless, cellular, private and common carrier fiber, satellite and submarine cable circuits. A common joke is that "the Internet runs over everything except wet string." The Internet operates as a highly distributed intelligent network that can automatically learn and adapt to dynamically route traffic over myriad alternative routes. A message or even pieces of a message may go different paths to an end destination at any time.

Enterprise Internets, which use the same technology, also exist on a large scale in many commercial and governmental institutions. There are hundreds of thousands of such networks. However, they are not generally publicly accessible and thus probably not relevant to the Committee's hearing, but indicative of the complexity of the environment.

On-Line Services are stand-alone commercial offerings of providers that allow their customers dialup access to their computer systems and a variety of fixed services on those computers. These exist separately from the Internet - although most of them can now exchange at least Email to the Internet via gateways. ***Bulletin Board Services*** are similar to On-Line Services, but generally operate at the community level on a relatively small scale, and most are not presently connected to the Internet, although this is changing rapidly as most new BBS software has Internet access built-in.

Other computer networks exist on a large scale, and have gateways to the Internet - largely for just EMail. These include, for example, UUCP networks, FidoNets, Bitnets, X.400 networks. Many of these are still used extensively in developing countries, where they were built using available computers and dialup telephone lines. However, low-cost Internet technology has recently become available and is now being implemented in many poor countries and regions. X.400 is principally a telephone company commercial Email service.

Cyberspace, by contrast, consists of all of the above, arguably including even stand-alone computer systems that may access materials physically transported by CD-ROM, diskettes, and tape.

Policy Implications

There are several basic policy implications that flow out of the fundamental nature of the Internet and the environment in which it has emerged.

Perhaps foremost, it would be exceptionally difficult for government at any level to actually govern operation and use, or dictate conduct that applies to the Internet as a medium. It is a massively shared, constantly evolving, global system for which the only model of comparable complexity may be the global economy. Furthermore, a 30 years legacy of basic regulatory policy at national, regional and international levels have proceeded on the premise that government should forebear from regulating the computer networking business. This includes the FCC's Computer I, II, III trilogy, the European Union's *Green Paper*, and the World Trade Organization GATS treaty. Indeed, the growth and dynamics of computer networking environment have confirmed the wisdom of those policies.

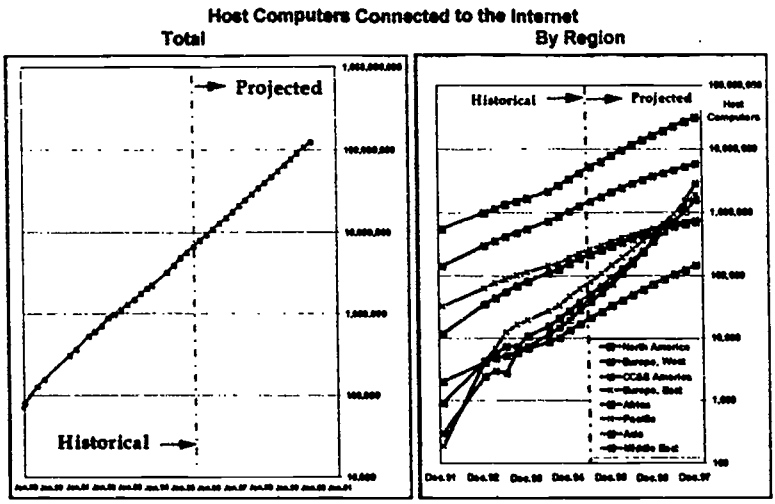
Furthermore, any exercise of legal jurisdiction and application of the different laws of potentially many jurisdictions in a massive network of constantly communicating computers spread among most of the countries of the world creates an instant Conflict of Laws nightmare. Such action would also induce similar actions by multiple jurisdictions that would lead to ever more complexity and conflict.

Because Internet traffic is dynamically routed in packets over multiple networks and paths, it's not feasible for any operators to be aware of the traffic content. In many cases, this inability to be aware of or to control content also applies to the services provided on the attached host computers. Imposing responsibilities on such providers for the passive passage of traffic would be utterly vicarious.

Lastly and perhaps most importantly, the Internet is simply a human communications medium, and all the existing civil and criminal law throughout the world still applies. Indeed, with the Internet increasingly interoperating with other media such as fax and even voice telephone services, it's becoming meaningless to distinguish among media. Civil and criminal actions have been brought in matters involving espionage, tort, libel, fraud, distribution of obscene materials, among others. Apart from the intractable problem of a lack of rules for resolving Conflict of Laws in this arena, it appears that existing law would suffice.

Internet Scaling and Growth Drivers

In dealing with the Internet, it's important to understand its dynamics and directions. Because it is essentially a seamless mass of computers distributed globally, key trend charts are those that depict the overall history and projections for connected machines, and those trends in different world regions.



At present there are about 7 million computers indicated as reachable on the Internet. The growth has been consistently doubling every year for the past several years. Conservative projections based on the actual average growth over previous three years indicate about 120 million connected machines at the end of the decade. Although North America has the largest number of connected computers, the trends are quite amazingly similar in other regions of the world - even if the numbers are smaller. In general, the aggregate growth outside the USA is greater than inside the USA, thus assuring a continual globalization of the network.

It seems likely that these growth projections will materialize. The optimism derives from a number of developments now underway that all converge to further the Internet phenomenon.

A major computer system vendor has publicly noted that computers - as a communications technology - are growing and diffusing worldwide faster than any previous communications medium, including telephones, television, or VCRs. There are now about two hundred million computers and the number proceeds inexorably upward. Thus there are a constantly expanding number of machines that are potentially able to be Internet connected.

The ability to connect a machine to the Internet is affected by several factors: the physical components in the computer, the operating systems, and the ready availability of cost-effective access service. In the past year, good high performance network cards and modems have become so inexpensive that they're routinely shipped with increasingly large numbers of computers. Even more importantly, the Internet has become so popular that the necessary access software has been included with virtually all new computer operating systems, and large numbers of companies worldwide in almost every form and using almost every kind of access medium have become Internet Service Providers of network access.

The stage for entering the Internet provisioning business has been set by an array of telecommunication and trade policies that have liberalized the use of telecom networks, driven the price of circuits down, and eliminated or diminished restrictions on providing enhanced or value added network services - the regulatory category into which the Internet falls. The bottom line -

it's easy to enter the Internet access business, and to offer customers high performance at low cost - usually at flat rates based on the access bandwidth provided.

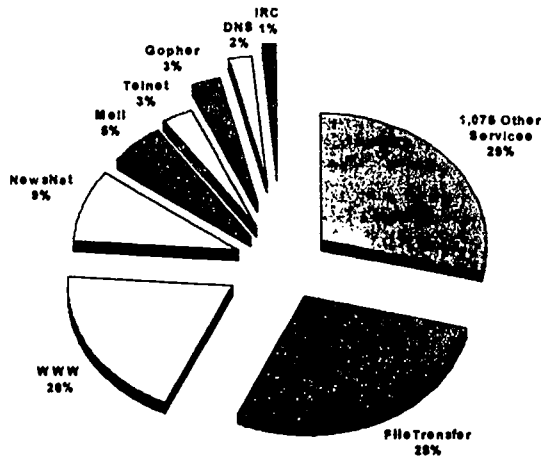
Meanwhile, a combination of innovative genius that resulted in such developments as the World Wide Web (WWW) and the Mosaic browser, as well as elegant user-friendly point-and-click tools inspired by the growing market, has enabled almost anyone over the age of five to use at least some of the Internet's capabilities.

The development of new tools has not stopped. With almost each passing day, new techniques, new software, new capabilities become available - usually on the network itself. The Internet has become the ultimate computer development engine for producing new applications, while all of its non-"geek" users avail themselves of a constantly expanding array of new capabilities to better collaborate, educate, do research, share information, market, sell, and correspond.

Perhaps underlying the Internet phenomenon is an intrinsic desire of people in the world to interact with others - near and far. For many families with college-age members, it has become a vital link between parents and children. For anyone with a global perspective, profession, business, or life-style, the Internet has become the most unifying personal medium of our age.

How is the Internet Used?

Although it isn't feasible to examine specific content on the Internet, it is possible to objectively look at what occurs across major Internet backbones in terms of services transpiring. Such a snapshot from February 1995 reveals that 1,090 different services were supported via a major USA backbone. They cover the gamut of operational and experimental, file transfers, information browsing, messaging, and even television-like multicasting



These services provide tens of millions of people with capabilities such as information sharing, global collaboration, distance education, software distribution, scientific research, product development, public services, marketing, sales, customer support, professional development, correspondence, and entertainment.

Only a minute fraction of this traffic is even potentially related to the transfer of objectionable materials, and recent assertions of significant transfer of "Cyberporn" on the Internet are totally misleading and contrary to the facts - evincing a profound ignorance about what even constitutes the Internet. (See Annex 2.)

This is not to say that on some of the Internet's 7 million computers, there aren't some publicly accessible offensive materials, or that some messages don't convey such materials. As the Internet continues to scale to encompass an ever larger slice of the general public worldwide, it is inevitable that some materials will exist that some individuals or groups will find offensive. It's just that the numbers are proportionally very small and likely to remain that way. It's also worth emphasizing that a significant amount of such material is actually made available via dialup computer Bulletin Board Services (BBS), and not the Internet.

Problems and Solutions - Enabling Reader Selectivity

Even though the distribution of objectionable materials is small, and can be lessened relatively easily through such common sense approaches as greater supervision of children by their parents, guardians, or teachers, there remains a clearly recognized need to provide effective tools to do this automatically. This has resulted in a wealth of new activities and solutions referred to here as *enabling reader selectivity*.

The most recent and largest scale of these activities was a special session last Wednesday at the 33rd Internet Engineering Task Force (IETF) meeting at Stockholm. The IETF is the international standards organization of the Internet. The special session was chaired by Internet pioneer Vint Cerf, and brought together several dozen experts from around the world to discuss their concerns and potential solutions. The occasion also provided opportunities for separate meetings and demonstrations of ongoing work. The session resulted in a proposal to create a new IETF Working Group directed toward developing necessary technical standards over the next six months.

In addition to the IETF action, the World Wide Web Consortium in Cambridge MA also announced its establishment of technical standards initiatives focused on WWW-based services. It was also apparent that several vendors have implemented initial products and that product development was underway in at least two research establishments.

Summary of Reader Selectivity Techniques and Tools

- **Host Access Control**
  - Two alternatives: exclude access to known objectionable material, or allow access only to acceptable material
  - Features: Poor granularity and hard to maintain, but quickly implemented
  - Examples: Surfwatch, caching proxies
- **Information filtering using source labels**
  - Features: fine granularity, easy to maintain, but relies on the source
  - Examples: First Virtual/Nathanial Borenstein KidCode, initiatives from WWW Consortium
- **Information filtering using ratings from third party**
  - Features: Fine granularity, allows multiple specialized groups to enter ratings business, but difficult to maintain
  - Examples: Los Alamos National Labs has Sun Hot Java based prototype; Dirk-Willem van Gulik implementation in Europe
- **Other alternatives**
  - Bandwidth and machine saturation
  - Industry/provider code of conduct and enforcement
  - Password accounts
  - Credit card access
  - Material encryption

The work is divided into four broad areas. The first - host access control - has actually produced products now on the market. These are effective, but have poor granularity (i.e., entire sites are either included or included), and are difficult to maintain because they require constant searching and updating by the vendors.

The second approach (also called 2nd party labeling) potentially allows individual files or pages of materials to be rated and filtered. It also relies upon the source to label the materials, and thus is easily maintainable. Non-labeled materials can be excluded.

The third approach allows 3rd parties to maintain labeling services. Thus one could potentially subscribe to a favorite commercial, educational, church or political rating service. However, this transfers a significant maintenance responsibility to that service.

The fourth category is a set of approaches that rely on different existing effects of techniques to limit access.

The Committee should note that the second or third approaches invoke some ancillary public policy considerations. For source labeling to be really foolproof, it will require the use of encryption-based authentication technology now subject to export controls and usage restrictions in some countries. The third approach - 3rd party labeling - will require some certification of institutions to be foolproof, and a role for the Patent and Trademark Office might be considered to assure that only one legitimate rating organization with the same name exists.

Much of this work has an additional positive benefit of bringing about more efficient discovery of information, and possibly assisting in the enforcement of copyright claims. On the negative side, however, concerns exist about the abuse potential of the tools by those intent upon instituting political, religious or cultural-based controls on a population, as well as those who might purposely select objectionable materials.

Summary

The global growth and evolution of the Internet are occurring at hyper speed. However, as problems have arisen, the Internet development community has responded with effective solutions. Objectionable materials in fact constitute only a very minor part of the Internet environment. To the extent this problem exists, the access to and distribution of such materials can be addressed with existing laws, emerging reader selectivity solutions, and Internet industry action. Legislative and regulatory approaches that attempt to deal with such a complex, global, and dynamic network environment are unneeded, unlikely to be effective, and may engender adverse international effects.

Annex 1
Anthony Michael Rutkowski

Tony Rutkowski was named Executive Director of the Internet Society in February 1994 after serving as Vice-President and founding trustee for two years. He created and scaled its international secretariat, developed its mission, and directs the continuing affairs of the organization. The Society is the global international organization which fosters the development of the Internet technologies, networks, applications and use. The Society's membership consists of thousands of individuals and 130 companies, non-profit organizations, and government agencies worldwide. It provides the global organizational umbrella for standards, administrative, and coordination activities necessary for the implementation and evolution of the Internet.

From 1992-94, Tony Rutkowski was Director of Technology Assessment in the Strategic Planning Group of Sprint International. His principal responsibility was driving the company in new and innovative directions through business planning, development and incorporation of advanced technologies and applications generally, and internetworking technologies specifically. He followed and coordinated a broad array of technological, economic, business, trade and institutional activities in the information-telecommunication field, internal and external to Sprint.

From 1987-1992, he was Counselor to two different Secretary-Generals of the International Telecommunication Union (ITU) in Geneva - the world's intergovernmental organization for telecommunications. He was responsible for analysis of major developments in the field and formulation of policies and international provisions, including many technical, legal, regulatory, organization management and GATT trade issues that arose at the highest international business and governmental levels. He came to the ITU in 1987 as head of its Telecommunication Regulations and Relations Between Members Division - which supports the coordination of laws, regulations and operational information among national administrations and public telecom service providers.

An electrical engineer (B.S.E.E.) - lawyer (J.D.), Rutkowski has for the past 30 years enjoyed a wide variety of positions in private and public sectors in the telecommunication and information industry - domestic and international; in business, government and education. Previous positions include:

- publisher and Editor-in-Chief of the industry's leading trade magazine, Telecommunications (1986-87)
- Research Associate, Massachusetts Institute of Technology (1986-87)
- staff advisor to the two Chief Scientists of the FCC, analyzing and shaping a wide variety of key domestic and international science and technology policies and strategies in the telecommunications field within the FCC and among other government agencies (1979-1986)
- teaching in New York Law School's graduate program in telecommunications law (1980-83)
- staff technical advisor to the FCC Cable Televisions Bureau and special international advisor in the Office of Plans and Policy (1974-1980)
- direct responsibility for design engineering and management support of the Apollo project communication systems and Shuttle control systems at the Kennedy Space Center (1967-74)
- election to local public office in Florida as a leading community legislative reformer (1972-74)
- in previous incarnations, he was a research microbiologist and broadcast engineer.
- active in the IEEE, ABA, and numerous other forums - including in several instances, their creation. He has authored or contributed to several books, written more than 100 published articles and reports. He has testified as a Congressional expert witness, and remains a visible and prolific analyst-writer - appearing at many industry forums.

He is 52 years old, enjoys biking and mountaineering, is married to sinologist-economist-analyst-writer Kathleen McGlynn Rutkowski who now publishes the leading K-12 Internet newsletter, and with two little computer-weenies, operates a home Internet and helps reshape the world through these technologies.

Annex 2
Letter to Time Magazine from members of the Internet Research Task Force Statistics Working Group (IRTF-SWG)

Dear Editor
Time Magazine

The examination of pornography on the Internet in the 3 July issue of Time makes at least three serious definitional mistakes, mostly in the article "On a Screen Near You: Cyberporn," by Philip Elmer-DeWitt:

1) It equates the alt.binaries.pictures newsgroups with all of USENET. In fact, there are about 50 alt.binaries.pictures newsgroups out of about 10,000 USENET newsgroups. Since pictures require many bytes, these newsgroups (including ones that carry pictures that are scientific in nature) constitute a larger fraction of traffic on USENET, perhaps as much as 1/8. Even so, they are hardly all of USENET, and to take any percentage of traffic on these newsgroups as a percentage of traffic on all of USENET is simply wrong.

2) It equates USENET with all of the Internet. USENET newsgroups are quite popular on the Internet, but FTP and the World Wide Web (WWW) each probably carry more traffic over the Internet than does USENET and both FTP and WWW carry many pictures, many of them scientific, advertising, iconic, or for other purposes. USENET accounts for only a small fraction of Internet traffic by bytes, so all the picture newsgroups would account for only a few percent of total Internet traffic. Exactly what fraction and what percent are topics for serious research. However, it is clear that to use any characterization of USENET as a characterization of the Internet at large is incorrect.

3) It includes dialup BBSes in its definition of the Internet. Evidently many of the images collected in the Rimm study were collected from dialup BBSes. Clearly people who take the trouble to dial a specific telephone number to procure specific information are doing something different from accessing the Internet, so whatever data was collected this way does not indicate what might be on the Internet.

For (1) and (2) the issue does include a qualification in one place, a page or so into the article, but that qualification is overwhelmed by the cover and interior art and the rest of the article. If Time's own arithmetic in that qualification had been carried out to a percentage, it would have shown that the picture newsgroups make up only a small fraction of USENET

The Rimm study used as a basis for the article was itself highly questionable, and has since been severely criticised by researchers such as Brian Reid (whose measurement tools Rimm used) who have years of experience in attempting to measure USENET. Rimm's study almost certainly would have received such criticism before publication if it had been available for peer review.

It is very unfortunate that a magazine of the international readership and respectability of Time and a reporter of the journalistic and network experience of Philip Elmer-DeWitt would choose to publish an article of such a misleading nature, based on such questionable source material. Such an article would be bad at any time, but coming as it did at the height of the controversy over Congressional proposals to censor the Internet, this article fanned the flames of misconceptions surrounding important questions of U.S. national policy and of international import.

We call on Time to publish a retraction of the article in question, including a detailed examination of the flaws in the Rimm study and of the way it was represented in the article.

We also strongly recommend that Time take a leading role in providing real information about the Internet to the public by publishing a balanced in-depth examination of the Internet, including both sides of the Internet censorship debate. It can be done, see the Survey section of the July 1st-7th Economist, principally written by Christopher Anderson.

Finally, we are members of the Survey Working Group (SWG) of the Internet Research Task Force. SWG's purpose is to provide coordination and peer review of surveys of the Internet. We invite Time to communicate with SWG regarding future articles about the Internet; we can be reached by electronic mail to swg-info@zilker.net.

John S Quarterman, Editor, Matrix News, MIDS
Jill H Ellsworth, author, Marketing on the Internet, Oak Ridge Research
Ole Jacobsen, Editor and Publisher, ConneXions -- The Interoperability Report, Interop
Tony Rutkowski, Executive Director, Internet Society
Michael Schwartz, Associate Professor, University of Colorado
Smoot Carl-Mitchell, Managing Partner, Texas Internet Consulting

For an HTML version, see http://www zilker net/swg/index.html.

Annex 3

Research Testbed
A Ratings-Based Filtering Demonstration

advanced computing laboratory

Los Alamos National Laboratory (LANL)

Uniform Resource Identifier (URI) Testbed

This page provides an entry into the LANL URI testbed.

- IETF URI-WG Charter
- What are URIs, anyway?
- Resolution of URNs accomplished via Hotjava and Apache.
- How to register a resource using our test bed.
- A demonstration page of URNs: URI mailgroup archive.
- Current status of the project.
- How can URCs do infon. ation filtering?

Here is an Example URN:

If you are using our specially modified version of HotJava, you could resolve the following URN.

xdns2:uri.acl.lanl.gov:uri_charter

Ron Daniel rdaniel@lanl gov
Ed Bulas edb@acl.lanl gov

Ratings-based Filtering Demo

Recently, a great deal of interest has risen in the notion of allowing parents, teachers, nd other responsible adults to have a means for restricting children's access to some of the seamier sides of the Internet. One recent proposal is KidCode, which asks publishers to change the URLs of their documents to be of the form:

```
protocol:host[:port]/path/KidCode.age[.type of offensive content]*
```

for example:

```
http://www.playboy.com/may95/articles/KidCode.18.nudity.language.sex
```

We believe that this scheme is inappropriate for several reasons. We have technical objections to how this scheme mixes resource identity, resource retrieval, acces restrictions, and content description. We do not like the way it mandates a naming system. We also have philosophical objections to this scheme because it makes providers responsible for rating their own content using one universal value judgement, and expressing that as a recommended minimum age for viewing. Given the difference in community standards in the United States, never mind the whole world, we believe this scheme is not an appropriate choice for standardization by an international body such as the IETF.

As an alternative, we have developed a proof-of-concept implementation of a URC-based filtering service. In contrast to the KidCode proposal, rating is done by third parties, and parents are free to choose the third party whose views most closely correspond to their own. As an example, browsers at the local school might be configured to use a rating service approved of by the PTA or the local school board. At home, the Smiths might subscribe to the rating service of the Southern Baptists. Their next-door neighbors, the Jones, might use the NAACP's, while the couple down the street subscribe to a movie rating service to help filter out the innane.

Our demo uses a Sample Rating System to describe the Internet resources. In addition to an age element, other elements are provided so that familes with a lower tolerance for violence or a higher tolerance for nudity can be more selective in their filtering.

