DOCUMENT RESUME

ED 433 007 IR 019 733

TITLE	Legislative Proposals To Protect Children from Inappropriate Materials on the Internet. Hearing on H.R. 3783, H.R. 774, H.R. 1180, H.R. 1964, H.R. 3177, and H.R. 3442 before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce, House of Representatives, One Hundred Fifth Congress, Second Session.
INSTITUTION	Congress of the U.S., Washington, DC. House Committee on Commerce.
ISBN	ISBN-0-16-057747-0
PUB DATE	1998-09-11
NOTE	90p.; Serial No. 105-119.
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/PC04 Plus Postage.
DESCRIPTORS	*Access to Information; Censorship; Children; Elementary Secondary Education; Federal Legislation; Federal Regulation; Freedom of Speech; Hearings; *Information Policy; *Internet; *Obscenity; *Pornography; Public Policy; Standards; Users (Information)
IDENTIFIERS	Child Pornography; *Child Protection; Congress 105th; Filters

ABSTRACT

This hearing addresses legislative proposals to protect children from inappropriate materials on the Internet. Among the issues discussed are federal investments and information access, defining standards for protection, child pornography and marketing to children, filtering technology and adult verification services, and freedom of speech. Included are the statements of: Laith Paul Alsarraf, President and Chief Executive Officer (CEO), Cybernet Ventures, Inc.; John Bastian, CEO, Security Software Systems, Inc.; Jerry Berman, Director, Center for Democracy and Technology; Dan Coats, U.S. Senator from Indiana; Jeffrey J. Douglas, Executive Director, Free Speech Coalition; Bob Franks, Representative from New Jersey; Agnes M. Griffen, Director, TucsonPima Public Library; Ernest J. Istook, Representative from Oklahoma; Andrew L. Kupser, CEO, Northwest Internet Services, LLC; Mary Anne Layden, Center for Cognitive Therapy, Department of Psychology, University of Pennsylvania; Lawrence Lessig, Professor, Harvard Law School; Peter Nickerson, CEO, N2H2; Stephen R. Wiley, Chief, Violent Crimes and Major Offenders Section, Federal Bureau of Investigation. (AEF)

LEGISLATIVE PROPOSALS TO PROTECT CHILDREN FROM INAPPROPRIATE MATERIALS ON THE INTERNET

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

ON

H.R. 3783, H.R. 774, H.R. 1180, H.R. 1964, H.R. 3177, and H.R. 3442

SEPTEMBER 11, 1998

Serial No. 105–119

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
50–939CC WASHINGTON : 1998

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-057747-0

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
DAN SCHAEFER, Colorado
JOE BARTON, Texas
J. DENNIS HASTERT, Illinois
FRED UPTON, Michigan
CLIFF STEARNS, Florida
BILL PAXON, New York
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
MICHAEL D. CRAPO, Idaho
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
RICK WHITE, Washington
TOM COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
THOMAS J. MANTON, New York
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
ELIZABETH FURSE, Oregon
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
THOMAS C. SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado

JAMES E. DERDERIAN, *Chief of Staff*
CHARLES L. INGEBRETSON, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE, AND CONSUMER PROTECTION

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL G. OXLEY, Ohio,
Vice Chairman
DAN SCHAEFER, Colorado
JOE BARTON, Texas
J. DENNIS HASTERT, Illinois
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICK WHITE, Washington
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
TOM BLILEY, Virginia,
(Ex Officio)

EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
BART GORDON, Tennessee
ELIOT L. ENGEL, New York
THOMAS C. SAWYER, Ohio
THOMAS J. MANTON, New York
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

	Page
Testimony of:	
Alsarraf, Laith Paul, President and CEO, Cybernet Ventures, Inc	50
Bastian, John, Chief Executive Officer, Security Software Systems Inc	68
Berman, Jerry, Director, Center for Democracy and Technology	34
Coats, Hon. Dan, a United States Senator from the State of Indiana	1
Douglas, Jeffrey J., Executive Director, Free Speech Coalition	44
Franks, Hon. Bob, a Representative in Congress from the State of New Jersey	17
Griffen, Agnes M., Director, Tucson-Pima Public Library	70
Istook, Hon. Ernest J., Jr., a Representative in Congress from the State of Oklahoma	18
Kupser, Andrew L., Chief Executive Officer, Northwest Internet Services, LLC	65
Layden, Mary Anne, Center for Cognitive Therapy, Department of Psychology, University of Pennsylvania	53
Lessig, Lawrence, Professor, Harvard Law School	57
Nickerson, Peter, Chief Executive Officer, N2H2	61
Wiley, Stephen R., Chief, Violent Crimes and Major Offenders Section, Federal Bureau of Investigations	24

LEGISLATIVE PROPOSALS TO PROTECT CHILDREN FROM INAPPROPRIATE MATERIALS ON THE INTERNET

FRIDAY, SEPTEMBER 11, 1998

HOUSE OF REPRESENTATIVES,
COMMITTEE ON COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS,
TRADE, AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:30 a.m., in room 2123, Rayburn House Office Building, Hon. Michael G. Oxley, presiding.

Members present: Representatives Oxley, Hastert, Cox, White, Shimkus, Wilson, Markey, Sawyer, Wynn, and Green.

Also present: Representative Greenwood.

Staff present: John Morabito, majority counsel; Anthony Habib, legislative clerk; and Andy Levin, minority counsel.

Mr. OXLEY. The subcommittee will come to order.

In the absence of the chairman, who is apparently under the weather, I will take the Chair. We will waive the original opening statements for now until we have an opportunity to hear from Senator Coats.

Senator Coats, if you can come forward. The Senator has a vote on the floor of the Senate, and so we will go out of order a bit and take his testimony.

We welcome Senator Coats from Indiana, our former colleague in the House and also on the Commerce Committee, and he has shown great leadership on the COPA legislation, and we are hoping to replicate his efforts on the House side as well.

A warm welcome from your former colleagues on the Commerce Committee, although there are very few of us left. Welcome.

STATEMENT OF HON. DAN COATS, A UNITED STATES SENATOR FROM THE STATE OF INDIANA

Senator COATS. Thank you. It is a distinct pleasure to come back to this room where I spent, along with you and the esteemed chairman, a lot of hours, most of them on the lower tier, I would say, and so it is particularly pleasing to come back and see one of my former colleagues here in the House occupying the chair, and I appreciate the opportunity to come and testify to you today.

I apologize for asking to go out of order. We are in the midst in some votes in the Senate, just having completed the cloture vote, and then another vote is pending.

On November 8 of last year, I introduced S. 1482, which has been subsequently unanimously adopted by the Senate and attached to our Commerce-State-Justice appropriations legislation. This legislation was designed to require commercial pornographers on the Web to restrict access by minors to pornographic material. Subsequently you and Congressman Greenwood on April 30, 1998 introduced counterpart legislation which you will be discussing today.

Our efforts are the product of a Supreme Court ruling in Reno v. ACLU, which struck down the indecency provisions of the Communications Decency Act, which Senator Exon and I put together over in the Senate and successfully passed there. However, it did not survive court scrutiny in all of its aspects, and I will discuss that in a moment, but this legislation that we are discussing today is the natural follow-on to that decision.

The bill which we are discussing requires that commercial pornographers on the Web take certain steps designed to restrict access by children to pornographic material. These steps include requiring a verified credit card, adult access code or PIN number. Fines and penalties under the legislation are identical to those imposed under the dial-a-porn laws which have passed and have survived court scrutiny.

It is first important to note that the Court did not strike down the entire Communications Decency Act; rather, the Court only struck down the indecent and patently offensive sections of the CDA. For example, the obscenity provisions of the act were not challenged and remain good law today. This is significant in the face of false arguments claiming that the Court established that pornographic material on the Internet cannot be regulated. It can be, and it is.

In fact, at the outset of its ruling in Reno, the Court reaffirmed that "the government has an interest in protecting children from potentially harmful materials," and acknowledged "the act's legitimate purposes." It is this compelling government interest and legitimate purpose that the legislation we are discussing today seeks to address.

The bill was carefully tailored to conform with the concerns outlined in the Court's ruling in the CDA. For instance, the "harmful to minors" standard adopted in this legislation was first upheld by the Supreme Court in Ginsberg v. New York. The New York statute prohibited the selling to minors under 17 years of age any material that was considered obscene as to those children even if not obscene to adults. It is a content standard familiar to the debate surrounding Internet regulation. In fact, Representative White offered the "harmful to minors" content standard as a modification to the CDA during the House-Senate conference of the Telecommunications Act as a compromise, which then was widely supported by the computer industry.

The Supreme Court found four primary differences between the CDA and the statute upheld in Ginsberg, and I would just like to briefly discuss those because we have attempted to address those concerns in this legislation. First the Court pointed out that, in Ginsberg, "the prohibition against sales to minors does not bar parents who so desire from purchasing the magazines for their chil-

dren." Now, it is hard for me to imagine why any parent would want to do this, but in accordance with the First Amendment protections, the Court indicated that in Ginsberg, that this prohibition of sale to minors will not bar parents who so desire to purchase that magazine for their children. Our legislation in no way prohibits parents from taking such actions. Much as I would like to do that, we feel constrained to comply with the Court's decision.

Second, the New York statute applied only to commercial transactions. Again, the scope of the 1482 and the Oxley-Greenwood legislation is strictly limited to commercial transactions. The operative term in the bill is "engaged in the business of," which is assigned the same definition contained in section 1466 of Title 18 of the U.S. Code. Section 1466 regulates the trafficking of obscene material.

The Court also pointed out in Reno the New York statute upheld in the Ginsberg decision combined its definition with the requirement that the material be without "social importance to minors" and that the material "lack serious literary, artistic, political or scientific value." By adopting the construction followed in the New York statute, these concerns are directly addressed. This ensures that the bill may not be construed as to restrict access to public health information, important works of art, literature and political information.

The "harmful to minors" standard is a three-prong test. It requires that the material appeal to the prurient interest, that it be patently offensive as to what is suitable to minors, and that taken as a whole it lacks any serious literary, artistic, political or scientific value as to the minors. All three prongs must be met for the material to be determined as harmful to minors.

Fourth, the New York statute defined a minor as a person under the age of 17. Our legislation adopts the same "under the age of 17" requirement.

Thus, each concern regarding the content standard outlined by the Court in Reno is specifically addressed under this legislative approach.

The use of credit cards, access codes and PIN numbers is standard technology for commercial activity on the Web. The Court acknowledged as much by stating, "Technology exists by which an operator of a Web site may condition access on the verification of requested information such as a credit card or an adult password." Further, the Court stated that although such verification is actually being used by some commercial providers of sexually explicit material, the district court's findings indicate that it is not economically feasible for most noncommercial speakers.

So, again, in a direct response to the Court's concerns, this legislation is strictly limited to the Web, where the Court established technological feasibility, and to commercial Web sites where the Court has established economic feasibility.