If you have our specially hacked version of HotJava, you can give the filtering test a whirl:

Nice Resource
: You should be able to get this one.

Nasty Resource
: You should NOT be able to get this one, although it is not really very nasty.

Ron Daniel / rdaniel@lanl.gov

Sample Rating System

The Sample Rating System provides a means for describing the sort of content likely to be offensive. so that familes with a lower tolerance for violence or a higher tolerance for nudity can be more selective in their filtering. An age recommendation element is also provided, since this most closely matches several existing rating systems. This is believed more appropriate than the universal age of Kidcode, since people have a choice of rating service and can find one whose notion of appropriate age matches their own, or the standard of their community.

The SRS provides the Age, Nudity, Sex, Violence, Language, Religion, and Politics elements. Other than Age, all the elements rate content on a scale of "All, 1, 2, 3, or 4". If a resource is rated "ALL" for language, then it means that the rating body believes that the language used in the resource is suitable for all audiences. If the reviewers rate a resource "1" for Nudity, then it means that they believe there is some content, revealing attire perhaps, that may offend some audiences. Rating a resource "4" for violence means that the reviews think the resource has enough violent content that only the most mature audiences should view it. Guidelines for rating resources are given in the table below.

This system was strongly inspired by the rating system developed by the Software Publisher's Association for rating video games. I have made changes to it in order to make it more broadly applicable.

```
Age
  An integer greater than or equal to 0. Typically the maximum value
  will be the legal age of majority in the culture of the reviewers.
  If no Age is supplied, 0 is assumed which means the content is
  suitable for all ages. If a value is supplied, then the rating body
  believes that to be the minimum age a person should be to view the
  material.

Nudity
  ALL - No nudity or revealing attire (default)
  1   - Revealing attire
  2   - Bare buttocks, brief display of bare femal breasts
  3   - Non-sexual frontal nudity
  4   - Provocative frontal nudity

Sex
  All - Romance, no sex (default)
  1   - passionate kissing, Clothed sexual touching
  2   - Non-explicit sexual activity
  3   - Explicit sexual activity
  4   - Sex crimes


Violence
  All - Harmless conflict, some damage to non-living things (default)
  1   - Damage or destruction of non-human living beings
  2   - Damage or destruction of living beings, including humans;
        Some blood
  3   - Destruction of living beings, including humans;
        Blood and gore
  4   - Wanton or gratuitous violence; Torture; Rape

Language
  All - Inoffensive slang; No profanity (default)
  1   - Mild explitives and profanity
  2   - Moderate expletives; Non-sexual anatomical references
  3   - Strong language; obscene gestures
```

```
  4   - Crude or explicit sexual references

Drugs
  All - No offensive content; some use of alchonol or tobacco (default
  1   - Heavy use of alcohol and/or tobacco
  2   - Some use of controlled substances
  3   - Heavy use of controlled substances; injection
  4   - Inducement to use of controlled substances

Religion (all of these ratigns are to be regarded as being made according
          to the religious orientation of reviewers)
  All - Doctrine or no religous content (default)
  1   - Presentation of doctrinare version of contrary religious views.
  2   - Apostasy
  3   - Heresey
  4   - Blasphemy

Politics (all of these are to be regarded as being made according to the
          political views of the reviewers)
  All - No offensive political content (default)
  1   - Disagreements along party lines
  2   - strong political speech;
  3   - offensive political speech; calls for non-violent criminal action
  4   - Incitement to riot; violent overthrow of legitimate governemt
```

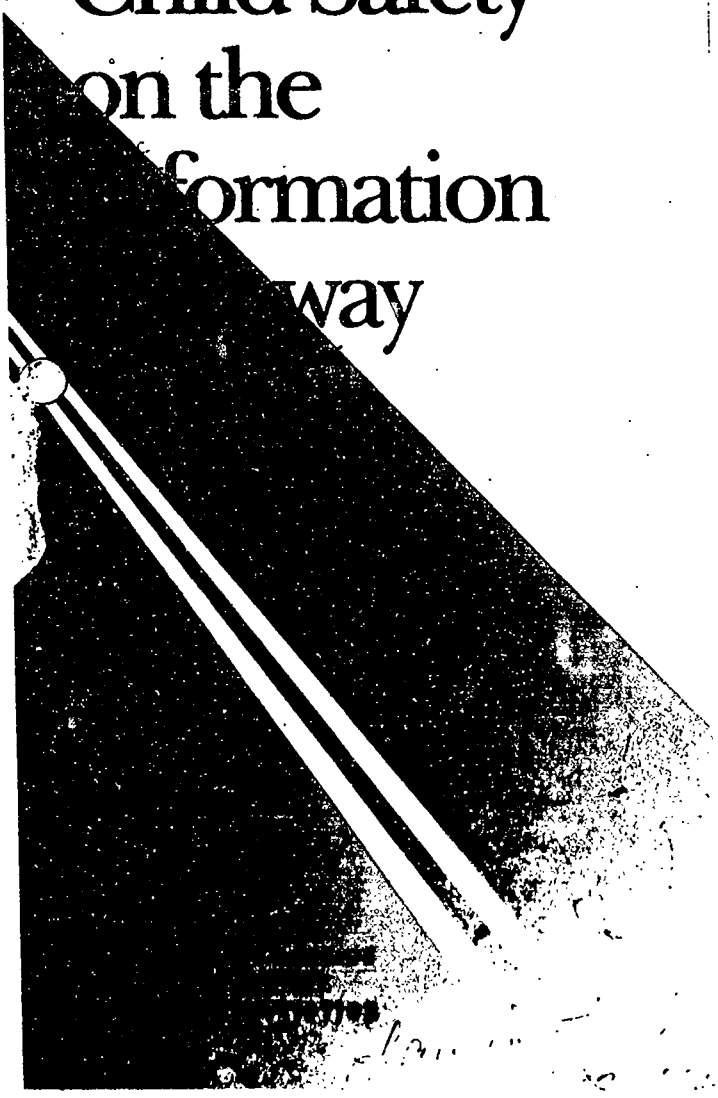
As an example of the use of the system, here is how I would rate Disney's "Beauty and the Beast":

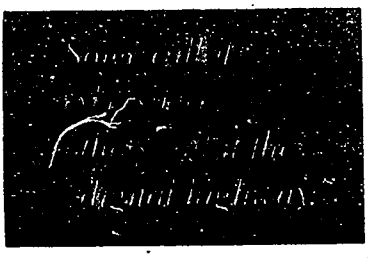
```
<rating scheme="SRS" type="Age">3</>
<rating scheme="SRS" type="Violence">2</>
```

Disney, naturally enough, might rate it "ALL" for violence.

Ron Daniel / rdaniel@lanl.gov

Child Safety on the Information Highway





Whatever it's called, millions of people are now connecting their personal computers to telephone lines so that they can "go online." Traditionally, online services have been oriented towards adults, but that's changing. An increasing number of schools are going online and, in many homes, children are logging on to commercial services, private bulletin boards, and the Internet. As a parent you need to understand the nature of these systems.

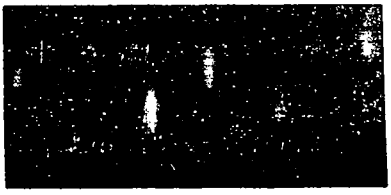
- Online services are maintained by commercial, self-regulated businesses that may screen or provide editorial/user controls, when possible, of the material contained on their systems.

- Computer Bulletin Boards, called BBS systems, can be operated by individuals, businesses, or organizations. The material presented is usually theme oriented offering information on hobbies and interests. While there are BBS systems that feature "adult" oriented material, most attempt to limit minors from accessing the information contained in those systems.

- The Internet, a global "network of networks," is *not* governed by any entity. This leaves no limits or checks on the kind of information that is maintained by and accessible to Internet users.

The Benefits of the Information Highway

The vast array of services that you currently find online is constantly growing. **Reference information** such as news, weather, sports, stock quotes, movie reviews, encyclopedias, and airline fares are readily available online. Users can conduct **transactions** such as trading stocks, making travel reservations, banking, and shopping online. Millions of people **communicate** through electronic mail (E-mail) with family and friends around the world and others use the public message boards to make new friends who share common interests. As an **educational and entertainment** tool users can learn about virtually any topic, take a college course, or play an endless number of computer games with other users or against the computer itself. User **"computing"** is enhanced by accessing online thousands of shareware and free public domain software titles.

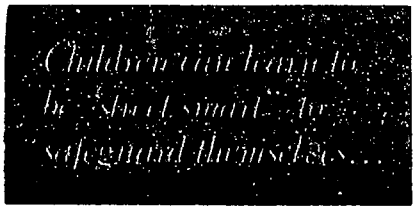


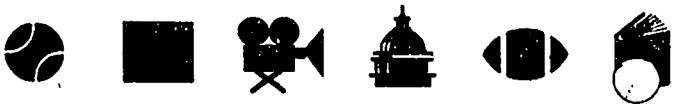
Most people who use online services have mainly positive experiences. But, like any endeavor – traveling, cooking, or attending school – there are some risks. The online world, like the rest of society, is made up of a wide array of people. Most are decent and respectful, but some may be rude, obnoxious, insulting, or even mean and exploitative.

Children and teenagers get a lot of benefit from being online, but they can also be targets of crime and exploitation in this as in any other environment. Trusting, curious, and anxious to explore this new world and the relationships it brings, children and teenagers need parental supervision and common sense advice on how to be sure that their experiences in "cyberspace" are happy, healthy, and productive.

Putting the Issue in Perspective

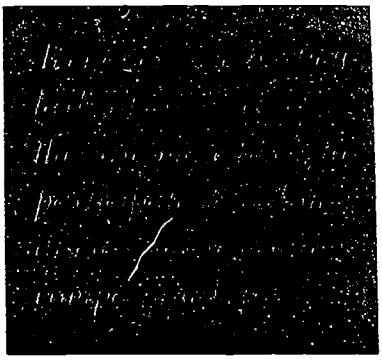
Although there have been some highly publicized cases of abuse involving computers, reported cases are relatively infrequent. Of course, like most crimes against children, many cases go unreported, especially if the child is engaged in an activity that he or she does not want to discuss with a parent. **The fact that crimes are being committed online, however, is *not* a reason to avoid using these services.** To tell children to stop using these services would be like telling them to forgo attending college because students are sometimes victimized on campus. A better strategy would be for children to learn how to be "street smart" in order to better safeguard themselves in any potentially dangerous situation.





What Are the Risks?

There are a few risks for children who use online services. Teenagers are particularly at risk because they often use the computer unsupervised and because they are more likely than younger children to participate in online discussions regarding companionship, relationships, or sexual activity. Some risks are:



Exposure to Inappropriate Material
One risk is that a child may be exposed to inappropriate material of a sexual or violent nature.

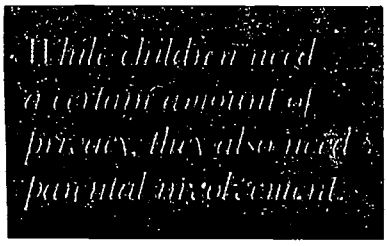
Physical Molestation
Another risk is that, while online, a child might provide information or arrange an encounter that could risk his or her safety or the safety of other family members. In a few cases, pedophiles have used online services and bulletin boards to gain a child's confidence and then arrange a face-to-face meeting.

Harassment
A third risk is that a child might encounter E-mail or bulletin board messages that are harassing, demeaning, or belligerent.

How Parents Can Reduce the Risks

To help restrict your child's access to discussions, forums, or bulletin boards that contain inappropriate material, whether textual or graphic, many of the commercial online services and some private bulletin boards have systems in place for parents to block out parts of the service they feel are inappropriate for their children. If you are concerned, you should contact the service via telephone or E-mail to find out how you can add these restrictions to any accounts that your children can access.

The Internet and some private bulletin boards contain areas designed specifically for adults who wish to post, view, or read sexually explicit material. Most private bulletin board operators who post such material limit access to people who attest that they are adults but, like any other safeguards, be aware that there are always going to be cases where adults fail to enforce them or children find ways around them.



The best way to assure that your children are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with your

children while they're online. Have them show you what they do and ask them to teach you how to access the services.

While children and teenagers need a certain amount of privacy, they also need parental involvement and supervision in their daily lives. The same general parenting skills that apply to the "real world" also apply while online.

If you have cause for concern about your children's online activities, talk to them. Also seek out the advice and counsel of other computer users in your area and become familiar with literature on these systems. Open communication with your children, utilization of such computer resources, and getting online yourself will help you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use.

Guidelines for Parents

By taking responsibility for your children's online computer use, parents can greatly minimize any potential risks of being online. Make it a family rule to:

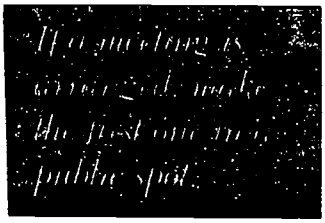
■ Never give out identifying information – home address, school name, or telephone number – in a public message such as chat or bulletin boards, and be sure you're dealing with someone that both you and your child know and trust before giving it out via E-mail. Think carefully before revealing any personal

information such as age, marital status, or financial information. Consider using a pseudonym or unlisting your child's name if your service allows it.

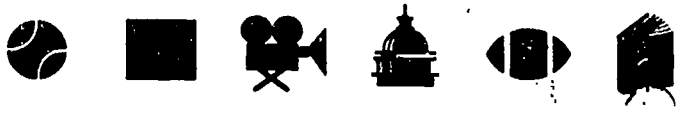
■ Get to know the services your child uses. If you don't know how to log on, get your child to show you. Find out what types of information it offers and whether there are ways for parents to block out objectionable material.

■ Never allow a child to arrange a face-to-face meeting with another computer user without parental permission. If a meeting is arranged, make the first one in a public spot, and be sure to accompany your child.

■ Never respond to messages or bulletin board items that are suggestive, obscene, belligerent, threatening, or make you feel uncomfortable. Encourage your children to tell you if they encounter such messages. If you or your child receives a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your service provider and ask for their assistance.



Should you become aware of the transmission, use, or viewing of child pornography while online, immediately report this to the National Center for Missing and Exploited Children by calling 1-800-843-5678. You should also notify your online service.



■ Remember that people online may not be who they seem. Because you can't see or even hear the person it would be easy for someone to misrepresent him- or herself. Thus, someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year-old man.

■ Remember that everything you read online may not be true. Any offer that's "too good to be true" probably is. Be very careful about any offers that involve your coming to a meeting or having someone visit your house.

■ Set reasonable rules and guidelines for computer use by your children (see "My Rules for Online Safety" on last page as sample). Discuss these rules and post them near the computer as a reminder. Remember to monitor their compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child or teenager's excessive use of online services or bulletin boards, especially late at night, may be a clue that there is a potential problem. Remember that personal computers and online services should not be used as electronic babysitters.

Be sure to make this a family activity. Consider keeping the computer in a family room rather than the child's bedroom. Get to know their "online friends" just as you get to know all of their other friends.

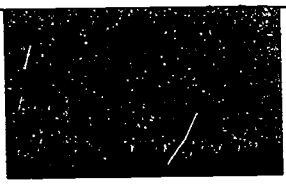
This brochure was written by Lawrence J. Magid, a syndicated columnist for the *Los Angeles Times*, who is author of *Cruising Online: Larry Magid's Guide to the New Digital Highway* (Random House, 1994) and *The Little PC Book* (Peachpit Press, 1993).

Child Safety on the Information Highway was jointly produced by the National Center for Missing and Exploited Children and the Interactive Services Association (8403 Colesville Road, Suite 865, Silver Spring, MD 20910).

This brochure was made possible by the generous sponsorship of:

AMERICA Online
CompuServe
The information service you won't outgrow.
DELPHI INTERNET
eWorld
GEnie.
Interchange ONLINE NETWORK
PRODIGY. Service

My Rules for Online Safety



- I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.

- I will tell my parents right away if I come across any information that makes me feel uncomfortable.

- I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.

- I will never send a person my picture or anything else without first checking with my parents.

- I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the online service.

- I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

For further information on child safety, please call the National Center for Missing and Exploited Children at 1-800-THE-LOST (1-800-843-5678).

Products Under Development to Empower Parents

Currently, a number of products are under development that can help parents control their children's activities in Cyberspace. These range from tracking programs to true "locks and Keys." However, no technological solution should be considered a total replacement for parents active and personal attention to their children's activities online. Below are a sampling of a few of the products that are available or under development.

Commercial online services such as CompuServe, AOL and Prodigy provide a wide range of options for parents including screening software, the ability to monitor children's activities online after the fact, locks and keys to prevent children from accessing chat areas and removal of certain newsgroups and web sites from being searched and accessed. The online services also teamed with the Interactive Services Association more than a year ago to develop the "Child Safety on the Information Superhighway" brochure to educate parents.

Surf Watch is designed to provide parental controls for families who choose to connect to the Internet directly rather than through an online service. Surf Watch resides on the personal computer and allows parents to block access to USENET Newsgroups, World Wide Web sites and FTP (File Transfer Protocol) sites that contain inappropriate materials. SurfWatch also employs professionals to log sites where inappropriate material is located and they embed these sites into the program.

Net Nanny is designed to prevent children from accessing areas on the Internet that a parent deems inappropriate and can prevent children from giving their name, address, and other personal information to strangers via e-mail and chat rooms. It can log off or shut down the computer if these activities are attempted. It also contains a dictionary in which parents can enter the names of sites known to contain inappropriate materials, making it easier for a parent to decide what to block. Parents can also enter phrases such as "Where do you live" or "What's your name?" If anyone asks these questions, the computer will be shut down. It is compatible with online services and with direct Internet access providers.

CYBERsitter allows parents to monitor their children's activity and can prevent children from downloading image, sound and video files. The program is launched when the computer is started up, regardless of whether a parent is present. It keeps a record of all activity on the computer allowing patents to monitor their children's use of the computer.

KidCode is an innovative proposal for an Internet protocol designed to block access to sites based on a common voluntary rating system. It is currently in development, but would be compatible with all of the parental control applications currently on the market.

Crossing Guard is software that will allow parents to block access to sites that may contain inappropriate materials. It will also allow parents to monitor their children's activities and set timer to control when and for how long their children can surf the Internet. This software is being integrated into Internet-In-A-Box for Kids, a product being developed by CompuServe's Internet Services.

Mr. SCHIFF. Thank you very much, Mr. Rutkowski.
Ms. Duvall?

STATEMENT OF MS. ANN DUVALL, PRESIDENT, SURF-WATCH SOFTWARE, INC., LOS ALTOS, CALIFORNIA

Ms. DUVALL. Thank you.

Chairwoman Morella, Chairman Schiff, and Members of the Committee. It is an honor to be asked to speak to you today about the Internet and its role in the lives of our children. It is an even greater honor to be here today because it is not often that we get to be true pioneers, and I believe that we in this room stand at such a moment.

Looking back on the history of this Country, it is the pioneer experience that has shaped what we think of as the American experience. The bravery of the Pilgrims, the mythology of the Old West—these are the stories and images we call upon to define what it is to be American.

The long-awaited information revolution is truly upon us. What we have called for the past years the "Information Superhighway," the "Internet", and now just the "Net" is rapidly becoming a true electronic community.

In this society of the future, we are the people who are settling this land. This is a community without the traditional borders that have given us national identity.

As in other communities, some of us choose to be farmers, some merchants, some missionaries, and some scoundrels. Whoever we are, though, we make our livings, raise our children, and live our lives in the midst of this community.

It is helpful to think of the Internet as a pioneering community in the way I've described for many reasons. I would like to address two here. First, the Internet was designed to be an open place that symbolizes for all of us the free exchange of information and the power of technology to better the lives of people.

The kind of information available on the Internet is astounding and the range of information is as vast as the human imagination.

Imagine being able to find with just the click of one button art in the Louvre, text about bills to be discussed in the House of Representatives, or a street map of a place you will soon visit on vacation.

Second, the Internet serves as a social tool, not simply a technological one. Social rules come and go on the Internet as it grows, and people use the Internet to relate to one another and find common ground.

Products and services on the Internet must develop quickly and be highly responsive to the electronic community in order to be effective.

In fact, a quick response to the needs of the electronic community was the genesis for SurfWatch.

My daughter, Jessica, is 14 years old and she thoroughly enjoys Internet. She uses the computer and our Internet connection to do her homework, research topics for her classes, and as a way to socialize with her online friends.

She even devotedly attends a weekly online chat about her favorite television show.

My husband and I encourage her to use the Internet because of the vast resources it makes available to her. Some examples of things we have done together on the Net include: Searching for information on the Fragile X syndrome for her science class; Viewing the NASA live space feed; and Competing together in a weekly trivia contest that originates in England.

However, at the same time, I was nervous about Jessie's Internet use because I knew that she could stumble across inappropriate material. The amount of valuable, exciting, and important information on the Internet greatly overshadows the unwanted material, but it is still there and accessible.

My husband, who was a pioneer himself on the Internet 25 years ago, became even more concerned that there was a problem. Shortly thereafter, he literally woke up in the middle of the night with an idea of how to begin to fix that problem, and that was the beginning of SurfWatch.

We committed our time, our own money, and our personal resources to this important issue. As Bill developed the technology, it became more and more clear to us that SurfWatch would be a useful tool for many parents who, like ourselves, wish to choose what comes into their homes via the Internet.

SurfWatch is a wonderful example of the pioneering spirit at work, because it is truly a first-of-its-kind, common-sense tool that parents can use to reduce the risk of their children accessing inappropriate material.

It is highly effective at keeping away unwanted material on the Internet. SurfWatch is an easy-to-install, easy-to-use product even for unsophisticated computer users. It sits on one's own personal computer.

If you attempt to access a location that is believed to contain inappropriate material, you get a message that it is blocked. This does not interrupt your Internet connection or impede the access of other Internet users.

In addition, a simple on/off switch, controlled by a parental password, allows access to any location that we have blocked.

SurfWatch identifies sites by using specially developed pattern-matching techniques and a database of known sites. If a site is on the list, then SurfWatch will block it.

The Internet is dynamic and, as new sites arise and are discovered, they are added to the database weekly. SurfWatch can be easily and automatically updated with the latest information over the Internet which serves to give SurfWatch users the best protection possible against unwanted material.

The SurfWatch Manager, which will be released before the end of the year, will allow parents to change, edit, or replace the list of sites provided. This acknowledges the importance of enabling individual parents to make their own choices about information that is appropriate for their own children.

SurfWatch is just one example of the computer industry responding to the needs created by our explosive growth of technology. Our goal is to make SurfWatch available to all parents and educators who wish to use it, and we have recently signed agreements to make sure people will be able to find SurfWatch in almost any of their local stores.

In addition, SurfWatch is working with America Online to provide SurfWatch technology to all 3 million America Online users. Other organizations and companies are beginning to propose rating systems for Internet sites, something that would enhance the performance of SurfWatch further and allow parents to be even more in control of the kinds of information coming into their homes through their computers.

As you know, information from millions of sites around the world is easily accessible over the Internet, and especially through the World Wide Web. In fact, we have found that about 30 percent of the sites we block originate in places outside the United States.

There is not a simple national solution to the problem of children accessing inappropriate material on the Internet. Excessive government regulations might jeopardize private-sector opportunities.

SurfWatch firmly believes that the technology industry can and must respond to these sociotechnological issues. We also affirm that parents must be involved in any solution. SurfWatch is not a total solution.

Parents must become educated about their children's use of the computer, teach their children to be Net "street smart," and provide guidelines for behavior in this new Internet community.

Bill and I maintain ongoing discussions with Jessie about the Internet, its wonders and its caution areas. This has become an important part of our relationship with our daughter.

It is still a bit unusual for a technology product to be seen as a solution to a social problem, and that puts SurfWatch into a different frame of reference than the usual software purchase, but we will see this situation more and more as the growth of technology makes it necessary for us to develop equally good technology to solve some of the social problems it has engendered.

Private industry is ideally suited to address the kind of issue which requires rapid response to rapid change and a great understanding of the technologies involved.

In closing, we at SurfWatch are committed to continuing to provide technological tools that help solve the problems that arise from integrating technology into our society.

Now, I would like to take just a minute to give you a very, very short demo.

[A computer presentation follows:]

Presently, we are looking at a screen that we are actually on the Internet connected to a computer sitting in California. This is what is called a "home page," which means it is the first page that comes up when I actually start my Internet connection. This happens to be the SurfWatch home page, which again millions of people can access to get general information about SurfWatch.

Now with just a simple click, I can now be on a page that will give me child-care resource information, including legislation that is pending on child rearing, pointers to pediatric medical information, patenting tips, and additional pointers that will take me to kids-oriented pages.

With another simple click of the button, I can now be at the Disneyland Park home page. If I were planning a trip to Disneyland, I could get information about accommodations, what attractions were, help in trip planning, with just a simple click.

The next click will take me to the weather page. This is a worldwide weather map out of Illinois that allows me to see weather all over the country. If I am planning a trip, I can download the radar weather map from wherever I am.

Now meanwhile, during this whole time that we have been looking at all these sites, SurfWatch has been loaded on this computer and running in the background, so no one actually knows it is there.

If, however, I decided that I wanted to access something that we believe contains inappropriate material—so if I didn't open, and typed in an access to a magazine that may have inappropriate material, and then attempted to open it, I would get a message "Blocked by SurfWatch." That is the simple way SurfWatch works. It does not interfere with anything. I thank you for letting me speak this morning.

[The prepared statement of Ms. Duvall follows:]

Testimony of Ann W. Duvall
President
SurfWatch Software Inc.

Before the Basic Research and Technology Subcommittees
of the Committee on Science
United States House of Representatives
July 26, 1995

Chairwoman Morella, Chairman Schiff, and members of the Committee:

It is an honor to be asked to speak to you today about the Internet and its role in the lives of our children. It is an even greater honor to be here today because it is not often that we get to be true pioneers, and I believe that we in this room stand at such a moment. Looking back on the history of this country, it is the pioneer experience that has shaped what we think of as the American experience: the bravery of the Pilgrims, the mythology of the Old West — these are the stories and images we call upon to define what it is to be American.

The long-awaited information revolution is truly upon us. What we have called for the past years the "Information Superhighway," the "Internet," and now just the "Net," is rapidly becoming a true electronic community. In this society of the future, we are the people who are settling the land. This is a community without the traditional borders that have given us national identity. As in other communities some of us choose to be farmers, some merchants, some missionaries, and some scoundrels. Whoever we are, though, we make our livings, raise our children, and live our lives in the midst of this community.

It is helpful to think of the Internet as a pioneering community in the way I've described for many reasons. I would like to address two here: first, the Internet was designed to be an open place that symbolizes for all of us the free exchange of information and the power of technology to better the lives of people. The kind of information available on the Internet is

SurfWatch Software, Inc. • 105 Fremont Ave., Suite F • Los Altos, CA 94022 • Phone 415.948.9500 • Fax 415.948.9577
Email info@surfwatch.com • http://www.surfwatch.com

astounding, and the range of information is as vast as the human imagination. Imagine being able to find with just the click of one button art in the Louvre, text of bills about to be discussed in the House of Representatives, or a street map of a town you will soon visit on vacation.

Second, the Internet serves as a social tool, not simply a technological one. Social rules come and go on the Internet as it grows, and people use the Internet to relate to one another and find common ground. Products and services on the Internet must develop quickly and be highly responsive to the electronic community in order to be effective.

In fact, a quick response to the needs of the electronic community was the genesis for SurfWatch. My daughter, Jessica, is 14 years old, and she thoroughly enjoys the Internet. She uses the computer and our Internet connection to do her homework, research topics for her classes, and as a way to socialize with her online friends. She even devotedly attends a weekly online chat about her favorite television show. My husband and I encourage her to use the Internet because of the vast resources it makes available to her. Some examples of things we have done together on the Net include searching for information on the Fragile X syndrome for her science class, viewing the NASA live space feed, and competing together in a weekly trivia contest that originates in England.

However, at the same time I was nervous about Jessie's Internet use because I knew that she could stumble across inappropriate material. The amount of valuable, exciting and important information on the Internet greatly overshadows the unwanted material, but it is still there and accessible. My husband, who was a pioneer himself on the Internet 25 years ago, became even more concerned that there was a problem. Shortly thereafter, he literally woke up in the middle of the night with an idea about how to begin to fix that problem, and that was the beginning of SurfWatch. We committed our time, our own money, and our personal resources to this important issue. As Bill developed the technology, it became more and more clear to us that SurfWatch would be a useful tool for many parents, who , like ourselves, wish to choose what comes into their homes via the Internet.

SurfWatch is a wonderful example of the pioneering spirit at work, because it is truly a first of its kind common-sense tool that parents can use to reduce the risk of their children accessing inappropriate material. It is

highly effective at keeping away unwanted material on the Internet. SurfWatch is an easy to install, easy to use product, even for unsophisticated computer users, that sits on a person's individual computer. If you attempt to access a location that is believed to contain inappropriate material, you get a message that it is blocked. This does not interrupt your Internet connection or impede the access of other Internet users. In addition, a simple on/off switch, controlled by a parental password allows access to any location we have blocked. SurfWatch identifies these sites by using specially developed pattern matching techniques and a database of known sites. If a site is on the list, then SurfWatch will block it. The Internet is dynamic, and as new sites arise and are discovered, they are added to the database weekly. SurfWatch can be easily and automatically updated with the latest information over the Internet which serves to give SurfWatch users the best protection possible against unwanted material. The SurfWatch Manager, which will be released before the end of the year, will allow parents to change, edit, or replace the list of sites provided by SurfWatch. This acknowledges the importance of enabling individual parents to make their own choices about information that is appropriate for their own children.

SurfWatch is just one example of the computer industry responding to needs created by the explosive growth of technology. Our goal is to make SurfWatch available to all parents and educators who wish to use it, and we have recently signed agreements to make sure people will be able to find SurfWatch in almost any of their local stores. In addition, SurfWatch is working with America Online to provide SurfWatch technology to all 3 million America Online subscribers. Other organizations and companies are beginning to propose rating systems for Internet sites, something that would enhance the performance of SurfWatch further and allow parents to be even more in control of the kinds of information coming into their homes through their computers.

As you know, information from millions of sites around the world is easily accessible over the Internet, and especially through the World-Wide Web. In fact, we have found that about 30% of the sites that we block originate in places outside the United States. There is not a simple, national solution to the problem of children accessing inappropriate material on the Internet. Excessive government regulations might jeopardize private sector opportunities. SurfWatch firmly believes that the technology industry can

and must respond to these socio-technological issues. We also affirm that parents must be involved in any solution. SurfWatch is not the total solution. Parents must become educated about their children's use of the computer, teach their children to be net "street smart," and provide guidelines for behavior in this new Internet community. Bill and I maintain ongoing discussions with Jessie about the Internet, its wonders and its caution areas, and this has become an important part of our relationship with our daughter.

It is still a bit unusual for a technology product to be seen as a solution to a social problem, and that puts SurfWatch into a different frame of reference from the usual software purchase. But we will see this situation more and more in the future, as the growth of technology makes it necessary for us to develop equally good technology to solve some the social problems it has engendered. Private industry is ideally suited to address this kind of issue which requires rapid response to rapid change and great understanding of the technologies involved. In closing, we at SurfWatch are committed to continue to provide technological tools that help solve the problems that arise from integrating technology into our society.

Mr. SCHIFF. We thank you for being present, Ms. Duvall
Mr. Heaton?

STATEMENT OF MR. STEVEN HEATON, GENERAL COUNSEL, AND SECRETARY, COMPUSERVE, COLUMBUS, OHIO

Mr. HEATON. Good morning.

I would like to begin by thanking the Chairs of this hearing, Representative Morella and Representative Schiff, and to the other Members, as well as to the Committee staff who have been so helpful.

It is my pleasure to have an opportunity to address the panel and participate in today's discussions. My name is Steve Heaton. I am General Counsel for CompuServe, Incorporated.

Although it is my task to represent CompuServe and the industry, I have personal reasons for wanting to be in front of you today, as well. I am a father with several young children who are beginning to explore the online world and the public Internet. So the issues we are discussing today are of a personal interest, as well as a business concern.

I will be covering today four points: A quick overview of CompuServe and its online business; Second, a brief statement on the relationship between the end user and the many sources of computer-based content; Third, an acknowledgement of the 'Cyberporn' issue; and Finally, possible answers to that issue, such as information and education, but also technology solutions in government and industry cooperation.

CompuServe, for those of you who are not familiar with our business, is a Columbia, Ohio, based company. We are best known for the CompuServe Information Service, sometimes known as CIS.

By using a computer and a modem, approximately 3 million members in 150 countries around the world get access to, among other things, information on every imaginable subject, a variety of entertainment sources, and electronic communication in various forms.

CompuServe also provides a pipeline to the Internet where members can access information residing on Internet host computers at universities, corporations, and at government agencies.

Because CompuServe is not the sole source of computer-based information, however, it is extremely important to focus on the end-user computer as the central point for any truly effective solution to the problem of Cyberporn.

You can liken to a wheel of a bicycle. The home computer is the hub, and each spoke a potential source or feed of computer-based information. CompuServe would represent one spoke, the Internet another, a government data base yet another, and so on.

Since information parents might find objectionable could come from any of these many sources, technical solutions are best located at the hub so that they are effective as to all information coming into the home or office.

Moreover, placing primary protections at the hub allows for as much personal choice as possible over what is and is not acceptable without needing to entrust these judgment calls to private companies or settling for a one-size-fits-all decision as to what content will or will not be admitted into the home.

Of great concern to consumers and to the industry today is the issue of electronic content available via computer that is inappropriate for children. Internet Newsgroups may provide a useful example.

These are a collection of thousands of online bulletin boards available on the Internet, each dedicated to a very specific issue or topic. Although of enormous value, both potential and real, Newsgroups also can be places where often language normally considered too coarse for typical face-to-face conversations is tolerated.

Also, like its Newsgroup subset, the Internet itself can also be used for both wholesome purposes and otherwise. For example, it can be used as a medium for the distribution of indecent or even obscene material by individuals who have chosen this medium as a vehicle for their own objectives.

Although only a small part of Internet content and activity, these questionable-to-illegal uses of the Internet are garnering a tremendous amount of attention, as you know. But no matter how relatively insignificant the traffic in this kind of material might be, parents are right to be concerned.

To deal with this issue, we in the industry are committed to empower parents with both education and technology. We want to give parents tools that they can use to block and filter materials they deem objectionable.

In addition to the development and distribution of technology-based tools themselves, a related and preliminary goal of CompuServe is to educate our members as to available options and solutions.

One such solution CompuServe will be offering is special online area through which information on both risks and solutions will be made available. This awareness will be supported through CompuServe Magazine, a monthly magazine published by CompuServe and tailored to the online community. An upcoming issue of CompuServe Magazine will focus on topics related to children online.

Another informational and educational source is this booklet, *Child Safety on the Information Superhighway*. More than a year ago, CompuServe and some of the other online services developed this brochure in cooperation with the Interactive Services Association and Los Angeles Times columnist, Larry Magid. The booklet has received broad distribution and we continue to make it available to parents.

I have brought a number of copies with me today for distribution, as appropriate. In addition to educational and information efforts, CompuServe has also addressed the issue of appropriate content through several technical measures it has undertaken and is planning.

For example, the search function for CompuServe's Internet access eliminates certain newsgroups that may deal in topics that could be particularly mature in nature. As a result, children are less likely to find those areas unintentionally.

Second, we have also worked within our own service—and continue to do so—to give our members the option of blocking certain online forums that, as parents, they find objectionable.

Third, our Internet division has announced a product called *Internet-In-A-Box for Kids*. This is an Internet-access product designed to safely provide Internet access to kids.

It will do this by way of a dedicated Internet site created specifically for kids, and by blocking out many other sites as well. This will make it easier for families to safely explore the Internet.

Fourth, we are also in the process of evaluating third-party software products that, when activated on a home PC, will work in conjunction with CompuServe and other points of electronic information access. This, we believe, will ultimately be the first and most effective line of defense in managing the nature of computer-based content that is available on the millions of PCs in homes, schools, and offices. Some of these software technology solutions we are evaluating include products known as, CyberSitter, NetNanny, SurfWatch, and others.

In fact, we are in discussions right now to include one of these products in our *Internet-In-A-Box for Kids* product as an added layer of protection.

Separately, I have printed up a list of some of these products and how they operate. In the interest of time, I have submitted copies to the panel for you to browse at your convenience.

Fifth, CompuServe also continues to look at still other options it might have specific to its own CIS network.

For instance, we are looking at ways to build technological blocking and filtering tools directly into our WINSYM interface software. That is the software by which all our members access the CompuServe service.

Even novice computer users, including parents who now ask their kids to set the clock on the VCR, will find these blocking and filtering tools easy to install, customize, access, and use.

Finally, but by no means least, we continue to cooperate with law enforcement and government agencies who work to prosecute those who choose to abuse the interactive information media.

Contrary to what some would have us believe, the online world is not a lawless wild, wild West. Existing laws against obscene and indecent material do exist and do apply in Cyberspace and are more than adequate to deal with the few who use computer media for illegal purposes.

Worth noting, once again, is the fact that many of the solutions we are examining are focused on the one point of convergence in all online activities—the end-user's personal computer.

Parents cannot control the Internet, but they can control their PC. By providing them access to software tools and new chip technologies, by supporting content rating systems and conventions, and even by reminding them that physical locks can be installed on the PC's on switch, we can help them take control of what comes into their homes.

I would like to depart for just a moment from my prepared statement to simply respond to the opening statements made today by indicating that these blocking and filtering technologies that are at work, I think, will eventually depend on a close collaboration with the many rating systems that are going on right now.

Essentially, in order to allow households to make the kind of personal choices as to what content they do or do not approve of, there

will be a dependency, I believe, on various rating systems which will then rely as well on the technical standards being developed so that voluntarily, providers of content can attach a rating to their systems.

Mr. SCHIFF. I would just like to add, since you diverted from your statement, I hope the rating system works better than I have seen it work on movies.

Mr. HEATON. Congressman Schiff, I believe that what we will find are a variety of rating systems that will give a variety of choices to people that will simply enable the many different levels of tolerance that are in all the households across the country, and indeed the world, to pick and choose and customize what does come into their homes. I see that arising already as we speak.

CompuServe also serves the welcome and interest on the part of Government to consider issues that relate to our business. We can use government's help in a variety of areas.

Government can help to educate parents and others about the risks and the benefits of the online environment. Government can help to shape laws and policies based on individual responsibility for one's own actions, and government can encourage the development and deployment of new technologies that empower parents in shaping their children's experience in Cyberspace.

Please keep in mind that the online industry is both fast moving and global. Lately, the industry has completely remade itself, even every few months. That presents challenges for regulators to stay abreast of the latest developments.

The Cyber community, made up of hundreds of thousands of computers distributed across the globe, is truly a world without borders.

This makes imperative that laws focus on individual responsibility and that education and empowerment among users and concerned parents be emphasized.

I would like to conclude by again thanking the chairs and organizers of this hearing most sincerely for the opportunity to speak on these timely issues.

CompuServe, as a responsible company and as a representative of the information services industry, is working hard to address these issues and to provide the tools parents want. We are committed to having Cyberspace be a safe and enjoyable place for both parents and their children.

Thank you.

[The prepared statement of Mr. Heaton follows:]

CompuServe Perspective on Challenges and Opportunities
for
Parental Controls in Cyberspace

presented by

Stephen M. Heaton
General Counsel, CompuServe Incorporated

at the Science and Technology Committee hearing titled:

Cyberporn: Protecting Our Children
From the
Back Alleys of the Internet

held

July 26, 1995, Rm 2318, Rayburn Building

INTRODUCTION

Good Morning. I would like to begin by expressing my gratitude to the Chairs of this hearing -- Representative Morella and Representative Schiff. It is my pleasure to have an opportunity to address the panel and participate in today's discussions.

My name is Stephen M. Heaton. I am General Counsel for CompuServe Incorporated.

Although it's my task to represent CompuServe and the industry here today, I also have personal reasons for wanting to be in front of you today. I am a father with several young children who are beginning to explore the online world and the public Internet. So the issues we are discussing today are of a personal interest as well as a business concern.

I will be covering today:

1. A quick overview of CompuServe and its online business.
2. A brief statement on the relationship between the end user and the many sources of computer-based content
3. An acknowledgment of the 'cyberporn' issue
4. Possible answers such as information and education, technology solutions and government and industry cooperation.

COMPUSERVE PROFILE

CompuServe, for those of you who are not familiar with the specifics of our business, is a Columbus, Ohio-based company. We are best known for the CompuServe Information Service (known as "CIS"). By using a computer and a modem, our approximately three million members in 150 countries around the world get access to, among other things, information on every imaginable subject, a variety of entertainment sources and electronic communication in various forms. CompuServe also provides a pipeline to the Internet, where members can access information residing on Internet host computers at universities, corporations and at government agencies.

Without spending too much time on the obvious, or going into too much detail for the time allotted, CompuServe's services allow individuals and businesses to communicate via e-mail, to shop and make travel reservations from their homes and businesses; to access up-to-the-minute news, weather, financial and sports information; to use instructional, educational, scientific and other reference databases, and to participate interactively in special interest discussion forums covering a dazzling array of topics.

Because CompuServe is not the sole source of computer-based information, however, it is extremely important to focus on the end user computer as the central point for any truly effective technology solution to the problem of cyberporn.

You can liken it to a wheel of a bicycle -- the home computer is the hub and each spoke is a potential source of computer-based information. CompuServe would represent one spoke, the Internet another, a government bulletin board another, and so on. Since information parents might find objectionable could come from any of these many sources, technical solutions are best located at the hub so that they are effective as to all information coming into the home or office.

Moreover, placing the primary protections at the hub allows for as much personal choice as possible over what is and is not acceptable -- without needing to entrust these judgment calls to private companies or settling for a one-size-fits-all decision as to what content will and will not be admitted into the home.

CHALLENGES OF CYBERPORN

Of great concern to consumers and to the industry today is the issue of electronic content, available via computer, that is inappropriate for children.

Internet "Newsgroups" may provide a useful example. These are a collection of thousands of online "bulletin boards" available on the Internet, each dedicated to a very specific issue or topic. Although of enormous value -- both potential and real -- Newsgroups also can be places where often language normally considered too coarse for face-to-face conversations is tolerated. Also, like its Newsgroup subset, the Internet itself can also be used for both wholesome purposes and otherwise. For example, it can be used as a medium for the distribution of indecent or even obscene material by individuals who have chosen this medium as a vehicle for their own objectives.

Although only a small part of Internet content and activity, these questionable-to-illegal uses of the Internet, are garnering a tremendous amount of attention. But no matter how relatively insignificant the traffic in this kind of material might be, parents are right to be concerned.

To deal with this issue, we in the industry are committed to empower parents with both education and technology. We want to give parents tools that they can use to block and filter materials *they* deem objectionable.

In addition to the development and distribution of technology-based tools themselves, a related and preliminary goal is to educate our members as to available options and solutions.

-- One such solution CompuServe will be offering is special online area through which information on risks and solutions will be made available. This awareness will also be supported through CompuServe Magazine, a monthly magazine tailored to the CompuServe community. An upcoming issue of the CompuServe Magazine will focus on topics related to children online.

-- Another informational and educational solution is the booklet: Child Safety on the Information Superhighway booklet (HOLD UP BROCHURE). More than a year ago, CompuServe and some of the other online services developed this brochure in cooperation with the Interactive Services Association and Los Angeles Times Columnist Larry Magid. The booklet has received broad distribution and we continue to make it available to parents and I have brought copies with me today for distribution as appropriate.