In fact, regarding this economic feasibility question, adult verification services, or AVSs, generally provide their services free of charge to Web site operators, even providing a kickback to site operators for customers referred to them. Therefore, it is not only economically feasible, but often profitable to use an AVS service.

Although credit cards likely will continue to be the most widely used access restriction measure, AVS services provide for other

means of verification and payment for adults who do not possess a credit card. As to the effectiveness of credit cards, though there are no laws specifically requiring that minors not be issued credit cards, the use of credit cards fall under State contract law to the extent that a contract entered into by a minor is unenforceable. Even then under this legislation the commercial operator is not held liable for the industrious minor who succeeds in defeating any of the proscribed access restriction measures. Rather, as the legislation provides, the commercial provider and operator enjoys a defense from prosecution simply by having the access restriction measures in place.

Another argument offered for those who would defeat efforts to protect children from this online smut material is that the Internet is a global medium that defies regulation and enforcement. On this point we need look no further than the headlines of the past few weeks, of the story of a multinational crackdown on an online child pornography ring. The details of this successful law enforcement effort point to the hollowness of the "unenforceable" argument.

In summary, the Oxley-Greenwood bill introduced as a companion to my Senate bill is a carefully crafted response to the Supreme Court's ruling in Reno v. ACLU.

I would like to close my remarks by reading from a letter sent to me by a group of teachers and administrators at South Knox High School in southern Indiana, and I think it states it better than any of us can.

Senator Coats, we are writing to express our concerns about the use of the Internet by America's children. We are all in agreement that the Internet is a technology that is and will be of enormous benefit in our classrooms. However, our concerns are with the magnitude of pornography on the Internet, and our inability to protect our students as we struggle to keep up with technology and to place computers in all of our classrooms.

In our school, students must be supervised by a teacher while using the Internet. But, as we move the Internet from the library into our teaching classrooms, constant supervision will not always be possible.

The school where we work and teach has two security blocks on our Internet system. We use both Cyber Patrol and Fortress. What we now know is that there is no blocking system available to us today that is adequate. We have one person in charge of the computer system in our school system who could work full time just blocking pornography that teachers and students have found and reported.

We are all working hard to make it possible for the students at South Knox High School, a small rural school, to have Internet exposure. Yet, Senator, how are we supposed to know that if you type in "Fiesta" on the Internet, you may get a bare-chested woman posing in a suggestive manner? We have seen pictures on the Internet in our school library of a man and woman participating in oral sex. We have also seen tattooed penises and testicles. If a child wants to look up a type of doll that she has, she can type in "water baby." One of the choices is a site with an adult woman naked except for a wet diaper, or a woman pictured from behind urinating in her underwear.

We spend 180 days, 8 hours a day, 5 days a week caring for and educating America's children. We must have a safeguard that works for the Internet during school hours so that we may keep up with the world, yet not have our children innocently exposed to pornography.

That letter is signed by a group of 19 teachers and administrators.

Sometime in the next few weeks, Congress will consider legislation that would establish a moratorium on Internet taxation. I, like so many members of this committee, generally support that effort. However, I think it would be a sad and indeed inviable proposition if Members of Congress acted to provide a tax shelter for commercial porn sites on the Web without first requiring them to take responsible measures to protect children from exposure to the smut they peddle for profit on that same web.

I want to thank you, Mr. Chairman, for the opportunity to appear here today. I commend the leadership of you and Congressman Greenwood in taking up this fight in the House of Representatives. I trust that you will gain the same kind of support that I was able to get in the Senate, which passed, as I said, by a unanimous vote the legislation we offered. It meets the constitutional requirements that the Court laid out when it rejected the CDA which did not comply with the Court's constitutional requirements.

We believe that this addresses a problem that invades every home in America that has a computer and every classroom in America that has a computer. We think that it is a reasonable means by which we can protect minors from unrestricted access to material that is not appropriate.

Mr. Chairman, thank you again for the opportunity to appear here today. I want to say hello to my colleague, the ranking member, and just repeat that I have had the privilege of spending many hours in this very room, sometimes on the side and sometimes on the opposite side of all of the members here, and it is a pleasure to be back.

Mr. OXLEY. Welcome back to the committee. You have raised the bar quite high for Mr. Greenwood and I to reach. We will do our best to try to emulate your success in the Senate. We know that you have the votes in the Senate, and we appreciate your testimony.

Senator COATS. I thank you.

[The prepared statement of Hon. Dan Coats follows:]

PREPARED STATEMENT OF HON. DAN COATES, A U.S. SENATOR FROM THE STATE OF INDIANA

I would like to begin by thanking the distinguished Chairman and Members of the Committee for providing me the opportunity to appear before you today.

On November 8 of last year, I introduced S.1482. This legislation is designed to require commercial pornographers on the Web to restrict access by minors to pornographic material. Subsequently, Congressmen Oxley and Greenwood, on April 30 of this year, introduced the counterpart legislation that will be discussed today. This legislative effort is a product of the Supreme Court ruling in *Reno v. ACLU* striking down the "indecency" provisions of the Communications Decency Act or CDA. The bill requires that commercial pornographers on the Web take certain steps designed to restrict access by children to pornographic material. Fines and penalties under the legislation are identical to those imposed under the dial-a-porn laws.

It is first important to note that the Court did not strike down the entire CDA. Rather, the Court struck down the "indecent" and "patently offensive" sections of

the CDA. For example, the obscenity provisions of the Act were not challenged and remain good law today. This is significant in the face of false arguments claiming that the Court established that pornographic material on the Internet cannot be regulated. It can, and is.

In fact, at the outset of its ruling in *Reno* the Court reaffirmed that "the Government has an interest in protecting children from potentially harmful materials," and acknowledged "the Act's legitimate purposes."

It is this compelling Government interest, and legitimate purpose that this legislation seeks to address. The bill is carefully tailored to conform with the concerns outlined in the Court's ruling in the CDA.

The "harmful to minors" standard adopted in this legislation was first upheld by the Supreme Court in *Ginsberg v. New York*. The New York statute prohibited the selling to minors under 17 years of age material that was considered obscene as to them even if not obscene to adults.

It is a content standard familiar to the debate surrounding Internet regulation. In fact, Representative White offered the "harmful to minors" content standard during House/Senate conference of the Telecommunications Act as a compromise widely supported by the computer industry.

The Supreme Court found four primary differences between the CDA and the statute upheld in *Ginsberg*.

First, the Court pointed out that in *Ginsberg* "the prohibition against sales to minors does not bar parents who desire from purchasing the magazines for their children." This legislation in no way prohibits parents from taking such action.

"Second, the New York statute applied only to commercial transactions."

Again, the scope of this legislation is strictly limited to commercial transactions. The operative term in the bill is "engaged in the business," which is assigned the same definition contained in Sec. 1566 of Title 18 of the U.S. Code. Sec. 1466 regulates the trafficking of obscene material.

The Court also pointed out in *Reno* the New York statute upheld in the *Ginsberg* decision cabined its definition with the requirement that the material be without "social importance to minors" and that the material "lack serious literary, artistic, political, or scientific value."

By adopting the construction followed in the New York statute these concerns are directly addressed. This ensures that the bill may not be construed as to restrict access to public health information, important works of art, literature, and political information.

The "harmful to minors" standard is a three-prong test. It requires that the material appeal to the prurient interest, that it be patently offensive as to what is suitable to minors and that—taken as a whole—it lack any serious literary, artistic, political, or scientific value as to minors. All three prongs must be met for the material to be determined harmful to minors.

"Fourth, the New York statute defined a minor as a person under the age of 17." Our legislation adopts the same "under the age of 17" requirement.

Thus, each concern regarding the content standard outlined by the Court in the *Reno* is specifically addressed under this legislative approach.

The use of credit cards, access codes and PIN numbers is standard technology for commercial activity on the Web. The Court acknowledged as much stating: "Technology exists by which an operator of a Web site may condition access on the verification of requested information such as a credit card or an adult password." Further, the Court stated: "Although such verification is actually being used by some commercial providers of sexually explicit material, the District Court's findings indicate that it is not economically feasible for most non-commercial speakers."

Again, in a direct response to the Court's concerns, the legislation is strictly limited to the Web, where the Court established technological feasibility, and to commercial Web sites where the Court established economic feasibility.

In fact, regarding this economic feasibility question, Adult Verification Services, or AVSs, generally provide their services free of charge to Web site operators, even providing a kick-back to site operators for customers referred to them. Therefore, it is not only economically feasible, but often profitable to use an AVS service.

Though credit cards likely will continue to be the most widely used access restriction measure, AVS services provide for other means of verification and payment for adults who do not possess a credit card. As to the effectiveness of credit cards, though there are no laws specifically requiring that minors not be issued credit cards, the use of credit cards fall under state contract law to the extent that a contract entered into by a minor is unenforceable. Most states define minors as those under 18 (some may use 21).

The practical effect of this is rare access to credit cards by those under 18. Even then, under this legislation, the commercial operator is not held liable for the indus-

trious minor who succeeds in defeating any of the proscribed access restriction measures. Rather, they enjoy a defense from prosecution simply by having the access restriction measures in place.

Another argument for those who would defeat efforts to protect children from on-line smut is that the Internet is a global medium that defies regulation and enforcement. On this point, we need look no further than the headlines of the past few weeks, of the story of a multi-national crackdown on an on-line child pornography ring. The details of this successful law enforcement effort point to the hollowness of the "unenforceable" argument.

In summary, the Oxley/Greenwood bill, introduced as a companion to my Senate bill, is a carefully crafted response to the Supreme Court's ruling in *Reno v. ACLU.*

I would like to read from a letter sent to me by a group of teachers and administrators at South Know High School in Southern Indiana:

"Senator Coats, We are writing to express our concerns about the use of the Internet by America's children. We are all in agreement that the Internet is a technology that is, and will be, of enormous benefit in our classrooms. However, our concerns are with the magnitude of pornography on the Internet, and our inability to protect our students as we struggle to keep up with technology and to place computers in all of our classrooms.

"In our school, students must be supervised by a teacher while using the Internet. But, as we move the Internet from the library into our teaching classrooms, constant supervision will not always be possible.

"The school where we work and teach has two security blocks on our Internet system. We use both Cyber Patrol and Fortress. What we now know is that there is no blocking system available to us today that is adequate. We have one person in charge of the computer system in our school system who could work full-time just blocking pornography that teachers and students have found and reported.

"We are all working hard to make it possible for the students at South Knox High School, a small rural school, to have Internet exposure. Yet, Senator, how are we supposed to know that if you type in Fiesta on the Internet, you may get a bare chested woman posing in a suggestive manner? We have seen pictures on the Internet in our school library of a man and woman participating in oral sex. We have also seen tattooed penises and testicles. If a child wants to look up a type of doll that she has, she can type in water baby. One of her choices is a site with pictures of adult women, naked except for a wet diaper, or a woman pictured from behind, urinating in her underpants.