In addition to educational and information efforts, CompuServe has also addressed the issue of appropriate content through several technical measures it has undertaken and is planning:

-- For example, the search function for CompuServe's Internet access eliminates certain newsgroups that may deal in topics that could be particularly mature in nature. As a result, children are less likely to find those areas unintentionally.

-- We have also worked within our own service -- and continue to do so -- to give our members the option of blocking certain online forums that, as parents, they find objectionable.

-- Our Internet division (SPRY, Inc.) has announced a product called Internet-In-A-Box for Kids, an Internet access product designed to provide Internet access only to pre-designated Internet sites, making it easier for families to safely explore the Internet.

We are also in the process of evaluating third-party software products that will work in conjunction with CompuServe and other points of access. This, we believe, will ultimately be the first and most effective line of defense in managing the nature of computer-based content that is available on the millions of PC's that are -- and will be -- in homes, schools and offices.

Some of these software technology products we are evaluating include: CyberSitter, Net Nanny, Crossing Guard, SurfWatch and others.

Separately, I have printed up a listing of these products and what they purport to do. In the interest of time, I request that I may submit the copies to the panel for you to browse at your convenience.

CompuServe also continues to look at still other options it might have, specific to its own CIS network.

-- For instance, we are looking at ways to build technological blocking and filtering tools, often referred to as 'locks and keys', directly into our interface software. Even novice computer users -- including parents who now ask their kids to set the clock on the VCR -- will find these blocking and filtering tools easy to install, configure, access and use.

-- Finally, but not least, we continue to cooperate with law enforcement and government agencies who work to prosecute those who choose to abuse interactive information media. Contrary to what some would have us believe, the online world is not a lawless Wild, Wild West -- existing laws against obscene and indecent material do apply in cyberspace and are more than adequate to deal with the few who use computer media for illegal purposes.

Worth noting once again, is the fact that many of the solutions we are examining are focused on the one key element in all online activities -- the personal computer.

The Internet was designed to be distributed around the world, with tens of thousands of widely scattered on-ramps and servers. It is constantly changing -- on a daily and even hourly basis. Issues arising on the Internet often entail judgment calls to address them. And there is no central point of control. Because of these factors, it is extremely difficult to conceive of how such an environment could be effectively managed by legalistic regulations and controls. However, the home PC, as the gateway for families into the Internet, is the logical place for empowerment tools to be focused and reside.

Parents cannot control the Internet, but they can control their PC. By providing them access to software tools, new chip technologies or even reminding them that physical locks can be installed on the 'on' switch, we can help them take control of what comes into their homes.

Today, the Internet and Information Superhighway have garnered a tremendous amount of attention among the public, the media and in government circles.

CompuServe welcomes this willingness and interest on the part of government to consider issues that relate to our business. And we can use government's help in a variety of areas. Government can help:

- to educate parents and others about the risks and the benefits of the online environment. The cyberworld is a tremendous resource for education, global communications and entertainment. Yet if an hysteria over issues like pornography prevails, it could inhibit an otherwise outstanding technology and a social and political opportunity.

- to shape laws and policies based on individual responsibility for actions. Today, we have laws on the books to prosecute individuals who deal in obscene and indecent material. We have laws to prosecute people who harass others. And we have laws designed to prosecute purveyors of fraud... all of these laws apply to cyberspace. What's needed is law that makes it clear that companies who responsibly seek to aid parents in controlling their online environment will not suffer liability for doing so.

- to encourage the development and deployment of new technologies that empower parents in shaping their children's experiences in cyberspace. At a time when we as a nation are turning back to parents to take responsibility for their families, parents should be encouraged and empowered to help their children avoid the hazards of cyberspace.

Keep in mind that the online industry is both fast-moving and global. Lately, the industry has completely remade itself every few months. That presents challenges for regulators to stay abreast of the latest developments.

The cyber community, made up of hundreds of thousands of computers distributed across the globe is truly a world without borders. Directly regulating cyberspace -- history's only true functioning anarchy -- may prove impossible. This makes it imperative that laws focus on individual responsibility and that education and empowerment among users and concerned parents be emphasized.

CONCLUSION

I wish to conclude by again thanking the Chairs and organizers of this hearing most sincerely for the opportunity to speak on these timely issues. CompuServe, as a responsible company and as a representative of the Information Services industry, is working hard to address these issues and provide the tools parents want. We are committed to having cyberspace be a safe, enjoyable resource for both parents and their children.

Mr. SCHIFF. Thank you, Mr. Heaton. Because I have another hearing to attend which is going on at this same time, I am going to turn the Chair over to Representative Morella, Chairwoman of the Technology Subcommittee.

Mrs. MORELLA. [PRESIDING] There are so many things competing at this time with this important committee hearing that we have—we have the Waco hearing, there is Whitewater, the base closing, and of course I am hoping that we can have a succinct hearing and have our second panel come on soon, because we are going to also be entertaining a joint address by the President of Korea, and many people have to travel.

But I very much appreciated the fact that you did make such great presentations and have demonstrated to us what this technology is all about.

I guess one of the questions I would like to ask is, I am curious about—and this would be to all of you—the hardware that is used to access the Internet, does it come equipped with the ability to block these pornographic sites?

I guess, Ms. Duvall, it is like, is there a need for SurfWatch—Mr. Rutkowski, Mr. Heaton, do you see this happening with what they call, what, the Router? Would you like to comment on that?

Mr. RUTKOWSKI. I think most of these techniques would be applied at the end-user's computer. There are some exceptions that involve blocking at other points that might be particularly appropriate, for example, for an elementary school where there is what is known as a proxy server that would be used at the gateway to the school, for example. But, generally, it would be effected through software that would reside on the end-user's computer.

Ms. DUVALL. May I comment on that?

Mrs. MORELLA. Yes. I would like to hear your comments, Ms. Duvall.

Ms. DUVALL. Even if you have a server, a central-location computer where everything is coming in, you still need software to be able to block what is there. So this will give many schools and other companies perhaps a choice either to block at a server, a central location, or to block individual computers. But regardless of which way you choose to go, you still need software. It will not be a hardware-based solution at this point.

Mrs. MORELLA. Do you agree, Mr. Heaton?

Mr. HEATON. Neither I nor CompuServe are in the business of manufacturing computers. However, I believe that what is going to drive these solutions more than any law that could ever be passed is going to be the market potential for meeting what the families who will be receiving this information want.

If it turns out that a chip in a computer is the answer, I believe it will be developed. However, I think that we have found that software has overtaken the hardware as a flexible solution. It certainly more easily allows modification and correction than does a hardware solution.

I believe, though, that it certainly could be provided. It is foreseeable that it could be provided as an added feature or option by PC manufacturers who might be trying to provide yet another edge to their products.

So oftentimes what we are really talking about is software that has simply been put in a chip in a hardware-type mode. So maybe we are talking about the same thing, but something in another medium.

Mrs. MORELLA. The reason I posed the question is because I had heard that as a matter of fact with hardware, this was being offered, and maybe more needs to be developed, or more information given. And I guess what you are saying is that software is still the appropriate response to it. But, nevertheless, I think it is important that people do know that with the hardware that there may well be this blocker.

I am concerned about the rating system, of course, but let me ask you about the recent press conference and legislation that has been developed not so much on the Senate side with Senator Exon, but really on the House side with Congressmen Cox and Wyden.

I wondered if you might just briefly like to comment on that? My understanding is that that may well be something that is going to be added to the telecommunications bill, and if you would like to just briefly comment on that, whether you think this is the correct way for a legislative body to move, or whether there would be something more appropriate, or that are not needed.

Mr. HEATON. I would like to comment.

First of all, I think that legislation is at least in part a response to some of the legislation that is on the Senate side. What we have found is that that legislation presents a far better solution that meshes with what the industry and the market is going to do or needs to do.

One of the difficult problems that companies like CompuServe faces on this very issue is a sort of Hobson's Choice.

There was a recent court decision in New York that you may have heard about. It is the *Stratton-Oakmont* decision versus *Prodigy,* another online service. There, Prodigy was shown in the court record to have taken certain efforts to deal with inappropriate material. Some blocking software was used, some word-detecting software was used.

What happened there, what was at issue in that case, was a defamation situation. The court found that because Prodigy had gone to the effort of looking into the content at least somewhat in order to block indecent material, they were found responsible as if they had been looking for defamatory material as well, a wholly different exercise would have been needed.

As a result, they were penalized for being what I think this Committee and Congress would see as a good citizen, and were found liable for defamation that they otherwise would not have been liable for under the law.

So I think that the Cox and Wyden bill represents an opportunity for companies like ours to actually go forward and work wholeheartedly with some of these technology solutions that are coming forward without the fear of inadvertently stepping into a morass of other liability.

Mrs. MORELLA. Briefly, do you agree, Ms. Duvall?

Ms. DUVALL. I support everything that he has just said.

Mrs. MORELLA. Mr. Rutkowski?

Mr. RUTKOWSKI. I would support the same. Again, the concern here is that effective global solutions be found.

Mrs. MORELLA. It was interesting, Mr. Rutkowski, you mentioned in your opening statement that the amount of pornographic material is really infinitesimal, and I think that is probably the case, even though it has gotten the cover of Time Magazine, Newsweek, the various hearings. It is dangerous, but that it is infinitesimal.

Mr. RUTKOWSKI. I think that is accurate. A lot of it is simply on other systems that often get confused with the Internet. It is all lumped under Cyberspace without making the distinctions.

There is obviously, I think, a phenomena, too, where some people are sort of challenging the system. I mean, it is so easy to simply scan anything out of a book and put it on a server connected to the Internet. I think the "hype", so to speak, has obviously engendered some people just to challenge the system.

Mrs. MORELLA. I would like to submit questions to you in writing. In the interest of time, I would like to now turn it over to Mr. Geren for any comments or questions he may have.

Mr. GEREN. I thank you very much.

I have been encouraged to hear how user-friendly some of these blocking systems are. This has been helpful to me in understanding that, and I think what I have read in the press about the avenues parents have to limit their children's access to it have failed to recognize much of the progress that has been made that you all have described today.

The concern I do have, though, is, as I mentioned in my opening remarks, and I think Chairman Schiff did, as well, for many of us our children's knowledge of the computer, just—to say it dwarfs ours is really not an exaggeration at all.

I feel like I have barely missed the information superhighway. I am 43 years old. I am trying to get on it. I got a computer last Christmas. I am crawling along the way, but I am still very intimidated by the whole system. I do not have any idea how to get on the Internet. I am just working my way through some of the basic programs, and I am enjoying my CD ROM.

I say that to try to make the point that the people who are familiar with computers and with the computer industry and younger people who have grown up with it, I do not think really appreciate how computer illiterate many of us are.

I get those books and—and I am not trying to be entertaining, particularly—but I got "Computers for Dummies," or "This Program for Dummies," and I thought when I finally learned how to do this, I am going to write a book that is "Computers for Real Dummies"

[Laughter.]

Mr. GEREN. Because the amount of knowledge that they assume even in some of those computer for dummies' books, for those of us who truly missed the computer age and did not have any of it in our earlier schooling, they do not realize where we are starting on it.

I think, as a parent—I have young children, and my 5-year-old uses the computer much better than do I—and I think the little I know sets me apart of a whole bunch of folks in my generation.

So I think you have a bunch of frightened parents who see that machine and literally do not know now to turn it on. I would have said the same thing a year ago.

I worry that some of you in the industry do not realize, as user-friendly as you think some of these safeguards are, for many of us we do not really take much comfort in that, because we know that our children can defeat any efforts that we have to control what they can do with that computer.

I do not really have a specific question, and I am encouraged that you all have made as much progress as you have and, Ms. Duvall, how easily you jumped from one thing to the other on the Internet and how that Stop Sign appeared. That gave me comfort.

But I do think, as you work with this subject, and it is a tremendous concern to parents, and with movies and books and magazines we try to control our children's access to that, but we have some comfort in at least knowing what we are dealing with.

This is a mystery to people my age and older, just an absolute mystery. You might think that you have taken steps that will comfort most parents, but I can tell you that most of us do not feel that we have the tools to implement them, as user-friendly as you might think they are.

I just think as a Congress, and you in the industry, and you who have taken these kinds of initiatives to protect your children, have to appreciate how far ahead you all are of us.

I have tremendous concerns with any sort of governmental censorship in this area. I think it is truly a slippery slope and I do not want to see it. But I worry that the private industry is not going to give us true computer dummies the tools that we need to feel comfortable that we are able to control what our children are exposed to.

I guess I would like to ask your all's observations on that, because you are working to make things more and more user friendly. What I would encourage you to do is to get a bunch of 45-year-old folks like me that literally do not know how to turn the darn thing on, and see if you satisfy them that what you have done is going to give them the tools to protect their children who are eight years old and can run circles around them.

Mr. Rutkowski? Mr. Gerry Rutkowski, as some might call you? [Laughter.]

Mr. RUTKOWSKI. Close.

I think your concern is a very real one, but let me describe some of the things that are going on. In fact, it occurred last Wednesday in Stockholm.

This Internet Engineering Task Force is not really like a typical industry group. These are the computer geeks who made all this happen, who develop the standards and that are kind of hackers themselves.

As they looked at all the different things that could be done, there was this dialogue. Well, I can hack my way around that with this; and, oh, we can fix it with that. So there is really kind of a remarkable effort by people who really can make many of these tools fairly foolproof for all but probably the most expert, determined kid hacker.

I took great comfort in that kind of dynamic going on. I think there may be, though, some things that may be coming back before Congress.

For example, to make some of this really foolproof, you will need effective encryption technology and that may raise some interesting issues regarding possibly export controls or getting the agreements in other countries to effect.

It may also, even as somebody suggested, involve a role for the Patent and Trademark Office to recognize names for rating services so people can't spoof them.

So I hear your concern, and it is a very valid one, but there are a lot of bright people out there trying to make something that is really foolproof to meet the problem.

Mr. GEREN. Mr. Heaton?

Mr. HEATON. Mr. Geren, I agree again with your warning, really, to be sure that simple is really simple. What I would say in response is, first of all, simplicity is really king, I think, in the marketplace.

I hear constantly about how important it is to be competitive that a system be simple. I think that is simply a fact of life that is being dealt with at a competitive level.

Again, I really believe that given the potential market that is seen in this industry, that competition is going to produce some of these incentives in and of itself to be sure that a system is actually workable and simple.

Secondly, I would say that up-front activation and installation really takes care of the lion's share of this. In other words, the simplicity issue can be addressed at a sort of single point of contact when one first installs a system.

That is where I think some of the activation choices will be. So that it does not take a week's time every month, et cetera, to maintain this to keep up with the complexities. Once it is put into place at the beginning point, that is sort of all you need to do to have taken care of the lion's share of the effort.

Third, I think we will find that some of the technologies will have built into them a sort of default toward a restrictive approach. At least that will be an option, so that one can simply feel safe that, if one does not understand all the options, he or she can select the most restrictive option to start with; and as familiarity with the technology grows, then further remove some of the restrictions as more comfort arises.

I am of the opinion that is how some of the technology will take shape. Also I would say that I have encountered some of the same feelings you have.

When I am presented with a complex transaction, I might be inclined to push it to the side, but I find that oftentimes, once I spend a little bit of time just getting into it, some of the initial mystery just falls away completely and it actually comes down to some fairly basic concepts.

I think that is true of the computer technology, too, especially given the advances that have been made over the last several years. It truly is far, far simpler technology to deal with today than it was just five years ago.

I think people are finding that it does not take days and days but really only a few hours to get beneath the surface of the mystery and be able to work at a very decent level to begin with.

Finally, I would like to say that the booklet that CompuServe and other online companies came up with addresses this issue. One point that it raises is the participation between parents and children.

People in general like to teach others. Children especially love, I think, to be in the position of teaching mom and dad something. It is a wonderful opportunity, and this book promotes it, to sit down with your children and have them teach you a thing or two about the computer.

I think, not only can they teach them, but that helps engender the sort of give-and-take between parents and children that will help this be a cooperative effort on the home level.

Ms. DUVALL. I would definitely support what Mr. Heaton said about having software that would become initially installed that would allow parents to have some blocking technology available to them at installation, would be a wonderful way to go.

But just to let you know from a small company point of view, we have technology that we have developed that we have not released just for the issue that you have mentioned, that we are working on the user interface to make it as simple as possible.

I personally do training of people just your age—in fact, a little older—mothers, and friends of mine. So I feel like I am constantly in touch with the level of knowledge that people have or do not have about computers.

You are absolutely right. There is a fear there, and we address it all the time. I think we have to stay aware of it and on top of it, and it is an issue that is very important in our small company. I think a lot of other small companies also pay attention to that.

The third thing I would like to say is we are finding an incredible response and need for our product in school systems. The teachers who are actually fairly knowledgeable about the Internet are having parental involvement in the classroom and parental classes that they are beginning to teach.

So I am hoping that from the school system where there is some knowledge about the computer, it will also begin to filter into the homes and increase the parents' knowledge of how to use the computer.

Mr. GEREN. Thank you.

I thank the gentlelady.

Mrs. MORELLA. The concept of EvenStart. I would like to ask the indulgence of the Members of the Committee, in terms of time, so we can get the second panel on, as well as our witnesses.

Mr. Ehlers, thank you for waiting.

Mr. EHLERS. Thank you. I will try to speak rapidly. First of all, to reassure my colleagues, Mr. Geren when you write your book if you are searching for a title, perhaps if you called it "Computers for Congressmen" you might have a real—

[Laughter.]

Mr. EHLERS. —best-seller on your hands.

[Laughter.]

Mr. EHLERS. But seriously, it is my experience that Congressmen and busy executives have the most difficult time learning it, because it is a problem of finding the time for the initial instruction.

On a more serious note, Ms. Duvall, I missed your presentation. I was at another meeting, but could you give me in two sentences how your software works? Does it scan on specific words? Or does it identify sites that are questionable and block out things from those sites, or what?

Ms. DUVALL. It does both.

Mr. EHLERS. It does both?

Ms. DUVALL. It does. We have a list of sites that we've identified that we are constantly updating. We also have some algorithms that do some searching on words and phrases.

Mr. EHLERS. And what about blocking visual images? Can it do that, other than blocking from sites?

Ms. DUVALL. It does block visual and textual images.

Mr. EHLERS. But how does it spot questionable visual images?

Ms. DUVALL. We block on the titles of the images, or images that we have actually located and seen. We have over 1500 sites presently that we include in our data base and are constantly adding to that.

Mr. EHLERS. Okay. Another first a comment and then a question.

I have always opposed any legislation that in some way makes the Internet or the online services companies or any of the providers responsible for the content that they are transmitting. I think that is like holding the post office responsible for obscene material that is mailed. That makes absolutely no sense.

However, we have for years been sending questionable materials through the U.S. Mails. It is difficult to enforce, but at least it sets a standard by which people should live.

I am wondering what you would think about the same thing? That we have laws prohibiting transmission of certain types of materials, the same standards we use for the Post Office. After all, there is no difference between the E-Mail and Snail-Mail other than the speed of delivery. Would that create any problems?

It does not affect you as entities. It sets a standard for the Nation of what is proper to transmit, and it does give a hook for getting out those who habitually transmit pornographic material or material that does not meet community standards.

I would appreciate comments from any and all of you on that—and you do not have to talk about the difficulty of the enforcement; I am aware of that.

Mr. HEATON. If I understand what you are suggesting, it is simply a law that addresses those who would initiate the transmission—

Mr. EHLERS. That is correct.

Mr. HEATON. —and simply focus it specifically on an electronic or computer-based activity as opposed to the mail.

My understanding—and I would be happy to address this more specifically in follow-up written comments—but my understanding is that existing laws already address that, would be my first point, in terms of indecent and obscene materials.

We need to keep in mind that part of the issue here is that of definition, as to what can and cannot Constitutionally be regulated.

But to the extent we can define it and it passes legal muster, I think [a] there are already laws that it might fall under, and in fact have been used; but, conceptually, to be more to the point of your question, a clarification that that in fact does apply, however you make that, however you initiate that material, seems to me to be productive.

Again your point, as I understand it, being that it is being aimed at those who initiate, who are responsible for doing things that they ought to know are illegal and wrong, and simply making it clear that it does not matter what medium you use. If you are initiating it, you are responsible.

Mr. EHLERS. Thank you. Any other comments?

[No response.]

Mr. EHLERS. There is agreement on that point. Good.

The final comment, Mrs. Morella, in regard to hardware versus software, I will firmly cast my lot with the responses of the panel that it has to be a software-oriented solution.

If you tried using a chip, it would be different from the television sets where we are talking about putting in a chip to block out certain rated programs. On the Internet, that simply would not work because you have millions of hackers out there who would regard it as a major challenge to bypass any chip that was put in, and I would guess they would succeed very, very quickly.

The software solution is something that is much, much better and can be modified almost instantaneously to counteract any bright hackers who manage to bypass it.

Thank you very much.

Mrs. MORELLA. Did you give those words to Congressman Ehlers? I always defer to him in terms of scientific matters.

Ms. Lofgren?

Ms. LOFGREN. I will be very brief—

Mrs. MORELLA. Thanks.

Ms. LOFGREN. —I know we have another panel, and I also have to go to the Waco Hearings, but I came here because this is a much more important issue for the country and the future of our country.

I am relieved to hear my colleagues express the view that they are for open systems and the First Amendment, and I am, as well.

I think the Exon approach, although I am sure sincere, is totally wrong. It is, as Mr. Ehlers said, like with Snail-Mail, asking the postal worker to accept responsibility. There is a complete misunderstanding of the technology that we are dealing with.

I do agree with my colleague here. We are out of time. It is very interesting. We are in a time of tremendous change in looking at the change that the Net is bringing to society and the world, but we are at this time sociologically where there is this whole group of people who may never get it.