"We spend 180 days, eight hours a day, five days a week caring for and educating America's children. We must have a safeguard that works for the Internet, during school hours, so that we may keep up with the world yet not have our children innocently exposed to pornography."

Sometime in the next few weeks Congress will consider legislation that would establish a moratorium on Internet taxation. I, like so many Members of this Committee, generally support this effort. However, I think that it would be a sad day indeed if Congress acted to provide a tax shelter for commercial porn sites on the Web without first requiring them to take responsible measures to protect children from exposure to the smut they peddle for profit.

I thank the distinguished Chairman for the opportunity to appear here today. And I commend the leadership of Congressmen Oxley and Greenwood in taking up this right in the House of Representatives.

Mr. OXLEY. The Chair will now go back to regular order with the opening statements.

The subcommittee meets today to consider proposals on how to protect children from inappropriate material on the Internet. It is a serious and growing problem, and a number of measures have been referred to the committee for its consideration.

I want to commend Chairman Tauzin and Chairman Bliley for calling today's hearing. This is an issue of great concern to a number of members of the committee. I thank our witnesses for taking the time to address the issues that confront us, especially the FBI and Dan Coats, who did an excellent job for setting out the case for the COPA legislation.

Congressman Greenwood and I have introduced a companion bill, the Child Online Protection Act, or COPA, requiring commercial adult Web sites to screen out minors. It is sponsored by 53 Mem-

bers of the House, including 20 members of this committee. It is endorsed by a coalition of 17 profamily and religious organizations throughout the country.

Freedom of speech is perhaps our most fundamental liberty, yet I seriously doubt that the Founding Fathers meant to protect the right of commercial pornographers and pedophiles to subject children to hardcore images. My colleagues, that is exactly what is happening in America today in homes, classrooms, and libraries across this country.

A recent national poll found that the No. 1 concern on the minds of voters is the moral decline of our society. We as a Nation hope to address the coarsening of our culture and the loss of values among our young people. We have to begin by addressing the most serious threat, to do so by protecting kids from the degrading content readily available on the Internet.

I am sure that everyone here is aware of last year's highly publicized molestation and murder of 7-year-old Sherrice Marie Iverson in a Las Vegas casino bathroom by the now 19-year-old who recently pled guilty to her murder, but few people are aware that the killer's own attorney testified that he had been a normal teenager and an honor student until Internet pornography took over his life. Police found vast files of hardcore material, including graphic child pornography, on the boy's home computer all downloaded from the Internet.

Some opponents of the Coats-Oxley-Greenwood bill will say all we need to do is promote screening software. I support screening software and cosponsored the bill introduced by our next witnesses, the gentleman from Oklahoma and the gentleman from New Jersey. It is my belief that the commercial providers of this smut ought to bear some responsibility for shielding it from the eyes of children.

Other opponents will say that voluntary industry measures are the answer, but I frankly doubt the sincerity of Internet pornographers to do anything effective about the problem or voluntarily abide by any standards that might be set. We hear about self-regulation whenever it looks like Congress might act on legislation, and then it quietly fades away.

It is quite true, as will be pointed out many times today, that the Supreme Court struck down most of the provisions of the Communications Decency Act. Members who were fellow conferees on the Telecom Act will recall I had serious reservations about the sweeping way that those provisions were drafted, and I think Senator Coats has also indicated that we as a conference committee made a serious mistake in using the indecency standard. The only actual vote that we took at the conference committee on Telecommunications Act was on that very issue, and I think it passed by a narrow vote, weighing the indecency standard versus the "harmful to minors" standard, and I think all of us on the conference committee will have to admit that that was a serious mistake, and many of us predicted that the Court would swiftly strike it down.

Working with Senator Coats and Mr. Greenwood in drafting COPA, we were wary of repeating the mistakes made in the CDA. I do not have the concerns that I had then that we might infringe on protected speech. It took the Congress a couple of tries to get

the dial-a-porn statute right. Ultimately we did, and the problem with a child accessing dial-a-porn largely disappeared without any chilling effect on adult speech.

This is a similar approach to a far more serious problem. Children cannot learn, nor can e-commerce flourish, in a red light district. When children who type the words "cheerleader" or "dollhouse" on their search engines are regularly confronted with pornographic images, we are failing in our responsibility as legislators to protect them from things that they should not see. Parents will not hook up home computers to the Internet in the numbers they otherwise would. Children will learn less online than they ought to, as Senator Coats said, and what some of them do learn may come back to haunt us all.

That is the Chair's opening statement, and I turn to the ranking member, Mr. Markey.

[The prepared statement of Hon. Michael G. Oxley follows:]

PREPARED STATEMENT OF HON. MICHAEL G. OXLEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

This hearing will come to order.

The Subcommittee meets today to consider legislative proposals to protect children from inappropriate material on the Internet. It is a serious and growing problem, and a number of measures have been referred to the Committee for its consideration.

I want to commend Chairman Tauzin, who is a bit under the weather, and Chairman Bliley for calling today's hearing. This is an issue of great concern to a number of Members of the Committee, and we appreciate the leadership of the chairmen.

I thank our witnesses for taking the time to address the issues that confront us, especially the FBI and our Member panel—and in particular Senator Coats, who made the long trek to this side of the Hill. Dan has a record of leadership on this issue, and is the author of one of the strongest proposals to protect young people from harmful material.

Congressman Greenwood, who joins the Subcommittee today, and I have introduced a companion bill, the Child Online Protection Act, or COPA, requiring commercial, adult Web sites to take steps to screen out minors. It is sponsored by 53 Members of the House, including 20 Members of the Commerce Committee. It is endorsed by a coalition of 17 pro-family and religious organizations.

Mr. Chairman, freedom of speech is perhaps our most fundamental liberty. Yet I seriously doubt that the Founding Fathers meant to protect the "right" of commercial pornographers to subject children to hardcore images. My colleagues, that is exactly what is happening in America today, in homes and classrooms and libraries across this country.

A recent national poll found that the number one concern on the minds of voters is the moral decline of our society. If we as a nation hope to address the coarsening of our culture and the loss of values among our young people, we have to begin by addressing the most serious threat, and do so by protecting kids from the degrading content readily available on the Internet.

I'm sure everyone here is aware of last-year's highly publicized molestation and murder of seven-year-old Sherrice Iverson in a Las Vegas casino bathroom by the now 19-year-old who recently pled guilty to her murder. But few people are aware that the killer's own attorney testified that he had been a normal teenager and an honor student until Internet pornography took over his life. Police found vast files of hardcore material, including graphic child pornography, on the boy's home computer, all downloaded from the Internet.

Some opponents of the Coats-Oxley-Greenwood bill will say that all we need to do is promote screening software. I support screening software, too, but it isn't nearly enough. It's my belief that the commercial providers of this smut ought to bear some responsibility for shielding it from the eyes of children.

Other opponents will say that voluntary industry measures are the answer, but I frankly doubt the sincerity of Internet pornographers to do anything effective about the problem or voluntarily abide by any standards that might be set. We hear a lot of talk about self-regulation whenever it looks like the Congress might act on

legislation, and then it quietly fades away when the threat subsides. Meanwhile, the problem only grows worse.

It is quite true, as will be pointed out many times today, that the Supreme Court struck down most of the provisions of the Communications Decency Act. As Members who were fellow conferees on the Telecom Act will recall, I had serious reservations about the sweeping way in which those provisions were drafted, and I think that Senator Coats will agree that Senator Exon—while he assumed a tremendous political leadership role in pushing the CDA—in retrospect, should have drafted much more carefully.

Working with Senator Coats and Mr. Greenwood in drafting COPA, we were wary of repeating the mistakes made in the CDA. I do not have the concerns that I had then that we might infringe on protected speech. As Members who have been around for a while will recall, it took the Congress a couple of tries to get the dial-a-porn statute right. But ultimately, we did, and the problem of children accessing dial-a-porn largely disappeared—without any chilling effect on adult speech. This is a similar approach to a far more serious problem.

Children can not learn, nor can e-commerce flourish, in a red light district. When children who type the words "cheerleader" or "doll house" on their search engines are regularly confronted with pornographic images, we are failing in our responsibility as legislators to protect them from things they should never see. Parents will *not* hook up home computers to the Internet in the numbers they otherwise would. Children will learn less online than they ought to, and what some of them do learn may well come back to haunt us all.

I now recognize the Ranking Member of the Subcommittee, the gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman. And I want to thank you and Chairman Tauzin for calling this hearing this morning.

I have often said that the wondrous wire that brings the Internet into homes and schools and businesses will have a certain Dickensian quality to it: It will be the best of wires and the worst of wires simultaneously. Even as we attempt to give kids the skill set and the tools of the information age to compete for jobs in a knowledge-based economy, there will also be available in cyberspace content that is without question indecent and inappropriate for children. We have to grapple with both aspects of this new mass medium, and with the duality that cyberspace presents us with.

The Telecommunications Act in 1996 contained a provision designed to make America's schools and libraries eligible for universal service funding so that these additional educational entities could receive discounted rates for telecommunications services. Now that the e-rate program is being implemented and the Internet is becoming available to kids across the country in school, some concerns have been raised about access to material on the World Wide Web. It is unsuitable for kids.

I have long believed that technology can often offer a solution to some of the problems that technology itself creates. Software filtering technology and blocking technology can help to provide some protection in schools to shield children from inappropriate online fare. In addition, I believe that other solutions may also help to mitigate against minors gaining access to Web sites that parents and educators feel are indecent and want to shield from young children. It is vitally important that local schools and libraries work in concert with parents and teachers and local officials to determine how they want to deal with these issues.

I have introduced legislation to require that any school or library that receives e-rate funding must establish a policy with respect to material that is inappropriate for children. I believe that the digital age will present both promise and problems. I also believe that we can embrace technological change, use it to empower our citizens,

and also face the challenges that technology poses for us. Again, we have to deal with the duality of cyberspace. This is true not only for Internet content that is inappropriate for kids, but also true for dealing with issues such as law enforcement and encryption technology, as well as with global electronic commerce and personal privacy protections.

In the final analysis it is important that before we embark on regulating aspects of the Internet, that this committee develop policies that recognize the unique characteristics of the new online medium that are consistent with constitutional protections and that effectively achieve our policy goals in the least intrusive manner.

It is, of course, with great irony that we hold this hearing this morning. We are discussing how we should deal with Internet content that is inappropriate for kids on the very same day that the House is voting to put Ken Starr's report on the Internet. This illustrates our problem. We want adult voters to have easy access to this material, some of which is obviously inappropriate for 8-year-olds. How do we strike this balance? And today presents this challenge in its pluperfect form, and I hope today that this discussion can bring us closer to finding a resolution to this dilemma. Thank you.

Mr. OXLEY. The gentleman from California, Mr. Cox.

Mr. COX. I thank the chairman and join with the ranking member for congratulating you and Mr. Tauzin for bringing this matter to our attention. It is a problem, a problem that needs a solution.

I have now three kids, although one is only a few days old and nowhere near Internet-ready, but the other two are surprisingly computer-literate, and I have a very personal stake in making sure that when my children are using the computer and when they are surfing the Net, that they do not run into this by accident. I can assure you that whatever the government standard is that they can look at, my standard is a little different. No matter how sturdy the legislation is that we might pass, my standard will be a little higher for my kids. Therein lies both a problem and an opportunity.

I want to make sure that as we attempt to solve this problem, we apply not a liberal test or a conservative test, but an empirical test, and we ask whether what we are doing is actually going to work. What are we going to do about the global aspect of the World Wide Web? What is the means of applying extraterritoriality in this legislation? Once we wipe out all of the U.S.-based smut providers, what happens to those who are sending it into our homes from somewhere else? Is what we are doing really going to work; and if not, then we better beef it up and find a way that works better.

Second, are we going to rely on the government to chase after the people who are putting out things that we don't want our kids to read, because if we are, we are going to fail. The government simply can't get after the content producers fast enough in order to make a system safe enough for me to expose my kids to it. Relying on the FCC to supervise content is just as bad as relying on the FCC to supervise technology. And to the extent that we have a technological basis in here in the form of prescriptions from the FCC as to what will and will not protect people from liability, we are far from being technologically neutral, dictating the future evo-

lution of the Internet or slowing it down because government is going to be in charge of what the Internet looks like.

I couldn't agree more with the comment that Mr. Markey made that technology is, in fact, a solution. If it poses the problem, it is also the solution. And I would like to know as we commence these hearings from our witnesses whether or not they think that the approach of, for example, H.R. 3783 might be applied to force Internet smut providers to zone themselves into a ".xxx" domain and whether we can apply the kinds of penalties in this bill to people who refuse to do that.

If an approach like that works, and I have no idea whether it will, then filtering technology becomes more effective because some of the things that Senator Coats drew our attention to, for example typing in something about your doll collection and getting back something else, can be much more easily avoided if the entire domain were off limits to the search engine. But that kind of thing is now open to us. It is a possibility, and I think we made significant progress in addressing the legal side of this, what the legal standard is.

And I know that we are going to hear from Professor Lessig, and having read your testimony in advance, Professor, it seems that you are giving a stamp of approval as to the effort made on the legal standard side, although I know other witnesses disagree with that. This is a marvelous opportunity for us to approach this problem with an open mind and come up with some solutions I hope that will really work. That in the end will be my test.

I don't want to see the FCC put in charge of content or technology. I don't want to see us try to regulate billions of providers. Rather, I would rather see us empower people at the threshold of their own computers to keep this stuff away from their kids and out of their households, out of their libraries, and out of their schools and lives. Thank you.

Mr. OXLEY. The gentleman's time has expired.

The Chair now recognizes the gentleman from Ohio, Mr. Sawyer.

Mr. SAWYER. Thank you, Mr. Chairman. Let me begin by expressing my gratitude to you and the ranking member for holding this legislative hearing on how to protect children from inappropriate material over the Internet.

Any tool that is powerful enough to do good is also powerful enough to do harm, and we have seen the results of that. One of the attractions of the Internet is its virtual anonymity. That same anonymity which is serving to protect dissidents in China and Indonesia is also serving to protect some of the lowest forms of humanity around the world.

Fortunately we are making inroads to bringing some of those people to justice. More than a week ago Federal authorities in conjunction with authorities in several foreign countries were able to undertake an international operation to raid a child pornography ring that was being conducted over the Internet.

Because the Internet respects no political boundaries and is mostly unregulated, serious thought has to go into the decisions about how to protect children from abuse or from obtaining inappropriate or dangerous material.

All of us are concerned about education. Technology plays an incredibly important, magnified role in the learning process. It has had a dramatic effect on the way students learn and communicate, and we continue to search for answers on how best to address this issue, and we have to keep a couple of basic things in mind. How do we keep inappropriate material away from children without denying them access to educational information or trampling on the constitutional rights of adults? What guarantees are there that the technology currently being developed will prevent children from viewing inappropriate material? As Mr. Cox mentioned, will it work? Who do we hold responsible if a child visits a site or if the preventions don't work?

Protecting children is a serious business, and it should not be taken lightly. And if we act on any of the proposals before us, we must do so with care and responsibility.

Let me compliment the gentleman from California on his observations. I am particularly interested in this notion of territoriality. The problem, it seems to me, is that the question is essentially nonterritorial. It exists wholly in a separate dimension and may well require us to think in a separate dimension as well if we are to undertake the worthy goals that we have set for ourselves. Thank you.

Mr. OXLEY. I thank the gentleman.

The gentleman from Illinois, Mr. Shimkus.

Mr. SHIMKUS. Mr. Chairman, I have no opening statement.

Mr. OXLEY. The gentleman from Maryland, Mr. Wynn.

Mr. WYNN. Thank you, Mr. Chairman. I don't have a formal opening statement, but I do want to compliment you and the committee Chair for putting this hearing together.

I would make the observation in a few hours we are about to put on the Internet material which a lot of people would consider inappropriate for children. I think it is an unfortunate irony, but it illustrates the seriousness of the problem, that it may not be in the technology, it may be in the definition of what is inappropriate, which is another part of the issue that we have to explore.

I am fascinated at the prospect of the technological solutions, and would certainly encourage their utilization, but I think as we move further along, the real problem is who determines what is inappropriate for young people, and that may be beyond the scope of this meeting. But I think this is a good hearing, and I look forward to hearing the witnesses' testimony.

Mr. OXLEY. The other gentleman from Illinois, Mr. Hastert.

Mr. HASTERT. Thank you.

I think there are three different areas that we need to look at. Sometimes the whole Internet issue still mystifies me in some ways, but I think from a common-sense perspective, as a father and person who has dealt with public schools for a long time, we would not allow a pornographic magazine to be purchased by the taxpayers, to be put into a school library. We wouldn't allow pornographic tapes to be put in school or public libraries where people have the ability to decide how to regulate and how to on a local basis do that.

I don't think then we should be hesitant to try to find ways for people to control the responsibilities that they have as school board

50-939 98 - 2

members, library board members, to be able to control that information that comes into their realms.

For that reason, I think this whole idea of pornographic material on the Internet ought to be set aside. If it is pornographic material, it ought to be in its own category of pornographic material and set aside as a special situation. That could be done by law.

Also, when people decide what comes into their own homes, that is a private issue. But if people want the technology to be able to sort that out or know or monitor what their children are looking at, they ought to have the ability to do that. The free enterprise system is doing that. We have testimony today from people who are very adept at being able to put together the software and sort out what your kids are looking at. As a matter of fact, they will probably be on the edge of saying who is sending things into your home if you need to know that, and you can have a record, and that can be turned over to the authorities if it is offensive.

We also need to be able to stop people from soliciting our children on the Internet system, and that is another realm, and that is not material necessarily, but it is a whole realm of chatrooms and that type of thing, and we also have to have the technology to encourage the free enterprise system to develop that type of material. We can do it. We need to unfetter those things that are stopping our technology in that direction. We also need to call pornographic material pornographic material, put it in its own special case and label it that and contain it in that area. I think that is the beginning.

So I salute the gentleman from Ohio and his colleague from Louisiana who brought this hearing today, and the ranking member. I think there are some common-sense solutions to it, and we ought to get at it. Thank you.

Mr. OXLEY. The gentleman's time has expired.

The gentlelady from New Mexico.

Mrs. WILSON. The protection of children is something that I have spent much of my adult life working on, and there is no question in my mind that the government has a compelling interest in protecting children from explicit material, whether that be in printed form or on the Internet. The problem with the Internet, of course, is that it is so accessible, which is also its greatest strength for educational material and other kinds of valuable information.

Like many of you also, I am a parent and when my second son turned 3, we got a computer for the home and plugged it in, and within an hour he was telling his dad, "Here, let me show you." Fortunately that was almost preschool, it was not a pornographic site.

The ability of young children to use computers is both a great gift, but also places on industry and parents a tremendous responsibility.

It seems to me that there are two approaches that I am interested in hearing about from those who are testifying today. One has to do with the suppliers, and the other has to do with tools for parents and schools. From the suppliers I find this idea of zoning to be interesting, the idea that they have an affirmative responsibility to protect children as members of businesses even though they are businesses that I would not frequent.

With respect to tools for parent and schools making readily available the technology, imperfect as it may be, to screen the materials that may be inappropriate for children and the further development of that technology I find particularly interesting, and I will be interested in hearing what those testifying today have to share with us.

Mr. OXLEY. The gentlelady's time has expired.

The gentleman from Washington, Mr. White.

Mr. WHITE. Mr. Chairman, I want to tell you, as you may recall, I had my children here for the last 10 days before the break, and when I got back a few days ago, I was surprised to find an image of a wolf, a very cute wolf, that was now installed as the screen saver on my laptop computer. And after checking, it was my 9-year-old daughter, who likes wolves very much, was responsible for that particular image. She found a picture of a wolf on the Internet, and now it is my screen saver, and I cannot figure out how to get it off.

I don't know when you type "wolf" into the search engine on the Internet, but I do know what you are going to get when you type the word "teen," and I can tell you it is absolutely appalling. It is appalling when you just look at the descriptions, not even clicking on the description, but just finding the descriptions of the material you get there.

So I think we have a problem in this area. I think it is a problem that is worse than it was 2 years ago when we adopted the Communications Decency Act, and I am committed to trying to find a solution.

Mr. Chairman, I am also committed to finding a solution that really works in the real world. I don't want a public relations advantage, and most of all I don't want to say that I have done something when what I have done is not going to have an effect on the problem, and that is what I am struggling with today.

There may be a role for a law like the one that we are considering today. Maybe now is the time to consider it. But the fact is that a law cannot solve this problem, at least a law in the United States cannot solve this problem, to the degree I would like to see it solved. Our laws don't apply in Amsterdam or Thailand or a lot of places where some of this stuff can come from.

Frankly, a law in some cases could even make it worse, because a law could lull people into a false sense of security that the government has solved this problem, and I can promise you that just like when you take your child for a walk in Times Square, no matter how much the government is trying to protect you, the government cannot protect your kids from everything on the Internet, and it would be a shame if we took a step that lulled people into that false sense of security.

So I am struggling with a decision on how we can do that. My own view is if we can harness some of the creativity and technological expertise and momentum and everything else that we see in the Internet community, we might be able to come up with a better solution. That is the reason Senator Lieberman and I in July of this year sent a letter to the Internet community asking them to really make one last 100 percent effort to come up with a program to really solve this problem where it was one click away and

could be taken care of very quickly. I think there is commendable effort under way right now in the Internet community to try to come up with some solution to the problem.

Frankly, I don't know that that effort will succeed. We have had efforts in the past that have been undertaken. We have had a very highly publicized meeting at the White House about a year ago, and I would say very little resulted from all of the wonderful talk and discussion that we had at the time, so I am disappointed in the result that we had there.

I do think that if we are going to find a solution that really works, it will probably combine some legal activity or legal changes made by our committee and Congress and some things happening in the real world that will actually have more of an effect.