It is like my grandmother always called automobiles "the machines." And yet my 10-year-old is doing basic programming this summer. So we have got to cope with it.

The parents are still calling them "the machines," and I very much agree that we have got to come and help the deficient at least get the tools to provide appropriate parental guidance.

It will never be a substitute for communication, any more than when you send your child off to school there is no guarantee that

your child will not sneak off at recess. But you need the tools to be appropriate as a parent.

I am interested, as we move forward, and I especially want to welcome Ms. Duvall, who is not from my District but certainly nearby. I have two children who love to surf the Net, and I do, too.

When I read your testimony—and I am sorry I missed it—it touched some common cords with me. I take a very tough stance on the creation of child pornography. In fact, I think that is one of the most serious crimes that exists in the country. I offered an amendment in the Judiciary Committee for life imprisonment as a penalty for those who do that. And yet, messing with the Net, is really not going to handle that.

I would be interested, not now but later in writing, if you would give some thought in terms of law enforcement pursuing those who are creating material that is a violation of the law—snuff films, child pornography—are there technological tools that you could recommend that would be of assistance to law enforcement, not to change the law but to help them enforce existing laws in those arenas.

I think if the government gets involved in this, number one, it will mess up the most exciting thing happening in the world. Number two, it will be inefficient. Number three, we will be here for decades waiting for an answer. So I just want to thank you for what you are doing, and encourage you to do more, and have asked you to, at least later, give me some information on that particular subject.

Thank you very much. I did not ask a question.

Mrs. MORELLA. Very good. Thank you.

Mr. GRAHAM. Thank you.

I want to echo the sentiment of do not overestimate our dumbness, or under-estimate it, I guess. I do not have a computer and do not know how to turn one on, so it is my job to get up to speed. But as a lawyer, I do have some concerns. Really this is probably for the second panel, but I would like to ask this group their comments. I have learned a lot from the hearing. Spokes and hubs is a good analogy. I think I understand bicycles better than computers.

From the spoke point of view, is it unreasonable to ask that you be involved in the screening process?

Mr. HEATON. First of all, I guess we are unavoidably involved in it simply because we need to at least be encouraging this kind of conduct.

One, I mentioned in my previous remarks and I will not bore anyone or take time repeating it. There are some legal difficulties the more we get involved with it today.

I believe those difficulties are beginning to be recognized. However, as recently as the New York cases I mentioned, they are not being recognized, or at least it is unclear where you are going to end up, depending on what court or what case you are involved in. So from that perspective, it is at least from a liability standpoint dangerous for us to get too closely involved ourselves.

At the same time, it is impossible for us to be, I think, a growing-concern business and not be involved. That is the Hobson's Choice I mentioned.

So we have got a very difficult tightrope we are walking right now. That is why we are so encouraged to see others besides ourselves taking on this effort so that we can join with those efforts, as well.

The other thing I would say is that, just to get one's hands around the magnitude of the content that one would have to sift through is mind-boggling. Statistics can be provided, but it is just mind-boggling. To expect people to be able to instantaneously—because that is what the market and the technology demands—to sift through that and make difficult choices about what is defamatory and what is not obscene, et cetera, sends all sorts of very, very difficult practical problems. So from that perspective, to address the reasonableness point, I would say it would be an understatement for me to say that that is a challenge.

Mr. GUTKNECHT. Would the gentleman yield, Mr. Chairman?

Mr. GRAHAM. I will gladly yield to the gentleman.

Mr. GUTKNECHT. Madam Chairman—and I thank the gentleman from South Carolina—I want to pursue one quick point.

It has always been said follow the money. I really want to get to how these people get reimbursed for their services.

It seems to me there ought to be a way that government can pull the plug. One of the things we tried to do in the state legislature over the 1-900 calls was make those debts unrecoverable in state courts.

In other words, if people wanted to offer that service, they would do so at their own risk. If people decided they did not want to pay for it, then all of a sudden it would take some of the fun out of this enterprise.

Would you respond to that, Mr. Heaton? Is there some way that we can follow the money and pull the plug?

Mr. HEATON. If I am following you, I think what you are suggesting, though, is if someone is doing something wrong in the first place that we can legally prosecute for.

If that is the case, certainly I think once they are located and the offense is identified and defined, et cetera, clearly whatever remedies the criminal laws provide for can be applied.

In fact, under the RICO laws, which would seem to me a potential situation here, because of the pattern that probably takes place by dealing with a variety of people over and over again, there are very, very strong seizure aspects to those laws which would allow you to pull the profits and even the equipment by which those companies operate.

Mr. GUTKNECHT. But my point is a little more to how these people get paid from the consumer. If consumers were aware that somehow there could be a definition put in place, and that they could not force this issue—in other words, they could not go into court to recover—in other words, if you had an outstanding bill of $500 or whatever, they had no way of legally recovering.

Mr. HEATON. I would have to do a little research, but let me just analogize to the gambling laws.

For instance, my understanding is that a contract for a wager is unenforceable in a court.

Mr. GUTKNECHT. That is exactly my point, and that is the way we pursued it. Gambling debts in the State of Minnesota are uncollectible.

Mr. HEATON. Right. It may well be, I just do not know offhand. That applies to any criminal activity; the law simply will not allow you to enforce a contract for engaging in an illegal activity. That is my guess, but it is only a guess without research.

Mr. GUTKNECHT. So, Mr. Heaton, what you are saying, though in here is that right now consumers cannot be forced to pay for this service?

Mr. HEATON. Well, I think the difficulty is getting to the conclusion that in fact there is something illegal being done of a criminal nature. I think that is the challenge, because as you know there are going to be—I do not know who will raise them, but some of them will—Constitutional challenges when definitions start being drafted and that sort of thing. So I think the real challenge is being able to define a particular activity as definitely being "criminal" in nature.

Mr. GUTKNECHT. I would like to thank the Gentleman from South Carolina. Madam Chair, as we go forward on this I hope we will pursue this particular angle, because I think if we can pull the financial plug, I think we can make a dent in this thing.

Mrs. MORELLA. You have made a very good point, and there will be subsequent hearings connected to this, too. I would like to now recognize the gentleman who has very patiently been here.

Mr. Luther?

Mr. LUTHER. I have no questions.

Mrs. MORELLA. Well thank you very much. I want to thank our panelists very much. And again as I mentioned, I hope that you will be open to receiving questions and responding to the questions that other Members will have who are not here, as well as those who are here.

Thank you very much. I am going to ask the second panel to come before us at the table for their presentations.

Mr. Kevin Manson, who is in the Legal Division of the Federal Law Enforcement Training Center at Glynco, Georgia; Mr. Mike Geraghty, a Trooper from the New Jersey State Police, West Trenton, New Jersey; and Mr. Lee Hollander, the Assistant States Attorney from Naples, Florida. This should be a very interesting panel, giving us a lot of the insight.

I want to welcome you, and look forward to your contribution to our understanding of the difficult issues which surround the investigation and prosecution of computer crime in general, and specifically, Cyberporn.

You have heard some of the questions that Members have had that refer to the kind of testimony you are going to be giving us.

In the interests of allowing the Committee Members to move directly to a dialogue with the members, we are dispensing with the reading of statements. In fact, this panel was not asked to prepare statements, although any material that you may wish to submit for the record will of course be welcome. So I guess I could start off by asking the panel members to respond maybe to a certain question, drawing on their individual experience and knowledge.

I would like to start off and ask you whether or not you have confronted Cyberporn, and what your reaction is to it. So maybe just a general statement in that manner. Would you like to start off in any particular order?

Mr. Geraghty.

STATEMENTS OF MR. MIKE GERAGHTY, TROOPER, NEW JERSEY STATE POLICE, WEST TRENTON, NEW JERSEY; MR. KEVIN MANSON, LEGAL DIVISION, FEDERAL LAW ENFORCEMENT TRAINING CENTER, GLYNCO, GEORGIA; AND MR. LEE HOLLANDER, ASSISTANT STATES ATTORNEY, NAPLES, FLORIDA.

Mr. GERAGHTY. Good morning. Yes. Over the past 18 months I have been working with our Child Exploitations Squad up in New Jersey, along with a Task Force of state and Federal agencies, and over that time period we have taken investigations 20 to 25 or so in number.

We have identified over 80 individuals that we have either arrested or are targeting for arrest. The "Cyberporn," as we call it, is prevalent among this group, but no more prevalent than I think anywhere else in society. It is just a new means that we are finding that pedophiles are distributing this information.

Mrs. MORELLA. Mr. Manson, are there any problems that you have faced, or issues that confront law enforcement people that you have experienced?

Mr. MANSON. Madam Chairman, thank you very much, first of all, for inviting us, and your staff as well.

As far as unique problems, I think Mike hit on one of them. That is, that this is a novelty to many people. There are a lot more people talking about the Internet than actually are coursing its various avenues.

There are some unique problems. One of them was mentioned, or came up this morning in my discussion with Ann Duvall, who asked me where she could go when she found illegal materials.

My job, when I am working at the Federal Law Enforcement Training Center, a part of the Department of Treasury, is basically to teach Cybercops how to obey the law while they enforce it. I should add, though—and I have indicated this in my statement, which I have asked be made a part of the record—that I am here testifying not in an official capacity as part of the Department of Treasury, but in my capacity as someone who is very interested in networking law enforcement agents throughout the world.

Really, there is no single answer to that question. Now, there are many agencies working on this problem now, and it is something that we do need to address. We need to have a simple way for people to be able to reach us when they do have issues that need to be brought to law enforcement's attention.

So I think it is something that is a problem. It is a unique problem to a certain extent, and I think it is unique in part because of the fact that we are dealing with a new medium now.

I think the citizenry has always wanted to know where to go as far as approaching law enforcement, but now in an electronic age it should be much easier than it ever has been in the past.

[The prepared statement of Mr. Manson follows:]

Written Statement of Kevin Manson, Webmaster, @CYBERCOP.ORG

Hearing Before the Committee on Science, Subcommittee on Technology of the House of Representatives on: "Cyberporn: Protecting our Children from the Back Alleys of the Internet"

Wednesday, July 26, 1995

My name is Kevin Manson. I am a SysOp of a Cyber Law Enforcement BBS and Webmaster for the private, non-profit, virtual organization called "@CYBERCOP.ORG". This is also the domain name I have registered on the Internet.

The URL for @CYBERCOP.ORG is:http://well.com:80/user/kfarrand/index.htm

@CYBERCOP.ORG is an Internet site that networks law enforcement professionals, citizens, the on-line business community and other non-profit organizations to provide an on-line venue for "community relations" for law enforcement on the electronic frontier.

I believe that a new collaboration between law enforcement and private sector businesses and organizations which meld technological savvy and a commitment to information security, privacy and civil liberties, will help define the state of the art in cyber law enforcement.

The market place will respond to the needs of parents concerned with adult content on the Net. Ann Duvall's SurfWatch, which I have referenced on the @CYBERCOP.ORG home page, is just one example.

I am submitting a text and HTML copy of the @CYBERCOP.ORG home page to the Committee on disk and would ask that it be included in the record.

I am also the founder and SysOp of the CYBERCOP computer BBS (Bulletin Board System), which is dedicated to networking and education for law enforcement.

Two and a half years ago, using my own personal computer hardware, software and dedicated data line, I developed the first computer BBS at the Federal Law Enforcement Training Center (FLETC) which is a Bureau of the Treasury Department where I serve as a Senior Instructor in the Legal Division. The system was initially created in December of 1992.

In February of 1993 my BBS became the focus of a project I completed in the

highly regarded Professional Development Training Program at the FLETC Management Institute (FMI). That project created the "FLETC FMI Infonet" BBS which was the FLETC's first BBS and served as the prototype for a FLETC BBS which was subsequently created by the FLETC Information Systems Division.

I continue to operate that BBS under a new name, CYBERCOP, as a non-governmental not-for-profit system whose mission is "Networking and education on the electronic frontier". the CYBERCOP BBS allows me to extend my reach as an instructor and permits me to network with professional peers in law enforcement around the nation and across the globe. Several panel members testifying at this hearing are CYBERCOP users.

I have traveled to today's hearing with my family, at my own expense, and on my own time. I would like to emphasize that my statement, comments or responses to questions represent my personal views only, and not those of the Federal Law Enforcement Training Center or the Treasury Department.

My testimony is offered from the perspective of a BBS SysOp and Internet Webmaster who has a strong personal interest in legal, law enforcement, and social issues associated with law and order on the electronic frontier. I also appear as the father of 12 year-old daughter who will grow up to be a "Net Citizen" in the Global Village, and the husband of a para-professional at St. Simons Island Elementary School in Georgia, who is studying the benefits and problems associated with on-line access for staff and students.

I am also involved with a group of interested community members in the Golden Isles of Georgia, where I live, to develop a community "Freenet" to provide free access to the Internet based on the National Telecomputing Network model. The issue of protecting our children from the back alleys of the Internet is critical for such an initiative. I am a frequent Compuserve and Internet user and am a member of the Internet Society and The Electronic Frontier Foundation (EFF).

Author and journalist Bruce Sterling, who serves as liaison between the Austin (Texas) Electronic Frontier Foundation (EFF) and law enforcement, has commented that cybercops are like "shy woodland creatures," noting that finding them on the Net is a bit difficult. Not surprisingly, the I'Way Patrol does not always want its presence publicized on the Net with "marked cars".

However, the lack of a public cybercop presence in the on-line world has contributed to public misunderstanding of the role, mission and attitudes of law enforcement who patrol the On-line world. If law enforcement remains aloof of the public it is sworn to serve and protect it will further exacerbate widespread cynicism that many already feel about government power and authority. Cybercops must have the support and confidence of the virtual communities they patrol every bit as much as the cop on the street. The cybercop's "beat" is relatively unfamiliar territory to the average American over the age of 18.

Unfortunately, cybercops seldom venture outside private, or a few select public venues, that are oriented toward hi-tech crime. The civil liberties community, on the other hand, has been quite successful in its outreach efforts. To that end I created a "virtual organization" on the Net called@CYBERCOP.ORG, where cutting edge law enforcement issues of this new frontier, such as protecting children in cyberspace, are discussed and presented.

Recently, I was invited by Bruce Sterling to participate as a guest "speaker" in a private, on-line "virtual seminar" on the WELL sponsored by the Global Business Network (GBN). Bruce was moderator of one of the Conference topics which dealt with the future of law enforcement on the edge of technology. The GBN is a group of high-powered visionary futurists who were featured in a recent WIRED magazine article.

GBN has taken a leadership position in the concept of "scenario planing", which contemplates planning for the future rather than being overtaken by it. Law enforcement is rapidly finding itself being overwhelmed by technology that traditional organizational paradigms simply cannot manage. Only those organizations willing to make a dramatic break with a regimented bureaucratic structure will survive in the Information Age. Peter Schwartz's conversation with Peter Drucker in a recent issue of WIRED magazine discusses this concept from the perspective of two titans in the discipline of managing change.

Bill Tafoya, who recently retired from the FBI, is a prime example of the kind of non-linear innovator that government must cultivate and empower. Bill was a driving force behind placing the FBI on the virtual street of the Internet to enlist the support of the Net community in the UNABOMB investigation. Bill now heads a think tank group serving police futurist.

The Internet and other computer mediated communications constructs will do no less than revolutionize the concept of "community". It is difficult to

envision any serious or effective attempts to legislate regarding this new communications realm without grasping its unique interactive community nature which makes it neither distinctly a publisher, common carrier nor broadcaster, yet having attributes of each.

If listserv, IRC, talk, CUSeeMe, newsgroups, Web sites and browsers, FTP, Telnet, search engines and intelligence agents are not part of one's vocabulary, the tendency is to treat the Internet as a monolithic, monocultural entity, which would be a mistake.

Those who have not explored the magnificent cultural, scientific, educational and recreational resources on the Internet and on-line services (including the large commercial services and BBS's), are often tempted to "demonize" the Internet by portraying it as being "permeated with pornography", which as Tony Rutkowsky has noted, it is not.

Perhaps the most responsible reportage covering the Internet in the major news weeklies has been US News and World Report's skillful and balanced stories written by Senior Editor Vic Sussman. His January 23, 1995 cover story on "Policing Cyberspace" and recent article on demonizing the Internet deserve a careful read by those who are developing this nation's policy on our national computer mediated communications infrastructure. The insight and perspectives of those articles transcend the narrow sensationalistic reporting seen in recent weeks from other quarters.

On-line services, BBS's and the Internet enable individuals and small groups to communicate, collaborate and cooperate with unparalleled ease. A single person or small team of dedicated individuals can command the same presence on the Net as a multibillion dollar corporation or massive government agency.

In the on-line world, the concept of a web of global collaboration has replaced the strictures of a chain of command. One's status in the world of collaboration is based on sharing information, not hoarding it. "Virtual organizations" cross departmental lines or international borders with equal ease.

Tom Peters in his best seller "Thriving on Chaos" commented that: "Information hoarding, especially by politically motivated, power-seeking staffs, has been commonplace throughout American industry, service and manufacturing alike. It will be an impossible millstone around the neck of tomorrow's organizations. Sharing is a must." Law enforcement is no different. When law enforcement officers and agents gather, the topic of

information sharing is a common one. Law enforcement must not let a lack of sharing between agencies and between management and line staff deflect them from their sworn duties to the public.

The virtual organization can free a tradition bound organization of "meeting paralysis" and empower line staff and management with tools such as video conferencing, document conferencing, and on-line seminars. Thanks to communications pioneers such as Ted Nelson, Tim Berners-Lee and Mark Andreesen, even the computer novice can now navigate complex systems such as the Internet with relative ease. Virtual Organizations consisting of small teams of creative pioneers can be created in a matter of hours.

Small teams meeting on-line will form the attack vessels that will be needed in the war on cyber (and other) crime. The old order of battle was to amass a fleet of powerful, but slow moving, unresponsive battleships in a fleet configuration. We can no longer rely on a lock-step order-of-battle to wage war on the pornographer, transnational criminal organizations, or money launderers.

The future of cyber law enforcement will consist of virtual organizations consisting of small groups of Net savvy cybercops collaborating with Net businesses and private think tanks. These small groups will reinvent the state-of-the-art for law enforcement in cyberspace.

Training cybercops how to patrol the Information Superhighway is a critical task for law enforcement. Unfortunately, cybercops are often saddled with woefully outdated hardware and software and many are paying for Internet or other on-line access out of their own pockets.

Most innovations in the training of Cybercops are being implemented by visionary organizations such as the Financial Fraud Institute at the FLETC, which has been training law enforcement agents about the Internet in programs such as the Telecommunications Fraud Program and the Computer Investigations in an Automated Environment Training Program.

To a great extent, this battle is not unlike the task of fighting other kinds of crime. It will yield to innovative and creative investigative and prosecutorial efforts. The successful application of those efforts will by necessity require very technical and intensive training to put and keep cybercops on the cutting edge of technology.

As a former congressional staffer I must confess that one of the several things I missed the most after leaving Washington was access to the

magnificent library we called our "office library", the Library of Congress. It was a watershed day when Speaker Gingrich announced that private citizens would be able to enjoy even greater access to the Library of Congress than I ever had while working on the Hill.

The dark side of on-line communications must not prevent our teachers, parents, business partners, family members and public servants from reaching out to students, customers, family members and friends in the world of cyberspace.

I am convinced that democracy itself, and the institutions at its core, will be redefined by the personal and institutional relationships that will be forged in this new world. One of the greatest challenges of our age will be to manipulate this technology as a tool for the advancement of civilized values. We cannot simply cower in its shadow.

I remain an optimist about the colonization of cyberspace.

I am heartened that the Subcommittee has provided this venerated venue to discuss an issue which is on the minds of millions of parents and teachers as they weight the opportunities and risks presented by the on-line world and look to Congress for guidance.

I believe that the solution to many of the problems associated with computer mediated communications will be found in a new partnership forged between the on-line community, business, the civil liberties community and law enforcement. To that end I have dedicated my Web site @Cybercop.org.

I would like to publicly thank my wife, Steph, daughter Heather, and Mother, for their unflagging support for their "on-line" father, husband and son. I have dedicate my efforts to my father's memory. He taught me that challenging conventional thinking can open new raods where none existed before. My thanks also go out to those members of my extended "on-line family" who have encouraged and supported the CYBERCOP.

Kevin Manson
kfarrand@well.com
70521.2003@compuserve.com

(Record Submission Follows)

@@
ITEM FOUR: COVER STORY BY VIC SUSSMAN, SR. EDITOR US NEWS AND WORLD REPORT
ABOUT: POLICING CYBERSPACE"
@@

U.S.NEWS & WORLD REPORT, JANUARY 23, 1995

COPS WANT MORE POWER TO FIGHT CYBERCRIMINALS. AS THEIR TECHNO-BATTLE ESCALATES, WHAT WILL HAPPEN TO AMERICAN TRADITIONS OF PRIVACY AND PROPERTY?

If ever a buzzword buzzed too much for traditionbound law enforcement, it's

CYBERCOP. It kicks up images of the clanking earnestness of a laser-guided RoboCop. Agents snickered when senior instructor Kevin Manson first used the word a couple of years ago at the Federal Law Enforcement Training Center near Brunswick, Ga. Nobody at FLETC laughs much anymore. They are too busy training cybercops. "The day is coming very fast," says FLETC's director, Charles Rinkevich, "when every cop will be issued a badge, a gun and a laptop."

Adding a high-speed modem, cellular phone, cryptography textbooks and a bulletproof vest to that arsenal might also be prudent because "crime involving high technology is going to go off the boards," predicts FBI Special Agent William Tafoya, the man who created the bureau's home page on the Internet, the worldwide computer network. "It won't be long before the bad guys outstrip our ability to keep up with them." These crimes are worrisome precisely because they use the advantages of cyberspace that have made it a revolutionary, liberating form of communication: its ability to link millions of computer and modem owners around the world; its technological breakthroughs, such as digital encoding, that allow average citizens to use sophisticated encryption to protect their data, and its wide-open culture, where cops and other agents of government are more often than not thought to be the enemy.