As of today, I still have an open mind on whether it is time now to adopt this law or whether we shouldn't wait for some more period of time working with the Internet community that will actually do a better job of solving this problem. So this hearing is one step that will help us find the answer to that question. I will be paying very close attention to the witnesses to try to get an indication of which way we should go.

Thank you, Mr. Chairman, and I appreciate your having this hearing.

[Additional statement submitted for the record follows:]

PREPARED STATEMENT OF HON. TOM BLILEY, CHAIRMAN, COMMITTEE ON COMMERCE

Thank you Mr. Chairman.

This Congress, the Commerce Committee has engaged in the extensive review of electronic commerce issues. We have moved legislation on encryption, Internet tax, WIPO implementation, and securities litigation reform. We have also held numerous hearings on other matters such as consumer protection, privacy, and electronic payment systems. The Committee seeks to ensure that Congress fulfill its role in shaping an electronic marketplace and that Congress acts only when absolutely necessary. I would like to thank Chairman Tauzin and other Subcommittee Chairmen for their leadership on this important electronic commerce agenda.

As the Committee has learned during the course of the 105th Congress, the Internet, and consequently, electronic commerce, will only continue to develop if it is safe, secure, and private. Consumers are less likely to engage in commerce on-line, or purchase access to the Internet for that matter, if they believe that their credit card numbers can be easily stolen, or if their children will be easily exposed to pornography on the Web or predators in chat rooms. The purpose of this hearing is to explore ways to increase the "safety" of the Internet for children.

One cannot freely use the Net today without being exposed to Web sites that contain material that is inappropriate for children. Current data shows that there are at least 28,000 adult Web sites promoting pornography on the Internet. Folks not seeking pornography stumble upon it by mistake. For example, the search term "teen" yields over 140,000 "hits" most of which are pornographic.

The Commerce Committee understands that the Internet stimulates a marketplace of ideas through Web pages, newsgroups, listservs, chat rooms, e-mail, and bulletin board services. These tools empower Americans to speak on more topics, to more individuals, and over greater distance, than we have seen from traditional mediums of communications in the past. I believe this innovation is good for consumer. As the lower court stated in the *Reno* decision, "the content on the Internet is as diverse as human thought."

The fact remains: Our children must be protected from inappropriate material. While the availability of pornography in the United States is already troubling, children getting access to it is much worse. Legislative solutions must be seriously considered, but if legislation is to survive, it must be narrowly tailored so that it doesn't squash the First Amendment rights of adults. I look forward to hearing from the panelists today on their efforts to protect kids. Regardless of what actions Congress may take, parents, educators, and industry must take some responsibility to ensure that our kids are not getting access to this harmful material.

Thank you Mr. Chairman for holding this hearing today and I yield back the balance of my time.

Mr. OXLEY. The aforementioned gentlemen, one from New York and one from Oklahoma, are welcome to join us.

Let me welcome our good friend from Pennsylvania, who is not on our subcommittee, but is a co-sponsor of the COPA legislation, and he is mute because the rules don't allow him to give an opening statement, which is rare for the gentleman from Pennsylvania, but he will participate in the question-and-answer period.

Let me now turn to the gentleman from Oklahoma, Mr. Istook, and the gentleman from New Jersey, Mr. Franks. Why don't we begin with the more senior member, Mr. Franks.

STATEMENT OF HON. BOB FRANKS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. FRANKS. Mr. Chairman, it is a delightful opportunity to be here, and particularly to have Congressman Greenwood here, particularly under the restrictions under which he is operating.

Mr. Chairman, I would like to commend you for holding this hearing to learn more about the dangers our children face in cyberspace. The Internet has opened up an exciting world of discovery for our kids. With a few clicks of the mouse, our children can find up-to-date information on every conceivable topic that they are studying in school. This Congress has gone on record as indicating that every child in America should have an opportunity to use this amazing learning tool. To help reach that goal, the Telecommunications Act of 1996 provided $2.25 million in special communications discounts. These discounts are available to help schools and libraries across America hook up to the Internet.

As co-chairman of the Congressional Caucus on Missing and Exploited Children, I have learned that when it comes to our children, we need to approach the Internet with some caution. Exploring cyberspace can innocently leave children exposed to materials that even most adults would find highly objectionable. We need to take extra precautions to protect our children, especially when they are using the Net as a learning tool in the classroom or at the public library. That is why I have introduced the Safe Schools Internet Act. It would require schools and libraries to use blocking technology if they accept Federal subsidies to connect to the Internet. This technology, which many parents have already installed on their home computers, would keep materials designed for adults only out of the reach of our children.

Let me note that the concept of placing restrictions on the kind of information available to our children in public institutions is not new. Schools and libraries routinely decide what books and other materials are appropriate for our children to read. The Safe Schools Internet Act would merely require that these same institutions exercise the same standard of care when it comes to the latest advances of the information age.

While the bill requires schools and libraries to use blocking technology, it leaves it up to the local school district and local library board to determine the type of filtering technology to use. It is important that parents and educators in our local communities set their own standards.

This bill is a step we can take to ensure that the Internet remains an exciting world of discovery and a safe avenue of learning for our children.

I urge the subcommittee to take action and report a bill to the House floor that would protect our children from the harmful material on the Internet while they are using computers in our public schools and in our public libraries.

Additionally, I would recommend that the subcommittee consider combining the goals of filtering in schools and libraries with Congressmen Oxley and Greenwood's goal to prevent commercial pornography operations from displaying their merchandise on Web sites without a mechanism to restrict the access of children.

I am a cosponsor of my colleagues' bill, and would appreciate the subcommittee's consideration of that request. Thank you.

[The prepared statement of Hon. Bob Franks follows:]

PREPARED STATEMENT OF HON. BOB FRANKS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. Chairman, I would like to commend you for holding this hearing to learn more about the dangers our children face in cyberspace.

The Internet has opened up an exciting world of discovery for our children. With a few clicks of the mouse, our children can find up-to-date information on every conceivable topic they are studying in school. Every child in America should have an opportunity to use this amazing learning tool.

To help reach that goal, the Telecommunications Act of 1996 provided $2.25 billion in special telecommunications discounts. These discounts are available to help schools and libraries across America hook up to the Internet.

As Co-Chairman of the Congressional Caucus on Missing and Exploited Children, I have learned that when it comes to our children, we must approach the Internet with caution. Exploring cyberspace can innocently leave children exposed to materials that even many adults would find objectionable. We need to take extra precautions to protect our children—especially when they are using the Net as a learning tool in the classroom or at the library.

That is why I introduced the Safe Schools Internet Act. It would require schools and libraries to use blocking technology if they accept federal subsidies to connect to the Internet. This technology—which many parents have already installed on their home computers—would keep adult-only materials out of the reach of our children.

The concept of placing restrictions on the kind of information available to our children is not new. Schools and libraries routinely decide what books and other materials are appropriate for children to read. *The Safe Schools Internet Act*—would merely require that these institutions exercise the same standard of care when it comes to the latest advances of the Information Age.

While the bill requires schools and libraries to use blocking technology, it leaves it up to the local school district and library to determine the type of filtering technology to use. It's important that parents and educators in our communities set their own standards.

This bill is another step we can take to ensure that the Internet remains an exciting world of discovery and a safe avenue of learning for our children.

I urge the Subcommittee to take action and report a bill to the House floor that would protect our children from harmful material on the Internet while in school or at the library.

Mr. OXLEY. Thank you.

Mr. Istook.

STATEMENT OF HON. ERNEST J. ISTOOK, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OKLAHOMA

Mr. ISTOOK. Thank you, Mr. Chairman. I appreciate the chance to be here. I wanted to explain my perspective as not only a father of five children, also as a former library system chairman. I was chairman of the metropolitan library system, which operates the

public libraries not only in Oklahoma City, but throughout central Oklahoma.

I would like to commend the many Members of Congress who have been working for years to combat pornography on the Internet, and in particular to protect children from it. These efforts have taken several approaches, including requirements imposed on those who operate commercial Web sites, linking e-rate funding and requirements for filtering software on the computers that are purchased with Federal funding. The rider that does that has been attached with my efforts to the Labor-HHS appropriations bill, and it is complementing the efforts that so many other people have under way.

The issue is important to parents and families. Like most of you, constituents have come to see me to ask about protecting our children from Internet porn, including access through public schools and libraries. The Internet is a marvelous tool. It can open windows on the world. I have used it with my children to assist them with their homework. Unfortunately, it is not like buying books and other printed material. You cannot choose what is appropriate to purchase and what is not. It all comes in one huge package, the good, the bad and the ugly. Our goal is to protect our children against the ugly.

The Federal Government is investing over $750 million each year in various programs that purchase computer hardware and software so the children can access the Internet. These programs include Title I, special education, Goals 2000, education technology programs, vocational education and many others. Over the years, these purchases with Federal funds have totaled billions of dollars. From 1996 to 1997, U.S. elementary and secondary schools spent $4.2 billion in combined Federal, State and local funds on computer hardware, software and other materials for Internet access. So because of this investment, and others each day millions of children across the country are able to access the Internet in schools and libraries. As of January of this year, there were nearly 30 million host Web sites.

As is the case with so many modern opportunities, it can be a blessing or a curse. Among these, there are over 100,000 Internet Web sites which feature pornography and obscenity of all types, from child nudity to graphic sex sites, and that figure, frankly, may be low. Even if you are not looking for it, it seeks you out, including ads and teasers on Web sites. Each day an estimated 200 new porn sites are created. The porn industry is huge. It is estimated to gross $8 billion a year compared with $6.6 billion for movie admissions and $6.7 billion spent on spectator sports. Online sex sites made an estimated $925 million in 1996.

But even though some of these sites charge for access, usually via credit cards, typically they will offer extensive free previews. There is plenty of graphic images offered without charge, and then they promise more, either more in quantity or simply more explicit for a few dollars more, and there are huge numbers of sites which offer access at no charge. They are extensively linked and cross-promoted. Accessing just one opens up a visual or multimedia barrage of enticement to go to others. Many of them have disclaimers warning about nudity or explicit images, and perhaps a statement

that somebody under 18 should not proceed any further. But usually those are about as effective as building a retaining wall out of tissue paper. They don't know if the user is 66, 16 or 6, and they provide no real protection for our youth. Our youth are vulnerable.

According to the U.S. Commission on Pornography, 12- to 17-year-old adolescents have become one of the largest consumers of porn in the country. So thus our schools and libraries, as they move to universal Internet access, which still is not present in all homes, are at particular risk that our schools and libraries can then be used as the entry points for this traffic in porn. Students are confronted not only with temptation, but with this aggressive marketing effort by purveyors of sex and pornography.

A recent example, staff received an unsolicited e-mail recently inviting the staff to go online to look at Russian babes on a site out of the Netherlands. There are some people, of course, that say just stay away from those sites, but they don't understand this marketing approach that is being used.