No one knows exactly how much computer crime there really is, though FLETC's experts agree that the damage starts in the billions of dollars and will surely surge upward. The size and scope of cybercrimes are limited only by the bad guys' imagination, technical skill and gall. But here are

the crimes that worry authorities the most:

* WHITE-COLLAR CRIME. Virtually every white-collar crime has a computer or telecommunications link, says Carlton Fitzpatrick, branch chief of FLETC's Financial Fraud Institute. Sometimes the crimes are simple, such as the case of the bookkeeper at a bicycle store who frequently entered incoming checks as returned merchandise, then cashed the checks. Even more damaging are cases involving skilled computerists. The FBI says that Kevin Mitnick, currently America's most wanted computer criminal, has stolen software from cellular-phone companies, caused millions of dollars in damage to computer operations and boldly tapped FBI agents' calls.

* THEFT. Given the expanse of computer networks, even seemingly small crimes can have big payoffs. "Salami slicing," for example, involves a thief who regularly makes electronic transfers of small change from thousands of accounts to his own. Most people don't balance their ledgers to the penny, so the thief makes out, well, like a bandit. A more targeted approach involves pilfering industrial secrets. Last November, someone infiltrated Internet-linked computers owned by General Electric and stole research materials and passwords.

* STOLEN SERVICES. Swiping and reselling long-distance calling codes is a big business, says Bob Gibbs, a Financial Fraud Institute senior instructor, as is breaking into private phone networks and selling long-distance access. One university discovered this the hard way when its monthly phone bill, a staggering $200,000, arrived in a box instead of an envelope.

* SMUGGLING. Drug dealers launder their proceeds through cyberspace and use the Internet to relay messages. Moreover, they cover up secret communications by cracking into corporate voice-mail systems and by operating their own cellular-telephone networks.

* TERRORISM. Since computers are the nerve centers of the world's financial transactions and communications systems, there are any number of nightmarish possibilities. Authorities especially worry that a cracker--cyberspeak for a malevolent hacker--might penetrate FedWire, the Federal Reserve's electronic funds-transfer system, or vital telephone switching stations. Key New York phone systems did go down temporarily in 1992, and though it has been chalked up to a software problem, some FLETC cybercops still wonder if it didn't involve a cracker testing his muscles.

* CHILD PORNOGRAPHY. There is a lot of it out there. Jefferson County, Ky., police Lt. Bill Baker broke a major kiddie-porn ring in England even though he never left Kentucky. An E-mailed tip from a source in Switzerland led Baker to an Internet site in Birmingham, England. After about three months of investigation that involved downloading 60 pages of file names related to child porn and 400 images, Baker called on Interpol, New Scotland Yard and police in Birmingham, who arrested the distributor.

To combat once and future cybercrimes, FLETC's Financial Fraud Institute conducts some 14 programs, regularly updated to keep pace with wrinkles in crime. Agents learn how to analyze evidence, track credit card fraud and apply constitutional search-and-seizure techniques when they find evidence of crimes on computer bulletin board systems, or BBSs. This is a new world for law enforcement, says Dan Duncan, a FLETC Legal Division senior instructor, because "cops have always followed a paper trail, and now there may not be one."

When they start rooting around for crime, new cybercops are entering a pretty unfriendly environment. Cyberspace, especially the Internet, is full of those who embrace a frontier culture that is hostile to authority and fearful that any intrusions of police or government will destroy their self-regulating world. The clash between the subculture of computerists and cops often stems from law enforcement's inexperience. The Internet buzzes with stories of cops who "arrest the equipment" by barging into BBS operations to haul off all the electronic gear, as if the machines possessed criminal minds.

Still, keeping up with wise guys in cyberspace will tax the imaginations and budgets of law enforcement agencies and put revolutionary pressures on America's notions of privacy, property and the limits of free speech. The rights of everyone are at stake. What follows is a look at perhaps the most crucial issues that will emerge as a profoundly new chapter in human communication unravels.

INVASIONS OF PRIVACY

Once upon a time, only Santa Claus knew whether you had been good or bad. But jolly supernaturalism has been supplanted by aggressive data processing: Your chances of finding work, getting a mortgage or qualifying for health insurance may be up for grabs, because almost anybody with a computer, modem and telephone can surf through cyberspace into the deepest recesses of your private life. A fairly accurate profile of your financial status, tastes and credit history can be gleaned from such disparate things

as your ZIP code, Social Security number and records of credit-card usage.

Even more personal information will be available as commercial transactions increase through online services. And that raises the most pressing cyberspace issues for everyday Americans, says Phil Agre, a communications professor at the University of California at San Diego. Such transactions will increase as the Internet grows more popular. Those records, enriched with demographic information and perhaps Social Security numbers, will be routinely sold to marketers, says Agre. He asks: ''Who will have access to the complete transaction data?"

Suppose you have a history of buying junk food or large amounts of over-the-counter drugs. Could an insurance company obtain that information and decide you are a poor health risk? If records showing purchases of cigarettes, liquor and red meat were collated with your medical records, would the picture look even worse? Computer networking and sophisticated data processing are making it easier and cheaper for businesses and the government to collect such personal data, says Esther Dyson, of EDventure Holdings, which observes the computer industry. ''It's really simple to call up amazing stuff about anybody," she says.

But legal access to data is only part of the problem. Another difficulty is unauthorized peeking into personal records, which Dyson says occurs with alarming regularity because company safeguards are often laughable. Knowing a person's Social Security number is usually enough to get into medical and financial records. A second problem is that wrong and harmful ''facts" can creep into the databases. Malicious tipsters can poison a person's record with innuendo, and it takes much effort to correct the mistake.

In this environment, it is virtually inevitable that Americans will demand stronger privacy protections. The United States has a law barring release of video rental records but no strong laws against scanning personal medical data. ''Many European countries have privacy commissions. and they find it strange that we don't," notes Anne Branscomb, author of WHO OWNS INFORMATION? and a law professor at the University of Pennsylvania. She urges laws that give citizens the right to control data about themselves.

The new Congress will soon begin deliberations over proposals that would offer privacy protections for Americans' medical, credit and telecommunications data. Similar proposals have not gotten off the ground in previous Congresses, but handicappers say passage of a bill limiting the

release of confidential medical records is much more likely in this Congress as is a measure to limit online service providers' ability to sell membership data. The potent telemarketing industry probably has the power, though, to soften a proposal barring the sale of personal data to commercial vendors without a person's consent, according to Evan Hendricks, publisher of the newsletter PRIVACY TIMES.

ENCRYPTING DATA

Cybercops especially worry that outlaws are now able to use powerful cryptography to send and receive uncrackable secret communications. That could make some investigations impossible and create a breed of ''cryptocriminals," says FLETC's Manson. But there is widespread agreement across the Internet and among entrepreneurs hoping to do business in cyberspace that cryptography is necessary for privacy in a networked universe.

Besides businesses, which will need cryptography for transmitting sensitive information, the other market for cryptography is the millions who use electronic mail. ''Without encryption, E-mail is no more secure than a postcard," says cryptographer Bruce Schneier, author of E-MAIL SECURITY: HOW TO KEEP YOUR ELECTRONIC MESSAGES PRIVATE. E-mail passes from machine to machine, and many people in the middle can read it. Systems are also vulnerable to break-ins, and passwords are commonly stolen. Some may decide they don't need the high level of privacy cryptography affords, especially given the additional effort encrypting data requires. But as Internet communication becomes common, people will want private contact with business associates, physicians, attorneys, accountants and lovers.

The increasing use of encryption leaves cops in the lurch unless they have a way to break the code. ''We are totally, enthusiastically supportive of encryption technology for the public," says Jim Kallstrom, the FBI special agent in charge of the Special Operations Division in the New York office. ''We merely think that criminals, terrorists, child abductors, perverts and bombers should not have an environment free from law enforcement or a search warrant. I think most victims of crime agree." Kallstrom sees the Clipper chip--which is supposed to offer phone privacy to consumers while providing police access--as a good way to give the public powerful encryption while still preserving law enforcement's ability to conduct electronic surveillance. The FBI won a round last year when Congress passed the Digital Telephony Act, which requires future telecommunications systems to be accessible to wiretaps. But officials have

not persuaded Congress or industry to back Clipper. Many opponents agree with the Electronic Privacy Information Center's Marc Rotenberg, who calls Clipper part of the ``Information Snooperhighway."

Law enforcers are also deeply worried about another aspect of cyberspace that offers absolute anonymity to anyone who wants it. Anonymous re-mailers--free E-mail forwarding sites in Europe and elsewhere--can convert return addresses to pseudonyms and render E-mail untraceable. Anonymity is crucial for whistleblowers and people expressing unpopular views against repressive governments, but it raises other problems, says the FBI's Tafoya. Anonymous re-mailers outside the reach of American authorities are being used by electronic vandals to bedevil their victims with threatening messages or ``mail bombs" composed of thousands of gibberish messages. They either clog a victim's mailbox or jam his computer system. Child pornographers also use anonymous re-mailers.

The simple truth, though, is that no legislative act can stop the spread of cryptography, according to Lance Hoffman, a computer-security expert and professor at George Washington University. ``There are 394 foreign encryption products; over 150 use DES--strong encryption," says Hoffman. ``And all are legal to import."

Cryptography will become even more popular once cybersurfers discover digital cash, which is the electronic equivalent of real money that resides in a computer. David Chaum, the developer of DigiCash, a Dutch-owned company, says his creation combines the benefits of anonymous legal tender with the speed and convenience of online commerce. There is no risky exchange of credit-card information. DigiCash is electronically transferred like actual cash, while powerful cryptography makes it theft-and counterfeit-proof, says Chaum. DigiCash can prevent consumers' names and personal habits from funneling into databases. Schneier thinks the enhanced confidentiality of electronic lucre will be good for society, but suggests that ``criminals will love digital cash. Anybody can use it to transfer money for legal or illegal purposes." Many people believe the widespread use of E-cash will be one more aspect of the Internet that erodes the power of central government control.

FREEDOM OF SPEECH

The advent of space-age telecommunications raises enormous questions about the future of government regulation of media. Though the First Amendment asserts there should be no law abridging freedom of speech or the press, there have been laws aplenty in the last three generations that regulate

speech on new kinds of technology. Different restrictions apply to telephones, radio and TV stations and cable TV. But cyberspace is a convergence of media and the blurring of distinctions between transmission modes. "With the advent of fiber-optic [cables], it is conceivable that a single transmission medium could become the conduit for newspapers, electronic mail, local and network broadcasting, video rentals, cable television and a host of other information services," says Robert Corn-Revere, a former Federal Communications Commission official who now practices First Amendment law. He argues that the day is passing when government can justify licensing and regulating media.

Modern telecommunications knows no borders and has few limits. For the first time in history, almost every recipient of information has the potential to become a publisher of information, says Jonathan Emord, an attorney and author of FREEDOM, TECHNOLOGY AND THE FIRST AMENDMENT. The liberating potential of that technology is exhilarating as it unleashes information and breaks down communications hierarchies. But it also creates a situation where Americans can be offended or otherwise victimized by information from people sitting at computers in foreign lands beyond the reach of U.S. authorities. "Right now, cyberspace is like a neighborhood without a police department," says FLETC's Fitzpatrick.

One of the most pressing dangers, says Fitzpatrick, is that people bound by hate and racism are no longer separated by time and distance. They can share their frustrations at nightly, computerized meetings. "What some people call hate crimes are going to increase, and the networks are going to feed them," predicts Fitzpatrick. "I believe in the First Amendment. But sometimes it can be a noose society hangs itself with."

Of course, the antidote to offensive speech, noted Supreme Court Justice Louis Brandeis, is MORE speech, and the Internet is still an equal-opportunity soapbox. Messages on public bulletin boards can be challenged and rebutted, which widens debate. Moreover, users can go where they choose on the Internet. So, those offended by discussions are always free to start their own groups.

Of all the material floating between computers, pornography best illustrates the difficulties of trying to apply old rules and laws to cyberspace. Late last year, a jury in Memphis, Tenn., convicted a Milpitas, Calif., couple of violating obscenity laws. Using a computer and modem in Memphis, a postal inspector downloaded pictures from the couple's California-based BBS. The couple were tried in Memphis, and a jury found

that the pictures violated local community standards. But the pictures, which existed only as data stored on a hard drive, were voluntarily extracted from a computer sitting in a community where the images were NOT illegal. People create their own communities in cyberspace, based on affinity rather than geography. This means the courts will have to unravel when, where and how potential crimes should be investigated.

Ultimately, there are no easy solutions to such problems because the First Amendment, designed to protect offensive speech, has always cut both ways: It encourages robust and healthy discussion, but it also allows everyone a platform. Mike Godwin, legal counsel for the Electronic Frontier Foundation, which promotes civil liberties in cyberspace, says: "I think we're still in the turmoil that comes when a new medium is presented to the public and to the government. There's a tendency to first embrace it and then to fear it. And the question is, how will we respond to the fear?"

INTELLECTUAL PROPERTY

John Perry Barlow, an Internet visionary, kicked up controversy last year when he suggested in a widely read WIRED magazine article that traditional notions of copyright were dead in cyberspace. "Digital technology is detaching information from the physical plane," he wrote, "where property law of all sorts has always found definition." The government's top copyright officer, Marybeth Peters, partially concedes the point, saying, "The Internet is the world's biggest copying machine." But she says that doesn't mean copyright is useless, just that it needs to work differently in a world where "property" is as evanescent as dots of light dancing on a computer screen.

One way, suggests Peters, will be to provide access to data only to those who pay. An example is WestLaw, an online law database. Students use an electronic card that gives them access to the system, and their law school pays the fee. Other information systems now being developed use encryption, selling the access key to users. But once someone gets a first look at data, sound or graphics files, it is easy to make copies--an economic nightmare for software developers.

TRADE WAR.

Ken Wasch, executive director of the Software Publishers Association, says pirated software costs the industry $9 billion a year. The issue is hot enough to spark a U.S.-China trade war. The Clinton administration recently

LEGAL ISSUES...

As with every crime, there are specific laws which punish illegal activity. Each state in America has statutes which prohibit these acts, and the Federal Government also has laws to punish violators. The Federal Statutes also address copyright violations which includes the unauthorized duplication of software. It is ILLEGAL to make a copy of commercial software for a friend without written permission of the author. Some of the Federal statutes include:

Title 17 Sec. 506 - Copyright infringement.

Title 18 Sec. 641 - Embezzlement and theft.

Title 18 Sec. 1029 - Fraud and related activity in connection with access devices; including trafficking in counterfeit access devices, theft via unauthorized devices, et al.

Title 18 Sec. 1030 - Computer espionage, accessing financial records, unauthorized access to government computer systems, fraud through accessing a federal computer, trespassing onto a federal computer.

Title 18 Sec 1343 - Wire Fraud

Title 18 Sec. 1362 - Malicious Mischief to Government Communications lines or systems

Title 18 Sec 2701 - Unlawful access to stored communications

Penalties for these and other offences range in severity from monetary fines through incarceration, depending upon a number of factors

SUPPORT/RESOURCES AVAILABLE...

There are a number of resources available if you have concerns about the activities of your child. The Navy Family Advocacy Program is able to provide a wide range of counseling services. Additional resources may also be available at your nearest Navy Family Service Center. Your sponsors' command ADP Security Officer may also be able to provide additional information.

Contact your local NCIS Resident Agency or Field Office if you have any additional questions about computer related crime.

NCIS FIELD OFFICES

Camp Lejeune, NC	910-451-8071
Newport, RI	401-841-2241
Charleston, SC	803-743-3750
Norfolk, VA	804-444-7327
Colts Neck, NJ	908-866-2684
Pensacola, FL	904-452-4211
Great Lakes, IL	708-688-5655
Puget Sound WA	206-396-4660
Honolulu, HI	808-474-1218
San Diego, CA	619-556-1364
Los Angeles, CA	909-985-2264
San Francisco CA	510-273-4158
Mayport, FL	904-270-5361
Washington, DC	202-433-3858
Naples, Italy	011-39-81-724-4502
Yokosuka, Japan	011-81-311-743-7535

NCISHQ, Computer Crime Investigation Support 202-433-9293

U.S. Naval Criminal Investigative Service

Computer Crime and The Electronic Frontier

Protecting your children in Cyberspace

A CYBERCOP BBS DOWNLOAD

INTRODUCTION

As a parent you wouldn't think of leaving your child alone in a strange neighborhood, allowing him or her to browse through an Adult Book Store, let them wander aimlessly on a busy street or highway, or let them have secret meetings with strangers. Neither should you leave them alone on the "Information Superhighway" or, in "Cyberspace", as it is sometimes referred to.

As the Department of the Navy's primary investigative and counterintelligence agency, the U.S. Naval Criminal Investigative Service is concerned about the safety of dependant children who are computer active. Certainly a child's interest in computers, ranging from mildly curious to deeply engrossed, is not a crime nor would the vast majority of them even consider it an opportunity to do wrong.

Our concern, however, is from two standpoints: first that they may be targeted for exploitation by the type of criminal who prey upon children, and second are those children who become embroiled in criminal activity either wittingly or unwittingly and are unable to get themselves out. There are numerous documented cases of each throughout the United States.

This pamphlet is designed to provide you, the parent, with a glimpse into Cyberspace along with our encouragement to learn about computers and the environment in which your child interacts. Computers aren't going to go away, nor will the potential problems or adversaries.

SOME DEFINITIONS...

Auto Dial - feature that enables a computer's modem to dial a telephone number and make connection by itself. Sometimes referred to as War Dialing.
BBS - Bulletin Board System. Software which allows the operator, or System operator, to turn his computer into a public forum. After logging in to the BBS, the user can send and receive electronic mail, read news items, or download files they find of interest.
Boot - to start up a computer system.
Byte - amount of space needed to store one character of information.

Kilobyte - (KB) one thousand bites
Megabyte - (MB) one million bytes. (A typical 240mb hard drive could hold up to 27 four drawer filing cabinets of information.
Gigabyte - (GB) one billion bytes.
Terrabyte - (WOW) one million megabytes.

Disk Drive - physical location of disks on a computer. Generally, internal hard drives are usually labeled as C Drive. Floppy drives are generally identified as A Drive or B Drive.
DOS - Disk Operating System.
Down Load - to transfer data, files, pictures from one computer to another.
Floppy Disk - magnetic media capable of storing large amounts of information. Example: a 5 1/4" disk can hold as much as 240 sheets of paper, a 3 1/2" disk can hold as much as 470 sheets of paper.
Graphic File Format - file name extensions used to identify graphic files. The extensions can include: GIF, TIF, PCX, BMP, GL, AVI, DL. FLI, and others.
Hacker - Not necessarily a negative term. A person who learns about computers by trial and error.
Hard Disk - a means of data storage generally located inside a computer, and not removable. The amount of storage varies from 40mb to more than 500mb in newer systems. As the technology develops, storage size will also continue to grow.
Modem - Converts a computers' digital impulses into a series of analog beeps that are sent over a telephone line.
Phreak(er) - one who "hacks" the telephone system to obtain free long distance calling, among other things.
Piracy - the copying and use of computer programs in violation of copyright and trade secret laws.
Program - A series of commands that instructs a computer to perform a desired task.
ROM - Read Only Memory. Currently, CD-ROM disks generally available in read only format. In the future, however, CD's will be able to be written to, as a floppy disk is now.
Scanner - A device which can look at a typed page or a photograph, convert it to digital format, and copy it onto a disk.
Shareware - type of software available on BBS's which is generally free to try. If the user finds the program useful, they are expected to send a nominal fee to the author.
Social Engineering - use of lies, deceit, etc to convince a legitimate user to divulge system secrets or passwords.
Trashing - to scavenge through a businesses garbage looking for useful information.
User Group - informal group with similar types of computers or software who share programs and tips.

POTENTIAL WARNING SIGNS...

Apparent "addiction" to the computer; withdrawal from friends, family, etc. along with a loss of interest in social activities.

Use of new or unusual vocabulary, heavy with computer terms, satanic phrases or sexual reference. Also watch for a sudden interest in posters, music or labels on computer disks which seem satanic or pornographic in nature

Use of words such as Hacking, Phreaking (or any words with "Ph" replacing "F")

Lack of interest in self and appearance or indications of lack of sleep, which may indicate late night modem activity.

Computer and modem running late at night, even while unattended.

Storing of computer files ending in: PCX, GIF, TIF, DL, GL. These are video or graphic image files and <u>YOU</u> should know what they display.

Obsession with computer fantasy/adventure games

Frequent trips to do-it-yourself electronics stores for unusual parts or items.

SOME THINGS YOU CAN DO...

Talk to your kids about their use of the computer. <u>LOOK</u> at the software they are using

Whenever possible, keep the computer in a common area of your home, such as a family room or den

<u>YOU</u> decide if your child has a legitimate need for access to a modem, and if you allow it, monitor the activity, times, and the numbers dialed. Then closely review your long distance telephone bill.

If the computer is left running unattended, check the screen. Take note of what is being displayed and ask about it.

If you are not "computer literate" - LEARN about computers .Take a course or two...ask a friend. .join a Club or User group ..or make the time and learn from your child

SOME MOTIVES FOR HACKING OR OTHER MISUSE OF THE COMPUTER...

- Peer Pressure
- Curiosity/Boredom
- The Challenge/self-esteem
- Vandalism
- Theft, or rumors of easy money

Mrs. MORELLA. Mr. Hollander, as Assistant States Attorney would you like to make any comments on that?

Mr. HOLLANDER. Just that I have given—

Mrs. MORELLA. Pull the microphone closer to you.

Mr. HOLLANDER. I have given legal advice to various agencies in Florida. We are very aggressive about pornography, about pedophiles cruising the net for children. We have—the Florida Department of Law Enforcement has an agent who poses as a young boy on various providers, and he has been solicited, and he invites them to Florida, and they get a tour of the Orange County Jail when they get there.