I recall one time using a search engine, looking up my own name to see what might be on the Internet about me. One of the sites to which it took me was a pornographic site. I found out they had constructed a link. If you search for any Member of Congress, you will hit on that particular site.

They do it every way that they can. You bring up "toys," and you may get an "adult toys" online. You bring a reference to male or female or anything else that is innocent or innocuous, and you don't know the links to which it can take you.

In my office a female staff member tried to download the text of a Presidential speech. Instead of typing in whitehouse.gov, she typed in whitehouse.com and got to a site that was a sexual parody of the White House. They deliberately had created a URL address mimicking the legitimate White House address just as a further way to get more people to access their Web sites.

These are simple examples but on the Internet they are multiplied extremely. There is no limit to the creativity of those who are seeking to sell sexual enticement and excitement via the Internet and they are indiscriminate in their market. Of course children and adolescents, being especially curious, are especially vulnerable. My point is that even if they don't go looking for obscenity on the Internet and, yes, some of them do go looking, but even if they don't go looking for it, it comes looking for them. Computers are machines. They will never stop the ceaseless temptation.

So it is up to us who are providing billions of dollars for Internet access to public schools and public libraries to do all that we can to minimize the temptation, to minimize the use of these as gateways to obscenity and gateways to disaster for our children. That is why Congress needs to act now through the legislation such as you have discussed and such as the rider which is currently on the Labor-HHS appropriations bill. Following the Federal funding link as a member of the Committee on Appropriations who pursued a simple rider, if you receive Federal funds to purchase a computer system for a school or library that provides Internet access, you are to install filtering software to diminish the ability to use those to access porn. As the Congressional Research Service has stated in looking over this legislation, because obscenity and child pornog-

raphy are not protected by the First Amendment, they may be banned and Congress of course has done so in respect to both of them in recent years.

We also of course avoid legal difficulties such as you were describing, Mr. Chairman, by putting this particular focus not on overall Internet access but only on those when they are used by minors, and of course that is in addition to the Federal funding link. The amendment was placed on the Labor-HHS appropriations bill unanimously in subcommittee so it certainly has full bipartisan support which, as Mr. Markey noted, is certainly essential in something such as this. Placing electronic filters on computer blocking software is the simplest and least expensive solution. In fact, it has already been adopted by a great many schools and libraries, including most of those within my own congressional district. I want to commend the schools and libraries which are already pursuing this remedy. As we are spending billions of dollars of Federal funds on this equipment, we have a duty to assure that we make sure that the effort that is undertaken is universal on this.

There is a different effort, of course, to try to control the sending of obscenity over the Internet by looking at the sending end of it. This of course is an approach that focuses on the receiving end of it. It does not block the person that may be sending out pornography, but it does block the ability to receive it and limits it on the computer that may be in a school or may be in a home. We have also avoided dictating what should be the software selected by the local government. We leave that decision up to the States and to the communities. Obviously there are a number of different vendors who have the software available and they can choose for themselves which is the most up to date and which they think will best suit their needs. I think you will have testimony from some of those vendors and, as they will certainly explain to you, this software has been updated a lot since it first came out. Some of the problems that were originally associated with it have been addressed. I think the most commonly mentioned one is when you say you want to research Middlesex, England and it filtered out Middlesex. It got more sophisticated than that and they no longer filter out that particular geographical location. But it is part of the technological approach. It is linked to the Federal funding. It is linked to the schools and the libraries that are used by juveniles as potential access points, and we make sure of course that we have within the legislation the ability with adult supervision to disable the software if for some reason it does get in the way of legitimate research on a particular search and then of course it is re-enabled after that particular search effort is ended.

Mr. Chairman, I am very grateful for your effort and this committee's effort to address this problem. Obviously we have multiple different approaches under way. I think that is very healthy because the problem is so insidious and so widespread that I think it is going to take these multiple approaches to be able to corner it and get a handle on it.

[The prepared statement of Hon. Ernest J. Istook, Jr. follows:]

PREPARED STATEMENT OF HON. ERNEST J. ISTOOK, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OKLAHOMA

INTRODUCTION

I would like to commend the many Members of Congress who have been working for years to combat pornography on the Internet, and in particular to protect children from it. These efforts have taken several approaches, including requirements imposed on those who operate commercial web sites, and linking E-rate funding to requirements for filtering software on the computers purchased with that funding. The rider that has been attached to the Labor-HHS appropriations bill is complementary with those approaches.

This issue is important to families and parents all across America. And like most of you, constituents have come to my office to ask about protecting our children from being exposed via the Internet to pornography in public schools and libraries. The Internet is a marvelous tool to open windows on the world; unfortunately, it is not like buying books and other printed material. You cannot choose what is appropriate to purchase and what is not. It all comes in one huge package—the good, the bad and the ugly. Our goal is to protect our children against the ugly.

FEDERALLY-FUNDED INTERNET ACCESS

The Federal government is investing over $750-million per year in various programs purchasing computer hardware and software so that children can access the Internet, with its vast links to knowledge, information and news. These programs include Title I, Special Education, Goals 2000, Education Technology programs, vocational education, and many other such programs. Over the years, these purchases to date have totaled billions of dollars.

From 1996-1997, U.S. elementary and secondary schools spent $4.2 billion in combined federal, state and local funds on computer hardware, software, and other materials necessary to connect them to the Internet. Because of this investment, each day millions of American children can access the Internet in schools and libraries.

PORNOGRAPHY ON THE INTERNET

As of January, 1998, there were nearly 30 million host web sites. As is the case with so many modern opportunities, this access can be a blessing or a curse. The Internet can be a treasure throve of information, learning and ideas, but there are also over 100,000 Internet web sites which feature pornography and obscenity of all types, from child nudity to graphic sex sites. That 100,000 figure, frankly, may be low. Even if you are not looking for it, it seeks you out, including ads and "teasers" on web sites. An estimated 200 new porn sites are being created each day. The porn industry is huge, estimated to gross $8 billion per year (U.S. News & World Report), compared with $6.6 billion for movie admissions, and $6.7 billion spent on spectator sports (U.S. Chamber of Commerce). On-line sex sites made an estimated $925-million in profits in 1996.

But even though some of these sites charge for access, usually via credit card billings, they typically offer extensive free "previews." There are plenty of graphic images offered without charge, which then promise more—either more explicit or simply more in quantity—for a few dollars. Additionally, there are huge numbers of sites which offer no-cost access.

The sites are extensively linked and cross-promoted, so that accessing a single one opens up a visual or even multimedia barrage of enticement. Yes, many of them have disclaimers warning of nudity or explicit images, and a statement that anyone under 18 should not proceed further. But these are about as effective as constructing a retaining wall out of tissue paper. They don't know if the user is age 66, 16 or 6. They provide no protection for our youth.

And our youth are vulnerable. Unfortunately, according to the US Commission on Pornography, 12-to-17-year-old adolescents have become one of the largest consumers of pornography. Thus, our schools and libraries, as they move to the universal Internet access which still is not present in all homes, are at particular risk to be used as entry points for this traffic in pornography.

Students are confronted not only with temptation, but with an aggressive marketing effort by purveyors of sex and pornography. A recent example includes an unsolicited email recently received by our staff that invited them to go on line to look at Russian babes on a site in the Netherlands.

Via the Internet, children are freely able to access material that various state and federal laws prevent them from obtaining at retail outlets. Transporting obscenity

on the Internet already is a Federal crime.[1] But simply declaring something illegal does not end the practice, nor end the temptations. And it still remains a larger problem because we are promoting growth of the Internet—the very medium which is the entry point for this marketing.

MARKETING TO OUR CHILDREN

Those who say that people should simply stay away from these Internet sites don't understand how this works, or perhaps they choose not to care. Whether a curious mind is seeking this material or not, if you use the Internet, it will come looking for you.

You might be using a search engine, and include as innocent a term as "male" or "female" or "toys" within your search term. Not only do a multitude of varied sites pop up as you explore these links, but soon so do colorful, enticing and lurid ads, depicting persons of that sex in provocative poses. "Toys" for example, brought up "Adult Toys Online" as a web site, with references to sex, bondage, etc. It is unpredictable what innocent terms will lead to graphic websites. For example, checking out a mention of my own name suddenly connected me to a sexually-explicit web site. Why? Because its sponsor had set up a link to the names of each and every member of Congress.

In my office, a female staff member was trying to download the text of a Presidential speech, and she typed in "www.whitehouse.com" instead of "www.white house.gov." Her screen suddenly showed a sexually-provocative image, standing with a bullwhip, with little White House website flags waving, and text inviting the user to "interview" the "intern of the week." It was a porn site which deliberately had created a URL address mimicking the legitimate White House website, knowing that it would be accessed by many people, who it hoped to lure in further.

These are simple examples, but they are multiplied endlessly on the Internet. There is no limit to the creativity of those who seek to sell sexual enticement on the Internet, marketing indiscriminately to adult and child alike.

It is impossible for any Internet user to avoid all temptation. And, under a constant barrage of enticements, we know that there will be wide-scale yielding to that temptation. Children and adolescents are especially curious, and therefore vulnerable. My point is that even if they don't go looking for obscenity on the Internet, it comes looking for them. Computers are machines, and they will never stop the ceaseless tempting. It is therefore up to us—we who are providing the money for so much of this Internet access—to do all that we can to minimize this temptation. To remove it all is impossible, but that is no excuse for not doing what we can.

IMMEDIATE ACTION IS NEEDED

Congress must act now, and continue to seek more ways to confront this problem. We already acted once with the Communication Decency Act, only to see the courts overturn that attempt to protect children. We need a further and immediate effort.

Fortunately, the courts recognize a key difference between our ability to control the content in general, and our ability to control the content of what is purchased with government funds.

Following this federal funding link, and as a member of the Appropriations Committee, I pursued an appropriations rider with a simple, understandable, and clearly constitutional approach. It has produced bipartisan support, because I know my colleagues on the other side of the aisle want to protect our children from obscenity just as I and others in my own party do.

As the Congressional Research Service has stated, "Because obscenity and child pornography are not protected by the First Amendment, they may be banned, even for adults. Congress has done so with respect to both, and in recent years has amended the relevant statutes to include transmission of obscenity and child pornography by computer." (CRS Memorandum issued June 29, 1998) Obscenity, defined by the courts under the *Miller* test, includes material dealing with depiction of sex acts, and with child pornography, and with other material that meets three tests—prurience, patent offensiveness, and lack of artistic value.

We also avoid legal difficulties by focusing on the access provided to children, rather than to adults. However, since we are talking about controls only on computers purchased with federal funds, this same approach should be generally suitable regardless of age groups.

[1] (Punishable by a fine and not more than 5 years in prison for the first offense and a fine and up to 10 years in prison for the second offense, plus a basic fine of up to $250,000. 18 USC 1462).

The amendment we have placed on the Labor-HHS appropriations bill—by unanimous vote in subcommittee—requires a school or library which receives Federal funds for the purchase of computers or computer-related equipment (modems, LANs, etc.), to install an Internet obscenity filter on any computer to which minors have access.