There are a lot of issues here, not just Fourth Amendment Search and Seizure of the computers that are seized, but the obscenity angle also when you are dealing with pornography. To that extent, the law is developing.

You have got jurisdictional issues such as the Amateur Action Board. The computer was located in California. The postal inspector was in Tennessee. Whose "community standards" apply, Tennessee or California? Because the inspector is the one that actually did the downloading. These photos were not sent to him; he initiated and completed the download to Tennessee. So those are all issues that are going to have to be trashed out in the courts.

Mrs. MORELLA. How do you hear about these cases? Are they because of pedophiles? Is it because parents contact you? Are they in relationship to other crimes? I am kind of curious. And has there been an increase?

Mr. GERAGHTY. All of the above. Initially our first investigation began with the U.S. Customs Service about two years ago.

From that, information developed in that investigation has led to other investigations. It seems like it is a mushroom. Every time that we take down a Bulletin Board system, or arrest a pedophile who uses the computer, there is so much more information in that computer that will lead us off in other directions and in other investigations. It is an ever-expanding tree of investigations that we have.

I want to go back just a second to some of the problems that we do see when we take these Bulletin Boards down in computers. Just as everybody here, as a trooper, as a detective, we have to keep up with the technology. As technology changes, it presents more and more challenges for us to stay abreast of it.

In that light, with some of these systems that we do bring in and we do analyze as evidence, we have to deal with some password protection schemes, and encryption schemes, the more advanced technologies, and how are we going to handle them?

Another aspect of it is that we have got computer systems that we are taking away from the bad guys that are so much more sophisticated than anything we have ever dealt with, and we have no background in it in order to examine it.

And the last thing, which I think is the most unique aspect of child pornography and computers, is the fact that we have to identify these images or pictures on the computer screen as child pornography.

With the computer software out there now, it is simple for a pedophile or anybody else who is in this business to take a picture

of an immature female, okay, who is above the age of 18, who looks very young, to take that body and then superimpose the head of a child on top of that body. That is not defined as "child pornography" although it is serving the purpose of that.

Mrs. MORELLA. You are also saying—and I will let you comment—that you need some education, also. You need that handbook that you talked about.

Mr. GERAGHTY. We need that handbook that Congressman Ehlers talked about.

Mrs. MORELLA. For law enforcement, too.

Mr. GERAGHTY. Yes.

Mrs. MORELLA. Yes, Mr. Hollander?

Mr. HOLLANDER. Just to respond to Representative Gutknecht's question regarding the money, we had a molester travel from Georgia to Florida in our jurisdiction, and he spent a weekend with a young boy. He was subsequently charged.

U.S. Customs and the Georgia Bureau of Investigation took down his Bulletin Board. He had 1000 subscribers. He was charging them $15 a month. That is $15,000 a month. The purpose of that board, besides containing pornography, was to match up older men and young boys. The one consideration that Mr. Gutknecht was talking about was what happens if we do not make the debt collectable in court?

Well, whether it is collectable or not, these people are going to pay because they want to continue to access these boards. That is why I am not sure that that, making them unenforceable, is going to have much of a deterrent effect. These people want to pay. They want continued access.

Mrs. MORELLA. Mr. Manson, do you want to comment?

Mr. MANSON. One thing I just wanted to mention is that, interestingly enough, the three panelists that are appearing before you right now are networked with each other, and we do that in several ways.

We have done it through CompuServe—and I am not here to promote just CompuServe; it happens to be a local call for me, which makes a large difference as far as I am concerned. Also, I had perceived a very important need for communication in networking among law enforcement two-and-a-half years ago, and as a result of that I developed the first Bulletin Board system, computer bulletin board system, at the Federal Law Enforcement Training Center.

I did this with my own software, my own hardware, and basically, I guess it was kind of an early form of reinventing government, if you will. The center did take that idea and it has since developed its own system.

I have continued to operate this system as basically more than a hobby, but really as a professional interest.

I have over 500 users that I am able to try to share the kind of information that you are hearing here today from your panelists so that we can all have the advantage of it.

Mrs. MORELLA. And you are including training courses, too, for those people who are involved in law enforcement? You find that they need technology training, too, do you not?

Mr. MANSON. Absolutely. It is an ever-moving target, and it is a very difficult challenge, but it is one that the Federal Law Enforcement Training Center has worked very hard at, and I am very proud to be a staff member there and be an instructor.

Mrs. MORELLA. Okay. Good. Thank you. I would like to turn it over now to Mr. Geren for his questions.

Mr. GEREN. Thank you, Madam Chair.

I guess what I want to ask each of you to do is just to make suggestions to us as Congress. What would you tell us to do if you could be king for a day, or speaker for the day, and wanted to encourage initiatives on the Congress. What might they be?

After hearing Mr. Hollander talk about pedophiles, using it to solicit their victims, the first idea that comes to my mind is the death penalty, personally.

What sort of other remedies would you all suggest to Congress, or not necessarily remedies, but just tools that perhaps we could give you to help you do your work, recognizing that, you know, we may not accept them, or we may think they go too far, or trample on civil liberties we are not willing to trample on, but if you were just king for a day and could ask us to empower you with the tools that would enable you to make sure that predators do not use the system for their activities?

Mr. HOLLANDER. One of the things that has occurred now is that you all recently amended the Electronic Communications Privacy Act. That was after, I believe, the FBI was in here talking to you.

I am not saying that this is one trade-off between privacy and law enforcement, and this needs to be considered because, by doing that, certain aspects of the amendments made investigative responses more difficult than I feel they should be personally. All right?

And these are just considerations that Congress is going to have to make when you are looking at, well, okay, let us do this, but it also has an effect down the line.

I think that that may be one consideration, especially not just the ECPA, but the access to stored communications and that sort of thing.

E-Mail, for instance. A lot of these salacious messages are coming through E-Mail. Well, that requires jumping through all sorts of hoops for us to get at E-Mail less than 180 days old, and a different set of hoops for over 180 days old.

If you would just please keep that in mind when you are thinking about this one issue—actually, two issues; you have got your pedophiles who are aggressive molesters, and you have got your pornography issue.

Personally, right now I have had more experience with the pedophiles, unfortunately; but some of the privacy acts—and I am not saying that people should not have their privacy, obviously, I like my own—has to be tempered in consideration of other factors.

Mr. MANSON. I guess considering, Madam Chair, the purview of this committee's charter as far as the technology issue is concerned, I understand that some of the issues have to be addressed by the Judiciary Committee and are not necessarily going to be directly addressed by this committee.

But as far as the technology aspects are concerned, I think that it is very important at some point that the Committee have some serious discussions about how we are going to treat the Internet. Are we going to treat it as a publisher? Are we going to treat it as a common carrier? Are we going to treat it as a broadcaster? Because quite frankly, right now I am not even certain that some factions within the Administration are prepared to even come up here and suggest how you should do that.

Last night Reed Hundt was on a chat that I was participating in that *U.S. News* had sponsored on CompuServe. Some questions came up regarding that issue of jurisdiction, and there are not simple answers. It is almost like one waiting for the other to suggest how one should proceed in this area.

I do not have the answers, but I can suggest that one thing about the Internet is that it is not an homogeneous entity. It cannot be treated like any other entity we have seen. It is going to truly revolutionize Democracy. It is going to revolutionize society. I think we have to tread very carefully, but we cannot wait long to take action in this area.

Mrs. MORELLA. I would like to recognize Mr. Barton, the gentleman from Texas.

Mr. BARTON. Madam Chair, did Mr. Geraghty have a comment? He looked like he wanted to say something.

Mrs. MORELLA. I'm sorry. Mr. Geraghty?

Mr. BARTON. He just looked like he wanted to say something. I did not want to cut him off.

Mrs. MORELLA. I would not want to cut you off, either.

Mr. GERAGHTY. I do not think—as far as Congress stands, I think the laws are in place. It is a matter of training law enforcement personnel like myself, the detectives and everyone else, along with the prosecutors and the lawyers and the judges along the line.

Each case that we bring, we draft an affidavit. I spent more time in chambers explaining to the Judge what the computer is, what a Bulletin Board system is, and the same goes for the local prosecutors, the county prosecutors, state prosecutors; that every time we bring a case like that, we have to train these people in just the technology that we are targeting here.

So I think it is a training issue on all parts. I think the laws are pretty good. It is a matter of us learning how to enforce them with this new technology.

Mr. GEREN. Thank you.

Mrs. MORELLA. It probably involves training juries, too, if you have jury trials.

Mr. GERAGHTY. Well, like you will find in just about any pedophile case, they rarely go to a jury. There is usually a plea bargain worked out beforehand.

I do not know if this is true for these cases or not, but we are dealing with technology issues that are advanced. Whether the prosecution feels comfortable with it, and whether the defense feels comfortable with it, may speed their decision to plea bargain before it goes to a jury.

Mrs. MORELLA. Now Mr. Barton, thank you.

Mr. BARTON. Thank you, Madam Chairman. I think this is an important hearing. I have been working on the Energy and Com-

merce Committee with Congressman Klink and Congressman Cox, to perhaps put some sort of an amendment on the Telecommunications Bill that is going to hopefully go to the Floor next week on this issue. We have got an Exon amendment, I think, that has passed the Senate. So my first question is:

I have tried to scan the testimony quickly. Apparently this panel and the previous panel have testified that you do not think we need additional Federal legislation in this area. Is that correct or incorrect?

Mr. HOLLANDER. That would be my opinion.

Mr. BARTON. Okay.

Mr. HOLLANDER. There are laws in place, now.

Mr. BARTON. Mr. Manson, do you concur or—

Mr. MANSON. I would generally concur with that, and I was very appreciative to hear what Mike had mentioned about training, because it is absolutely critical that we have people that are competent and able to handle these cases. Training is absolutely essential.

Mr. BARTON. Well, if in fact it is true that we do not need additional legislation, it is going to be difficult for those of us that support family values to vote against some of these amendments.

The Klink Amendment in the Commerce Committee passed by a voice vote unanimously. The Exon amendment in the Senate, I think, had a handful of negative votes. It is very hard as a Congressman or a Senator to go back to his or her district and say I voted against the amendment that was to prohibit child porn on the Internet.

Mr. HOLLANDER. No one wants to vote against decency; I understand.

Mr. BARTON. So, if in fact we do not need additional legislation, what we do need as decision makers and policy makers here are some ideas fairly quickly about how to enforce the existing laws to assure parents.

I am on this. My PC in Ennis, Texas, is on CompuServe, so we need some fairly quick guidance on how to let the American people know that we are going to enforce the existing statutes such that this information is either not available, or is screened to such a way that only consenting adults can have access to it.

Mr. MANSON. I think we really need to forge a new unity between law enforcement and business. I think the business community is acting right now.

I know that Mark Andreessen and the folks at NetScape, which is the browser—as a matter of fact, it was used here today to view some of these screens on the Internet—are working on voluntary standards.

CompuServe has already mentioned what they are working on now. We have already had representatives testify here today to empower families and empower individuals to take control over this, because this is truly an interactive medium that we are talking about.

Mr. BARTON. If we have to vote for something in this Congress, which of the three proposals that are before the Congress—the Exon amendment in the Senate, the Cox-Largent provision that I do not think has been introduced yet, or the Klink Amendment

that passed the House Commerce Committee, if we have to vote for something, which of those would you prefer we support?

Mr. MANSON. I am not as familiar with the Klink Amendment as I would like to be. I have heard about Cox-Wyden.

Mr. BARTON. The Klink Amendment just requires, I believe the Attorney General, to conduct a study.

Mr. MANSON. That would be similar to Senator Leahy's amendment, then, I would understand, then.

Mr. BARTON. Right.

Mr. MANSON. Well, I certainly think that would be a wise idea, but—

Mr. BARTON. And that is in the bill that has been reported to the Rules Committee.

Mr. MANSON. And I don't know that that is inconsistent with what Cox-Wyden contemplates as far as industry standards. So I don't know that one has to choose one to the exclusion of the other.

Mr. BARTON. Mr. Hollander, do you want to comment on that?

Mr. HOLLANDER. Now that you have explained what the other two were—

[Laughter.]

Mr. BARTON. We talk in inside-baseball so much up here that we don't realize that people in the real world not only do not know, but most of the time do not care. So my apologies for that.

Mr. HOLLANDER. As Kevin said, I would agree with him on those two other amendments. Even as a prosecutor I have several problems with the Exon amendment, both from a—my opinion now—Constitutional, but also putting it into practice from the enforcement angle. So I would be in favor of the other two amendments, whatever names they are.

Mr. BARTON. If we—I am very willing, and I probably have used my time—are willing to try to get existing enforcement updated and beefed up, but if we are going to go that route we really need in the prosecutorial realm, we need some cases and we need some headlines to show that that is literally true; that we can pop the bad guys.

We also need to—and I was not here for the first panel, but the people that have the blocking software need to upgrade their media ability so that parents know—I did not know. I mean, I did not know until I came to the hearing and read in the briefing for the hearing that some of that technology was available for me to put on my home computer. So, Madam Chairman, with that I would yield back. Thank you for holding the hearing. I think it is very important.

Mrs. MORELLA. Thank you, Mr. Barton. I think you posed some very good and appropriate concerns.

I wanted to ask you all, since the examples that you have given basically are on Bulletin Boards run by individuals, it is a separate problem from Internet. I just wonder about how the Bulletin Boards compare with the Internet on the number of cases that come to you?

I would think there would be many more cases that would come from the Bulletin Boards, which again as I say, people do not come to realize there is the division.

Mr. GERAGHTY. Many of our Bulletin Board cases that we have investigated and we have made arrests on have material where it originates from the Internet, and that the system operator of that Bulletin Board system will go out onto the Internet through whatever account it may be, download the graphic images, and then post them on his Bulletin Board for those that are users of the Bulletin Board.

We have had cases where, nowadays, just about every college, every student gets an Internet account when they register. The system operators will steal an account from the university or the college, and they go out onto the Internet and download the pornography and search for the child pornography.

Most of our cases do have links back to the Internet where this stuff originates. Just because it is a local Bulletin Board system, all that does is give those within a certain area code and exchange a chance to call and sometimes make downloads without charging the rates that you would need on a Compuserve or an America Online, or other Internet providers, and stuff like that.

Mrs. MORELLA. Would you like to comment, Mr. Manson or Mr. Hollander?

Mr. MANSON. Madam Chair, I think that one of the issues that has been raised very recently in the popular press has to do with a study that came out of Carnegie Mellon University. I am quite honestly afraid that what had happened in that case is the perspective, not so much the study itself as the way it was portrayed in the popular press, was misleading, quite frankly.

The numbers that were discussed in the study, if one reads it carefully and I have read perhaps two thirds of that study—I tried to read it as I was coming up from Georgia—is quite honestly a small percentage of the images that were covered in the study that came from the Internet.

I do not necessarily disagree with Mike as far as where ultimately some of those images may come from. These days I understand you can get 50,000, or 10,000 or 20,000 images—these graphic images—and put them on a Bulletin Board, and do it at very, very low cost.

What the study really did was to talk about the demographics of selling pornography. I think that we have to take a very close look at this in terms of not demonizing the Internet. I think that is, quite frankly, what has happened.

I do not want to see my wife Stephanie, who teaches in grade school, deterred from taking her students on the Internet, or my daughter, Heather, from being allowed to go on the Internet because we are afraid that bad things may happen there.

It does not keep our schools from doing field trips where it is likewise possible they may have injuries that could be suffered as a result of an auto accident.

So I think that we need to be a little more level-headed and even-handed with this, and that is why I am very frankly glad to see this committee holding these hearings because I think this is a much more calm atmosphere than I am seeing this matter discussed, and that I am afraid is being discussed in many other quarters.

Mrs. MORELLA. That we planned. Thank you. Did you want to comment on it, Mr. Hollander?

Mr. HOLLANDER. I have nothing to add, thank you.

Mrs. MORELLA. Just one final question and I have no others. That is, you know when your children are growing up you tell them don't talk to strangers, be careful of this, et cetera.

What admonitions, or what instructions should parents be giving their children with regard to the perils of the Internet or Cyberporn? Any one of you, or all of you.

Mr. HOLLANDER. Just being on the Internet, or connecting to a local BBSS, report undesirable contacts to the parents, who should report it to the police. Perhaps—and this may be beyond most parents, maybe not—maybe it could be built into the technology we are talking about today to record online sessions.

A lot of communications programs do that now if you set it to do so. And then, finally, a real low-tech method is move little Johnny's computer out of his bedroom and into the living room.

[Laughter.]

Mr. HOLLANDER. The parents are constantly, "Oh, my son never gets in trouble. He is not hanging out in the corner. He is up in his room." Oh, yeah. He is out there doing all sorts of things on that computer because he knows mom and dad—first off, he can hear them coming; and second of all, they have not got a clue. But if he takes the risk of having them walk by and see some image on the screen, he is a lot more circumspect. That would be probably the best thing.

Mrs. MORELLA. Very good. Good point.

Mr. MANSON. I guess it is hard to add much to what Lee said, other than the two very key words "parental supervision," but parents now are struggling to learn about the technology that is necessary to do that.

The National Naval Criminal Investigative Service has published a very interesting little pamphlet that I have made available to your staff and I hope will be included in the record that gives good advice to parents.

The National Center for Missing and Exploited Children has some very fine materials. I publish those on my Bulletin Board, as well, along with pictures of missing children. So I think there are some mechanisms out there available.

Mrs. MORELLA. Did you want to comment on that, Mr. Geraghty?

Mr. GERAGHTY. One thing I would like to add is, just like Mr. Manson said, we see these headlines and we tend to demonize the Internet and the Bulletin Board systems.

Honestly, you cannot find pornography out there unless you go looking for it—on the Internet especially. You have to take a reasoned decision that you want to go looking for child pornography and search it out.

I have been online for a number of years, and I have never been approached. That is both in the capacity of an investigator and in my personal being.

My kids are online all the time, also. They have never been approached. It is just not what is happening out there. Those instances are very far and few between and can only happen under special circumstances.

Mrs. MORELLA. Thank you.

Mr. Geren?

Mr. GEREN. Madam Chair, while we have the members of the other panel here, I wanted to follow up on something that Congressman Barton said.

He is one of those older Americans that is very active on his computer. It interested me that he said that he was not familiar with some of these options that you can use to block access of your children to this sort of information, which surprises me, frankly.

I was not aware at all of the previous panel's testimony until reading it and hearing you discuss it, that those services were out there, and yet we see so much in the press about this subject. You do not see much mention at all of these sort of blocking devices.

I just assume that is just me, the computer illiterate 43-year-old, but for Congressman Barton not to be aware of it, and that not to be part of the public debate on the subject, I think, is really a problem, because you do see parents out there that are scared to death of this, and scared of this machine that is called a computer and wonder what in the world can I do to protect myself, and somebody as active on the Internet and with his computer as Congressman Barton to not know about it makes me think that this public debate we are having is very uninformed.

That is why hearings like this are important, not only to help us learn from you and you learn from us, but to help engage the public in this discussion.

And if he has not been brought along, then there is a whole bunch of us who have not been brought along, because he is way up the scale as far as computer literate folks in this country.

So I hope as we proceed and as the Congress debates some of these issues—in which very important civil liberty issues and issues of privacy, and issues of censorship, and so much of what this country is all about—we need to make sure that the public understands that this is not just the pornographers against the world, and that the Federal Government is all that stands between their children and pornography. They really need to understand what CompuServe has done, and what Ms. Duvall [SurfWatch] has done.

I do not think that is part of the public debate. I think that could lead to Congress doing some unwise things with most of us parents thinking that not much is going on out there that is going to help them.

In the absence of any sort of private sector action, in some of these horrendous things that we have read about that we think could end up in Johnny's upstairs room with him, I can see why the public is demanding action and why Mr. Exon, or some of these initiatives, are popular and some of the concerns about civil liberties take a backseat when it is your 5-year-old and you will do anything you can to make sure your 5-year-old is not exposed to that.

So I do not know what needs to happen. The concern has gotten so much attention, and the potential for abuse has gotten a lot of attention, and these options that are available to parents have not gotten a heck of a lot of attention.

Before we rush headlong into doing things legislatively, I think it is incumbent upon us as a Congress and you in the private sec-

tor, and perhaps you in the law enforcement community, to help make sure our parents understand that there are tools short of somebody up in a big grey building here in Washington putting his or her big old heavy foot down on one of the most important technological developments that is taking place in the world today.

I do not know what we can do about it, because we as a Congress are moving ahead. Joe Barton pointed out how they voiced a vote on this. Are you for or against decency?

That is a pretty hard vote for Congress to make. We have not heard the whole story. I have a feeling we are going to be voting on it before we hear the whole story, and I would just express some concern about that.

I do not know what to do about it, really, but I have a feeling that we in Congress are going to be acting on this before neither we nor the American people understand what is going on out there.

Thank you, Madam Chair.

Mrs. MORELLA. There is no panacea or easy solution. I guess it is parental supervision and understanding. It is education of all of us. It is training in technology and where we are moving.

Having you on this panel has been very helpful to us, and we thank you for the work you are doing and for sharing your experiences and your knowledge.

We thank the panelists on the first panel, also. I think this has been a very good hearing for us, and we appreciate your coming from Georgia, and New Jersey, and Florida to make the presentation and respond to our questions.

Thank you all very, very much.

Mr. HOLLANDER. Thank you, Madam Chairman.

Mr. GERAGHTY. Thank you.

Mr. MANSON. Thank you.

[Whereupon, at 11:25 a.m., the meeting was adjourned.]

APPENDIX

For Immediate Release

Contact:
Jay Friedland
SurfWatch Software
Phone: 415-948-9500
Fax: 415-948-9577
jay@surfwatch.com

SURFWATCH DEMONSTRATES INTERNET BLOCKING SOFTWARE TO KEY MEMBERS OF CONGRESS

Software helps Parents and Educators take responsibility for what children see on the Internet

Washington, July 17, 1995 -- At a demonstration here before key members of Congress, SurfWatch Software, Inc. today announced relationships with America Online and Ventana Communications Group and the availability of SurfWatch™ 1.0 for Windows, the first Internet software product for blocking unwanted sexually explicit material.

"Twenty-five years ago when I wrote the original software which allowed access to the Internet, we had no idea what kind of information would be available," said Bill Duvall, CEO of SurfWatch Software, Inc. "As Congress continues to debate the key issues of protecting our children while maintaining the rights of adults, we believe that SurfWatch can provide a true technological alternative to Internet censorship."

SurfWatch Software creates Internet software products for both Windows and Macintosh platforms and licenses Internet access control technology to the online services industry. SurfWatch is a powerful tool for a wide audience of Internet users, including parents, educators, and employers who wish to reduce the risk of children and others accidentally or deliberately accessing sexually explicit material.

(more)

SurfWatch Software, Inc. • 105 Fremont Ave., Suite F • Los Altos, CA 94022 • Phone: 415 948 9500 • Fax: 415 948 9577
Email: info@surfwatch.com • http: www.surfwatch.com

SurfWatch Demonstrates to Congress — 2 — 2 — 2

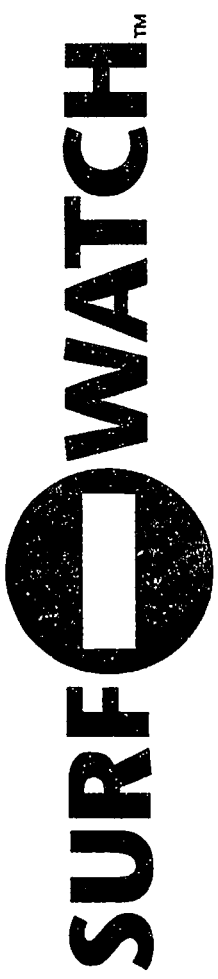
"America Online wants to empower parents with the appropriate tools to restrict access to various parts of AOL and the Internet for their children," said Ted Leonsis, President, America Online Services Company. "Today we are announcing plans to use tools from SurfWatch to expand our Internet parental control capability."

"Ventana has a reputation for exceptional Internet-based software products; we are looking forward to playing a primary role in the distribution of SurfWatch, the most popular Internet parental control software," said Josef Woodman, president of Ventana Communications Group. "Along with our best-selling Internet Membership Kit and NetScape Navigator Personal Edition, we expect very strong demand for SurfWatch in retail stores."

Because new sites appear on the Internet daily, SurfWatch Software also offers the SurfWatch Subscription Service which provides updates to the database of blocked sites. Custom site databases are also available which block according to specific preferences. SurfWatch supports all of the popular browsers and major Internet applications on both Windows and Macintosh. The product works with direct Internet connections via modem (SLIP or PPP), ISDN, or high-speed link.

SurfWatch Software, Inc. based in Los Altos, CA, is pioneering the development of new technologies for the Internet. Founded in January 1995 with a vision of creating high-quality technology products which have a positive impact on peoples' lives, SurfWatch's first products enable parents, teachers, and employers to block sexually explicit material on the Internet. SurfWatch Software can be reached at 415-948-9500 or via the World Wide Web at http://www.surfwatch.com.

—30—



Sexually explicit material is on the Internet.

Do you want your kids to see it? SurfWatch helps you to decide.

Currently there are more than 200 Internet newsgroups which contain sexually explicit material including erotica, bondage, fetishes, pornography, prostitution, and pedophilia. Sites on the World Wide Web contain pictures and written material depicting sexual situations. There has been no way to shield anyone from receiving this material, until now...

SurfWatch

SurfWatch is a breakthrough software product which helps you deal with the flood of sexual material on the Internet. By allowing you to be responsible for blocking what is being received at any individual computer, children and others have less chance of accidentally or deliberately being exposed to unwanted material. SurfWatch is the first major advance in providing a technical solution to a difficult issue created by the explosion of technology. SurfWatch strives to preserve Internet freedom by letting individuals choose what they see.

Parents and Educators

Are your children on the Internet? If so, they have ready access to indecent material. A password protected on/off switch gives you the ability to allow or prevent access. SurfWatch was designed with the aid of caring educators and parents to help protect their children from viewing unwanted material.

Employers

Do you provide Internet access to your employees? Do you know your potential liability as an employer for condoning sexually explicit material in the workplace? Your employees can access the Internet while SurfWatch reduces access to sexually explicit material.

Automatic Updates

SurfWatch comes ready to block hundreds of sites containing material we would not want our children to see.* New sites appear on the Internet daily. We offer a subscription program which updates our list of unwanted sites. If you find a site you feel is objectionable, please let us know.

> ***"This is an important and timely product. We were concerned about our students having unlimited access to the Internet because of all of the indecent material. Now we can install SurfWatch and let them explore the Net."***
>
> ***Susan Larson, Teacher***
> ***Hemingway School,***
> ***Ketchum, Idaho***

Key Features

- Screens for newsgroups likely to contain sexually explicit material
- Keeps your computer from accessing specified World Wide Web, FTP, Gopher, Chat and other sites
- Subscription automatically updates blocked site list
- Customized lists are available
- Fast and easy to install

System Requirements

- Macintosh or Power Macintosh
- System 7.x with MacTCP 2.0 or higher
- Direct access to the Internet via modem, ISDN, or high-speed link
- Not for use with online services (America Online, CompuServe, or Prodigy)
- Windows version available soon

Protect your kids on the Net...

SURFWATCH™

SurfWatch Software, Inc. • 105 Fremont Ave., Suite F • Los Altos, CA 94022
Phone 415-948-9500 • Fax 415-948-9577 • info@surfwatch.com • http://www.surfwatch.com

*Our service is based on our own subjective standards. As a result, we may have blocked sites that a particular user may want available, or we may have made sites available that a particular user would have wanted blocked. Please contact us if you have questions about our policy or are interested in custom site lists.

76

SurfWatch Fact Sheet

SurfWatch Software, Inc.

Vision

SurfWatch Software was founded in January 1995 with a vision of creating high-quality technology products which have a positive impact on peoples' lives.

Mission

SurfWatch Software's mission is to deliver tools which help people better use technology to solve social problems created by the explosion of technology.

Company

- Shipped first product, SurfWatch 1.0, May 1995
- SurfWatch™ is the first Internet software product which blocks sexually explicit material.
- A real alternative to Internet censorship, giving parents and educators the opportunity to limit unwanted material locally without restricting the access rights of other Internet users.
- Announced exclusive retail distribution partnership with Ventana Communications Group, July 1995.
- Licensed SurfWatch technology to America Online, July 1995.
- Proprietary core technology has broad application to solve a variety of Internet and online issues.

Financial

SurfWatch is a privately held company.

Product

SurfWatch 1.0 Overview

- Parents and Educators can use SurfWatch to reduce the risk of children and others accidentally or deliberately being exposed to unwanted material.
- Comes ready to block more than fifteen hundred sites.
- Password protected on/off switch gives the ability to allow or prevent access.
- Employers can use SurfWatch to reduce employee access to sexually explicit material.
- Works with direct Internet connections via modem (SLIP or PPP), ISDN, or high-speed link.

Key Features of SurfWatch 1.0

- Screens for newsgroups likely to contain sexually explicit material
- Keeps a computer from accessing specified World Wide Web, FTP, Gopher, Chat and other sites
- SurfWatch Software offers a subscription service which updates the list of blocked sites.
- Customized site databases are available
- Apple Macintosh version shipped May 1995
- Microsoft Windows version shipped July 1995

Management

- Ann Duvall, President of SurfWatch Software, has performed a wide variety of roles in high-tech over the past 18 years including the formation of four technology start-ups. Her operations experience coupled with her skills as a mother and teacher provide a unique perspective to SurfWatch Software.
- Bill Duvall, CEO, has been involved with founding and developing technology companies for the past 30 years. He has the distinction of writing the software which sent the first packet across the Internet (the original ARPAnet) in 1969 while at SRI.
- Jay Friedland, Vice President of Marketing and Sales, has managed the development, sales and marketing of high-tech products for more than 15 years, including 5 years at Sun Microsystems. Most recently he has assisted Internet start-up companies in establishing new business models for commerce on the Net.

Contact

For more information on SurfWatch Software, please contact:

Jay Friedland
SurfWatch Software
415-948-9500
jay@surfwatch.com

Email:
press@surfwatch.com or
info@surfwatch.com

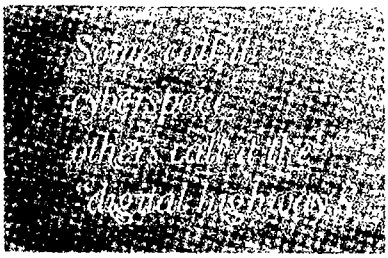
World Wide Web:
http://www.surfwatch.com

Location

105 Fremont Avenue, Suite F
Los Altos, California 94022
Phone 415-948-9500
Fax 415-948-9577
Email info@surfwatch.com

Protect your kids on the Net...

SURFWATCH

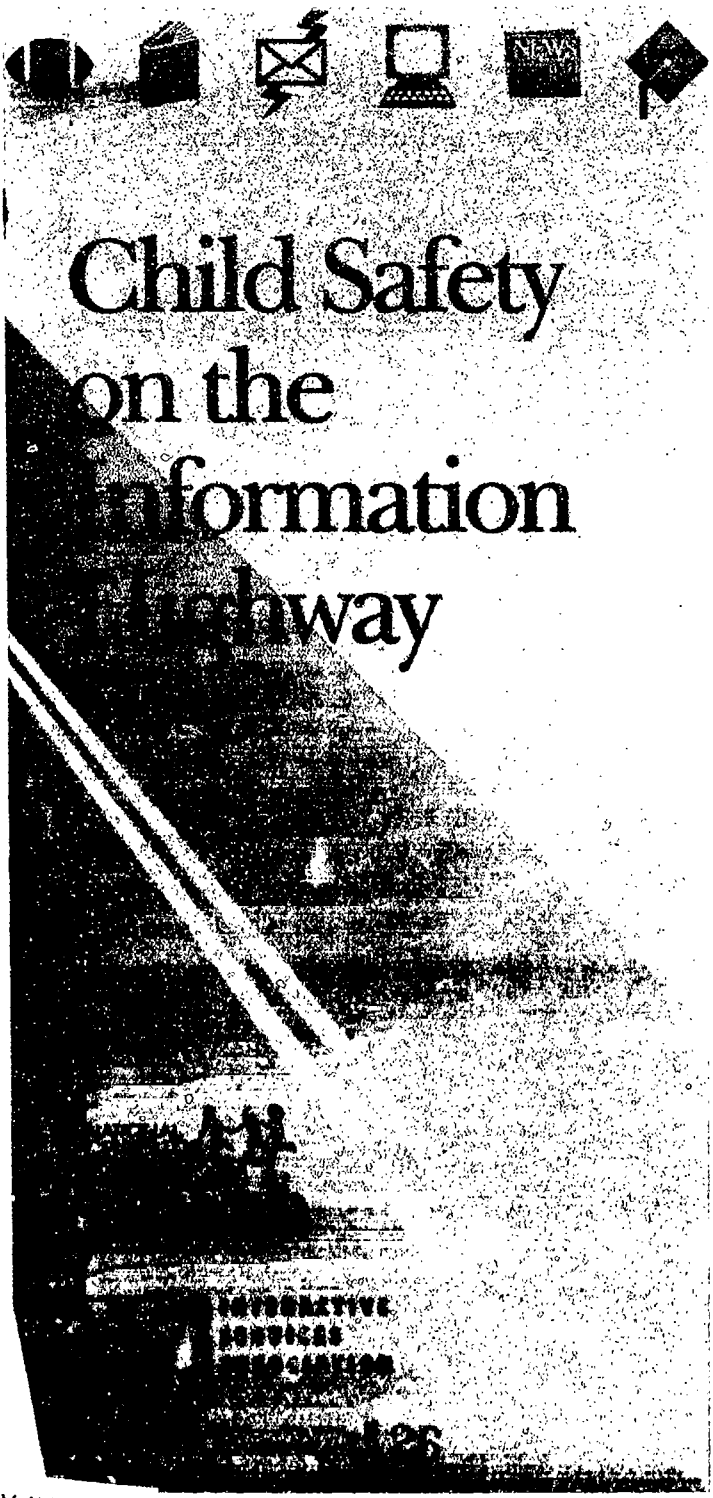


Whatever it's called, millions of people are now connecting their personal computers to telephone lines so that they can "go online." Traditionally, online services have been oriented towards adults, but that's changing. An increasing number of schools are going online and, in many homes, children are logging on to commercial services, private bulletin boards, and the Internet. As a parent you need to understand the nature of these systems.

- Online services are maintained by commercial, self-regulated businesses that may screen or provide editorial/user controls, when possible, of the material contained on their systems.

- Computer Bulletin Boards, called BBS systems, can be operated by individuals, businesses, or organizations. The material presented is usually theme oriented offering information on hobbies and interests. While there are BBS systems that feature "adult" oriented material, most attempt to limit minors from accessing the information contained in those systems.

- The Internet, a global "network of networks," is *not* governed by any entity. This leaves no limits or checks on the kind of information that is maintained by and accessible to Internet users.



Children and teenagers get a lot of benefit from being online, but they can also be targets of crime and exploitation in this as in any other environment. Trusting, curious, and anxious to explore this new world and the relationships it brings, children and teenagers need parental supervision and common sense advice on how to be sure that their experiences in "cyberspace" are happy, healthy, and productive.

Putting the Issue in Perspective

Although there have been some highly publicized cases of abuse involving computers, reported cases are relatively infrequent. Of course, like most crimes against children, many cases go unreported, especially if the child is engaged in an activity that he or she does not want to discuss with a parent. **The fact that crimes are being committed online, however, is *not* a reason to avoid using these services.** To tell children to stop using these services would be like telling them to forgo attending college because students are sometimes victimized on campus. A better strategy would be for children to learn how to be "street smart" in order to better safeguard themselves in any potentially dangerous situation.

Children can learn to be "street smart" to safeguard themselves...



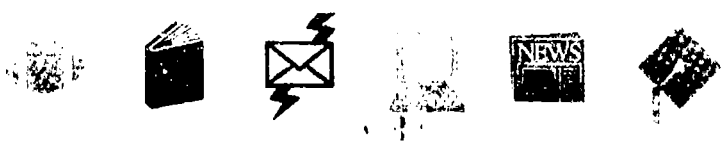


The Benefits of the Information Highway

The vast array of services that you currently find online is constantly growing. **Reference information** such as news, weather, sports, stock quotes, movie reviews, encyclopedias, and airline fares are readily available online. Users can conduct **transactions** such as trading stocks, making travel reservations, banking, and shopping online. Millions of people **communicate** through electronic mail (E-mail) with family and friends around the world and others use the public message boards to make new friends who share common interests. As an **educational and entertainment** tool users can learn about virtually any topic, take a college course, or play an endless number of computer games with other users or against the computer itself. User **"computing"** is enhanced by accessing online thousands of shareware and free public domain software titles.

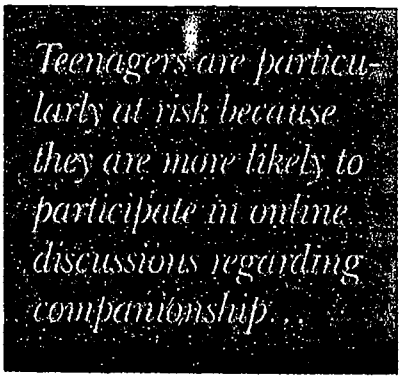
As an educational tool users can learn about virtually any topic...

Most people who use online services have mainly positive experiences. But, like any endeavor – traveling, cooking, or attending school – there are some risks. The online world, like the rest of society, is made up of a wide array of people. Most are decent and respectful, but some may be rude, obnoxious, insulting, or even mean and exploitative.



What Are the Risks?

There are a few risks for children who use online services. Teenagers are particularly at risk because they often use the computer unsupervised and because they are more likely than younger children to participate in online discussions regarding companionship, relationships, or sexual activity. Some risks are:



Exposure to Inappropriate Material
One risk is that a child may be exposed to inappropriate material of a sexual or violent nature.

Physical Molestation
Another risk is that, while online, a child might provide information or arrange an encounter that could risk his or her safety or the safety of other family members. In a few cases, pedophiles have used online services and bulletin boards to gain a child's confidence and then arrange a face-to-face meeting.

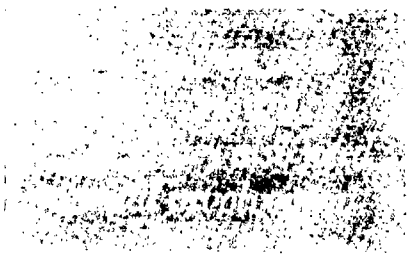
Harassment
A third risk is that a child might encounter E-mail or bulletin board messages that are harassing, demeaning, or belligerent.




How Parents Can Reduce the Risks

To help restrict your child's access to discussions, forums, or bulletin boards that contain inappropriate material, whether textual or graphic, many of the commercial online services and some private bulletin boards have systems in place for parents to block out parts of the service they feel are inappropriate for their children. If you are concerned, you should contact the service via telephone or E-mail to find out how you can add these restrictions to any accounts that your children can access.

The Internet and some private bulletin boards contain areas designed specifically for adults who wish to post, view, or read sexually explicit material. Most private bulletin board operators who post such material limit access to people who attest that they are adults but, like any other safeguards, be aware that there are always going to be cases where adults fail to enforce them or children find ways around them.



The best way to assure that your children are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with your

children while they're online. Have them show you what they do and ask them to teach you how to access the services.

While children and teenagers need a certain amount of privacy, they also need parental involvement and supervision in their daily lives. The same general parenting skills that apply to the "real world" also apply while online.

If you have cause for concern about your children's online activities, talk to them. Also seek out the advice and counsel of other computer users in your area and become familiar with literature on these systems. Open communication with your children, utilization of such computer resources, and getting online yourself will help you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use.

Guidelines for Parents

By taking responsibility for your children's online computer use, parents can greatly minimize any potential risks of being online. Make it a family rule to:

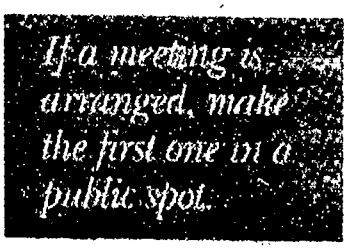
■ Never give out identifying information – home address, school name, or telephone number – in a public message such as chat or bulletin boards, and be sure you're dealing with someone that both you and your child know and trust before giving it out via E-mail. Think carefully before revealing any personal

information such as age, marital status, or financial information. Consider using a pseudonym or unlisting your child's name if your service allows it.

■ Get to know the services your child uses. If you don't know how to log on, get your child to show you. Find out what types of information it offers and whether there are ways for parents to block out objectionable material.

■ Never allow a child to arrange a face-to-face meeting with another computer user without parental permission. If a meeting is arranged, make the first one in a public spot, and be sure to accompany your child.

■ Never respond to messages or bulletin board items that are suggestive, obscene, belligerent, threatening, or make you feel uncomfortable. Encourage your children to tell you if they encounter such messages. If you or your child receives a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your service provider and ask for their assistance.



Should you become aware of the transmission, use, or viewing of child pornography while online, immediately report this to the National Center for Missing and Exploited Children by calling 1-800-843-5678. You should also notify your online service.

■ Remember that people online may not be who they seem. Because you can't see or even hear the person it would be easy for someone to misrepresent him- or herself. Thus, someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year-old man.

■ Remember that everything you read online may not be true. Any offer that's "too good to be true" probably is. Be very careful about any offers that involve your coming to a meeting or having someone visit your house.

■ Set reasonable rules and guidelines for computer use by your children (see "My Rules for Online Safety" on last page as sample). Discuss these rules and post them near the computer as a reminder. Remember to monitor their compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child or teenager's excessive use of online services or bulletin boards, especially late at night, may be a clue that there is a potential problem. Remember that personal computers and online services should not be used as electronic babysitters.

Be sure to make this a family activity. Consider keeping the computer in a family room rather than the child's bedroom. Get to know their "online friends" just as you get to know all of their other friends.

This brochure was written by Lawrence J. Magid, a syndicated columnist for the *Los Angeles Times*, who is author of *Cruising Online: Larry Magid's Guide to the New Digital Highway* (Random House, 1994) and *The Little PC Book* (Peachpit Press, 1993).

Child Safety on the Information Highway was jointly produced by the National Center for Missing and Exploited Children and the Interactive Services Association (8403 Colesville Road, Suite 865, Silver Spring, MD 20910).

This brochure was made possible by the generous sponsorship of:

My Rules for Online Safety

Tear off and keep this pledge at your computer.

- I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.

- I will tell my parents right away if I come across any information that makes me feel uncomfortable.

- I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.

- I will never send a person my picture or anything else without first checking with my parents.

- I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the online service.

- I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

For further information on child safety, please call the National Center for Missing and Exploited Children at 1-800-THE-LOST (1-800-843-5678).

END

U.S. Dept. of Education

Office of Educational
Research and Improvement (OERI)

ERIC

Date Filmed
April 22, 1996

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement (OERI)
Educational Resources Information Center (ERIC)

NOTICE

REPRODUCTION BASIS

☐ This document is covered by a signed "Reproduction Release (Blanket)" form (on file within the ERIC system), encompassing all or classes of documents from its source organization and, therefore, does not require a "Specific Document" Release form.

☒ This document is Federally-funded, or carries its own permission to reproduce, or is otherwise in the public domain and, therefore, may be reproduced by ERIC without a signed Reproduction Release form (either "Specific Document" or "Blanket").