Placing electronic filters on computers—"blocking" software—is the simplest and least expensive solution, and in fact has already been adopted by a great many schools and libraries, including most of those in my own congressional district. I want to commend those schools and libraries which are already pursuing this remedy. But we are spending billions on this equipment, so we have a duty to assure that this remedy is universally applied to all purchases made with this federal money.

I am always very concerned about local control, and wanted to make sure that the states maintain proper control over their own schools and libraries. Therefore, this measure says the states should select the filtering software they wish to use, rather than have it dictated by us. There is no authority for the U.S. Department of Education to dictate this selection, other than for federal programs, such as Department of Defense schools and libraries. This will mean that different states may select different software, so it will not only assure local control, but will also foster competition in the software market.

Because the filters are not yet perfect, and might inadvertently block non-obscene websites, the provision allows users to bypass the blocking software temporarily with the assistance of an adult. For example, it was widely reported that some older filters would block Middlesex England's web site because of the letters "s-e-x" within the word. Newer filters are more sophisticated and solve that particular problem. The variances in the different software available, and the way it is upgraded, is another key reason that the implementing decisions are properly left to the state and local levels.

The filter software is required only for computers to which minors have access, so, for example, it would not restrict a teacher's computer in their personal office, or any computer in a strictly-adult section of a library. If the filtering software is not installed, the school or library involved would have funds withheld for further payments toward computers and computer-related services, until they comply with the law.

CONCLUSION

The time to act is now; everyday the number of lurid web sites is growing. The three approaches being discussed here today—requiring filters when minors use federally-provided computers, attaching filtering requirements to the e-rate, and requiring pornographic sites to properly identify themselves—are all steps which help to protect our children from this onslaught against them.

Whatever else this committee does, the Istook amendment should be allowed to move forward, with its already-demonstrated bipartisan support. We will have made a first step to help parents everywhere protect their children from the pervasive obscenity on the Internet.

Mr. OXLEY. To both of you, thanks for your leadership and your direction on this issue. We appreciate your testimony and we thank you for your participation.

The Chair will now call the next witness, Mr. Stephen R. Wiley, Chief of the Violent Crimes and Major Offenders Section, Federal Bureau of Investigation.

Mr. Wiley, welcome to the Committee on Commerce. We appreciate your willingness to come up here and participate in this discussion about on-line pornography as it relates to children. You may begin.

STATEMENT OF STEPHEN R. WILEY, CHIEF, VIOLENT CRIMES AND MAJOR OFFENDERS SECTION, FEDERAL BUREAU OF INVESTIGATION

Mr. WILEY. Thank you, Mr. Chairman. Good morning, Mr. Chairman and members. I appreciate this opportunity to discuss the serious issue of protecting our children against sexual exploitation fa-

cilitated by the Internet. Our children are our Nation's most valued resource and they are the most vulnerable members of our society. There is no greater outrage in our society than when we hear of a child who has been mistreated, sexually abused or murdered. It is paramount that as a society we protect our Nation's children and keep them from being victims of crime. Advances in computer and telecommunications technology have allowed our children to broaden their horizons, thus increasing their knowledge and cultural experiences. This technology, however, has also allowed our Nation's children to become vulnerable to exploitation and harm by pedophiles and other sexual predators.

Commercial on-line services on the Internet provide the opportunity for pedophiles and other sexual predators to meet and converse with children. Our investigative efforts have shown that pedophiles often use chat rooms to contact children. These chat rooms offer users the advantage of instant communication throughout the United States and abroad. They provide the pedophile with anonymous means of identifying and recruiting children into sexually explicit relationships.

Through the use of chat rooms, children can chat for hours with unknown individuals, often without the knowledge or approval of their parents. A child does not know if he/she is chatting with a 14-year-old or a 40-year-old. To date the FBI has investigated 152 cases involving pedophiles traveling interstate to meet undercover agents or officers posing as juveniles for the purpose of engaging in an illicit sexual relationship. Many more FBI cases involve individuals trafficking in child pornography over the Internet. The advancement and availability of computer telecommunications also demands that all of us, public officials, law enforcement, parents, educators, commerce and industry leaders be more vigilant and responsible by teaching our children how to avoid becoming victims of sexual predators. Parents must talk to their children about the potential dangers they may encounter throughout the Internet and on-line services. Several groups, including the National Center for Missing and Exploited Children, have issued guidelines for parents on safeguarding children who use computers linked to the information highway. Recently, utilizing funds provided by this Congress in support of the FBI's Innocent Images National Initiative, the FBI published a parent guide to Internet safety. This publication was recently posted in the FBI's World Wide Web page at www.fbi.gov. It is also available through contact with any FBI office. I have attached copies of the FBI document as well as the National Center for Missing and Exploited Children's guidelines to this statement. I urge parents to review these guidelines and discuss them with their children. Schools that offer computer classes and access to the Internet should include appropriate discussion of this problem in their curriculum. Creating awareness of the problem is a first step toward reducing a child's vulnerability to sexual predators.

Blocking mechanisms for the Internet access are available for parents to restrict access to sexually oriented Internet and on-line bulletin boards, chat rooms and Web sites. These mechanisms can help reduce but will not totally eliminate the vulnerability of our children. It is possible that children such as teenagers may be able

to circumvent the restrictions of the blocking mechanism or that pedophiles will still be able to meet children through what may at first appear to be innocent noninteractive activities such as responding to a news group or Web site posting. The FBI is attacking this problem of pedophiles establishing sexually elicit relationships with minors through use of the Internet and the proliferation of child pornography on the Internet and on-line services through a comprehensive initiative on crimes against children.

One facet of the FBI's crimes against children program is the innocent images initiative which was initiated based upon information developed during a child abduction investigation. In May 1993, the disappearance of a 10-year-old named George Burdynski, Jr. led two Prince George's County, Maryland police detectives and FBI agents to two subjects who had sexually exploited numerous juvenile males over a 25-year period. Investigation into the activities of these two subjects determined that adults were routinely utilizing computers to transmit images of minors showing frontal nudity and sexually explicit conduct as well as luring minors into illicit sexual activity. It is through this investigation that the FBI recognized that the utilization of computer telecommunications was rapidly becoming one of the most prevalent techniques by which pedophiles and other sexual predators share sexually explicit photographic images of minors and identified and recruited children for sexually explicit relationships. The illicit activities being investigated by the FBI and others are conducted by users of both commercial and private on-line services as well as the Internet. The FBI's national initiative on child pornography focuses on those who indicate a willingness to travel for the purpose of engaging in sexual activity with a child; those who produce and/or distribute child pornography and those who pose illegal images on the on-line services in the Internet.

Through this initiative FBI agents and task force officers go online in an undercover capacity to identify and investigate those individuals who are victimizing children through the Internet and on-line service providers.

Fifty-five FBI field offices and a number of legal attaches offices are assisting in conducting investigations in support of the innocent images initiative. The Innocent Images National Initiative is coordinated through the FBI's Baltimore office. This initiative provides for a coordinated FBI response to a nationwide problem by collating and analyzing information and images obtained from numerous sources to avoid duplication of effort by all field offices. The Baltimore division's investigative operation involves the commitment and dedication of Federal, State and local law enforcement agencies working together in a task force environment. The FBI believes that enforcement agencies should work together in a coordinated effort to address crimes against children, facilitated by the Internet. It is this sharing of manpower and resources that will ultimately provide the most effective tool in combating this egregious crime problem.

Although the Innocent Images Initiative is coordinated through the FBI field office at Baltimore, this operation has expanded to other FBI field offices throughout the United States. To date the following accomplishments have been recorded as a direct result of

the innocent images national initiative: 196 indictments, 75 informations, 207 convictions, 202 arrests. In addition, 456 entry searches have been conducted. The FBI also conducts an outreach program to inform the public and local law enforcement agencies about this national initiative. In the past 2 years, the FBI has addressed a number of civic, judicial, prosecutive and law enforcement organizations concerning this initiative and the assistance the FBI can provide in investigating crimes against children facilitated by the Internet.

This year alone the FBI has conducted 4 Internet child pornography symposiums around the country for State and local law enforcement. The FBI recently assigned a supervisory special agent on a full-time basis to work at the National Center for Missing and Exploited Children. As I mentioned earlier, the FBI has investigated 152 cases involving pedophiles traveling interstate to meet minors for the purpose of engaging in illicit sexual relationships. One example of a traveler case involved a resident of Rockville, Maryland who pled guilty to two counts of interstate travel to engage in sexual activity with a minor. Through investigation this individual was found to have traveled from his Maryland home to the Springfield, Virginia public library for the purpose of meeting a 12-year-old female in order to have sex. After the subject's arrest a review of his Internet e-mail messages revealed that the subject had been posing as a 16-year-old and had communicated with a number of other girls, attempting to meet them for sex.

Crimes against children are among the most emotional and demanding cases that investigators and prosecutors must face. The FBI will continue to work closely with other law enforcement agencies, the National Center for Missing and Exploited Children and the Department of Justice's Child Exploitation Obscenity Section to investigate, arrest and convict those individuals who prey upon our Nation's children.

That concludes my opening statement.

[The prepared statement of Stephen R. Wiley follows:]

PREPARED STATEMENT OF STEPHEN R. WILEY, CHIEF, VIOLENT CRIMES AND MAJOR OFFENDERS SECTION, CRIMINAL INVESTIGATIVE DIVISION, FEDERAL BUREAU OF INVESTIGATION

Good morning, Mr. Chairman and members of the subcommittee. I appreciate this opportunity to discuss the serious issue of protecting our children against sexual exploitation facilitated by the Internet. Our children are our Nation's most valued resource and they are the most vulnerable members of our society. There is no greater outrage in our society then when we hear of a child who has been mistreated, sexually abused, or murdered. It is paramount that, as a society, we protect our nation's children and keep them from becoming victims of crime.

Advances in computer and telecommunications technology have allowed our children to broaden their horizons, thus increasing their knowledge and cultural experiences. This technology, however, has also allowed our Nation's children to become vulnerable to exploitation and harm by pedophiles and other sexual predators.

Commercial on-line services and the Internet provide the opportunity for pedophiles and other sexual predators to meet and converse with children. Our investigative efforts have shown that pedophiles often utilize "chat rooms" to contact children. These "chat rooms" offer users the advantage of instant communication throughout the United States and abroad, and they provide the pedophile an anonymous means of identifying and recruiting children into sexually illicit relationships. Through the use of "chat rooms", children can "chat" for hours with unknown individuals, often without the knowledge or approval of their parents. A child does not know if he/she is "chatting" with a 14 year old or a 40 year old. To date, the FBI has investigated 152 cases involving pedophiles traveling interstate to meet under-

cover agents or officers posing as juveniles for the purpose of engaging in an illicit sexual relationship. Many more FBI cases involve individuals trafficking in child pornography over the Internet.

The advancement and availability of computer telecommunications also demands that all of us, public officials, law enforcement, parents, educators, commerce and industry leaders, be more vigilant and responsible by teaching our children how to avoid becoming victims of sexual predators. Parents must talk to their children about the potential dangers they may encounter through the Internet and on-line services. Several groups, to include the National Center for Missing and Exploited Children (NCMEC), have issued guidelines for parents on safeguarding children who use computers linked to the information highway. Recently, utilizing funds provided by this Congress in support of the FBI's "innocent images" national initiative, the FBI published "A Parents Guide to Internet Safety". This publication was recently posted on the FBI's world wide web page at www.fbi.gov. It is also available through contact with any FBI office. I have attached copies of the FBI and NCMEC guidelines to this statement. I urge parents to review these guidelines and discuss them with their children. Schools that offer computer classes and access to the Internet should include appropriate discussion of this problem in their curriculum. Creating awareness of the problem is a first step toward reducing a child's vulnerability to sexual predators.

Blocking mechanisms for Internet access are available for parents to restrict access to sexually-oriented Internet and on-line bulletin boards, chat rooms and web sites. These mechanisms can help reduce, but will not totally eliminate, the vulnerability of children. It is possible that children, such as teenagers, may be able to circumvent the restrictions of the blocking mechanism or that pedophiles will still be able to meet children through what may at first appear to be innocent non-interactive activity, such as responding to a news group or web site posting.

The FBI and other law enforcement agencies must continue to develop innovative investigative strategies for dealing with crimes committed in cyberspace and build strong legal precedent to support these investigations and prosecutions.

The FBI is attacking the problem of pedophiles establishing sexually illicit relationships with minors through use of the Internet, and the proliferation of child pornography on the Internet and on-line services through a comprehensive initiative focusing on crimes against children. This initiative encompasses several major crime problems, including: the sexual exploitation of children; child abductions; child abuse on government and Indian reservations; and parental/family non-custodial kidnapings. In May 1997, each of the FBI's 56 field offices designated two special agents as crimes against children coordinators. These coordinators have been tasked with developing multi-agency teams of law enforcement, prosecutive and social service professionals capable of effectively investigating and prosecuting child victim crimes that cross legal and geographical jurisdictional boundaries and which enhance the interagency sharing of intelligence and information. The FBI has and will continue to aggressively address all crimes against children facilitated by the Internet.

One facet of the FBI's crimes against children program is the "innocent images" initiative which was initiated based upon information developed during a child abduction investigation.

In may 1993, the disappearance of ten year old George Stanley Burdynski, Jr., led Prince George's County, Maryland police detectives and FBI agents to two suspects who had sexually exploited numerous juvenile males over a 25 year period. Investigation into the activities of these two suspects determined that adults were routinely utilizing computers to transmit images of minors showing frontal nudity or sexually explicit conduct, as well as to luring minors into illicit sexual activity. It was through this investigation that the FBI recognized that the utilization of computer telecommunications was rapidly becoming one of the most prevalent techniques by which pedophiles and other sexual predators shared sexually explicit photographic images of minors, and identified and recruited children for sexually illicit relationships. The illicit activities being investigated by the FBI are conducted by users of both commercial and private online services, as well as the Internet.

The FBI's national initiative on child pornography focuses on those who indicate a willingness to travel for the purpose of engaging in sexual activity with a child; those who produce and/or distribute child pornography and those who post illegal images onto the online services and the Internet. Through this initiative, FBI agents and task force officers go on-line, in an undercover capacity, to identify and investigate those individuals who are victimizing children through the Internet and on-line service providers. Fifty-five FBI field offices and a number of legal attaches are assisting and conducting investigations in direct support of the "innocent images" initiative.

The "innocent images" national initiative is coordinated through the Baltimore division of the FBI. This initiative provides for a coordinated FBI response to a nationwide problem by collating and analyzing information and images obtained from numerous sources to avoid duplication of effort by all FBI field offices.

The Baltimore division's investigative operation involves the commitment and dedication of Federal, State and local law enforcement agencies, working together in a task force environment. The FBI believes that law enforcement agencies should work together, in a coordinated effort, to address crimes against children facilitated by the Internet. It is this sharing of manpower and resources that will ultimately provide the most effective tool in combating this egregious crime problem.

Although the "innocent images" initiative is coordinated through the FBI field office at Baltimore, this operation has been expanded to other FBI field offices throughout the United States.

The FBI has taken the necessary steps to ensure that the "innocent images" national initiative remains viable and productive. These efforts include the use of new technology and sophisticated investigative techniques and coordination of this national investigative effort with other Federal agencies that have statutory investigative authority, including the United States Customs Service, the United States Postal Inspection Service; the Department of Justice's child exploitation and obscenity section (part of the criminal division); the NCMEC; and numerous commercial and independent on-line service providers.

To date, the following accomplishments have been recorded as a direct result of the "innocent images" national initiative: 196 indictments, 75 informations, 207 convictions, and 202 arrests. In addition, 456 evidentiary searches have been conducted.

The FBI also conducts an outreach program to inform the public and local law enforcement agencies about this national initiative. In the past two years, the FBI has addressed a number of civic, judicial, prosecutive and law enforcement organizations concerning this initiative and the assistance the FBI can provide in investigating crimes against children facilitated by the Internet. This year alone, the FBI has conducted 4 Internet child pornography symposiums around the country for state and local law enforcement. The FBI recently assigned a supervisory special agent, on a full-time basis, to the NCMEC. The FBI strongly believes that it must work closely with the NCMEC, a national resource center for child protection, to locate and recover missing children and raise the public awareness about ways to prevent child abduction, molestation and sexual exploitation. I believe that the assignment of this FBI agent will enhance coordination between the two organizations and benefit the nation in our fight to combat crimes against children.

As I mentioned earlier, the FBI has investigated 152 cases involving pedophiles traveling interstate to meet minors for the purpose of engaging in illicit sexual relationships.

One example of a traveler case involved a resident of Rockville, Maryland, who pled guilty to 2 counts of interstate travel to engage in sexual activity with a minor (title 18, USC, section 2423). Through investigation, this individual was found to have traveled from his Maryland home to the Springfield, Virginia, public library for the purpose of meeting a 12 year old female in order to have sex. After this subject's arrest, a review of his Internet e-mail messages revealed that the subject had been posing as a 16 year old and had communicated with a number of other girls, between the ages of 10-15, attempting to meet them for sex.

In another similar case, a Bensalem, Pennsylvania school bus driver traveled from his home to the Pentagon City Mall in Arlington to engage in sex with an individual he thought was a 13 year old boy. The supposed 13 year old boy was actually an undercover officer assigned to the Baltimore FBI's Mid-Atlantic Child Exploitation Task Force (MARCET). The undercover officer came in contact with the subject during on-line undercover sessions. The subject was arrested when he arrived at the Pentagon City Mall. The subject was recently sentenced to 24 months in Federal prison.

Crimes against children are among the most emotional and demanding cases that investigators and prosecutors must face. The FBI will continue to work closely with other law enforcement agencies, NCMEC and the Department of Justice's CEOs to investigate, arrest and convict those individuals who prey upon our Nation's children.

This concludes my prepared remarks.

Parental Guidelines Regarding Their Children's Use of Computers, Contributed by the National Center for Missing And Exploited Children

- 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

50-939 98 - 3

are 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.

- 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, or a sexual nature, or threatening, forward a copy of the message to your service provider and ask for their assistance.
- 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. Discuss these rules and post them near the computer as a reminder. 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 service should not be used as electronic babysitters. Get to know their "online friends" just as you get to know all of their other friends.

Mr. OXLEY. Thank you for your testimony. We have a vote on the floor. We would like to have you back for question and answer. You can check with the director, if that is all right, to stay for a little longer.

We will return at 12:15.

[Brief recess].

Mr. OXLEY. The subcommittee will reconvene. Thank you, Mr. Wiley, and the other witnesses on the next panel for your patience. Let me begin with some questions for you. First of all, some of the members in their opening statements made reference to the fact that we really have a global phenomenon here that the World Wide Web indeed carries a lot of illicit information, pornography and the like. What has been the FBI's experience with that? Is it in fact a worldwide problem and if it is a worldwide problem how can we deal with it within the confines of just the United States and our own statutes?

Mr. WILEY. Mr. Chairman, it is a worldwide problem. It is a significant problem, particularly in child pornography, and generally speaking child pornography is illegal in almost all countries, not all, so that makes it probably easier to investigate international cases because international law enforcement will investigate their own violations of their own laws.

Mr. OXLEY. Was that the case in the recent case we read about?

Mr. WILEY. Yes, sir. I might mention that was a U.S. Customs Service case working with other foreign law enforcement so there was a mutual need to work together. That may not necessarily be true in adult pornography.

Mr. OXLEY. Do you know anything about the Dial-A-Porn issue and how that has affected the ability of our country to deal with the Dial-A-Porn problem as it relates to foreign initiated calls?

Mr. WILEY. No, sir, I am really not very conversant in the adult aspect of this. We have pretty much focused all of our efforts in the child pornography area.

Mr. OXLEY. In your opinion, if this law were to be passed, to what extent would this increase the Bureau's ability to detect and arrest these folks and would it in fact require more resources on the part of the FBI than have currently been allocated?

Mr. WILEY. Here I will address your last question first. I think it would require significant resource enhancement. I would suspect that we would have a lot of people calling every office talking about coming up on the Web site and seeing these locations and reporting them. We would have to do something with it and try to determine whether it fell under whatever the statute defines as a commercial entity. We would have to determine that.

Mr. OXLEY. Now, the Bureau would not be the only agency that would be involved with that process. You point out, for example, Customs. We recently had a case in my district involving pedophiles who were men masquerading as women on the Internet and enticed a young boy from Mansfield, Ohio to where they wanted them to join him. That was handled, I met with the parents, talked with the parents. That was handled by the postal authority. So there are several agencies, Federal and local, that deal in these kinds of issues.

Mr. WILEY. Yes, sir. Postal obviously are involved in incidents involving the mails. However, they work on our innocent images task force as well as an agent from Customs so that we are able to, if we have a postal case, they get the case and they work with it. The same with a foreign case, we give it to Customs. And in the task forces in the field we try to do the same thing with State and local and the other Federal agencies, as I mentioned in my testimony, to really try to leverage resources and the different jurisdictions to work together.

Mr. OXLEY. There was a recent article, I think it was in USA Today and appeared in several other periodicals, that dealt with a small town in Massachusetts where the officer there was involved in a number of cases, just in that small town in Massachusetts. I gather from the article that that was handled on a local basis for the most part. Am I to assume then that that kind of activity in terms of law enforcement is going on all over the country now?

Mr. WILEY. It is certainly becoming more prevalent by investigations by local law enforcement. This Congress, in addition to giving the FBI additional funds for this initiative, made available grant money to the Department of Justice, who is making that money available to State and local law enforcement to form their own task forces. So we will have more law enforcement tasks forces addressing the child pornography issue.

Mr. OXLEY. Does the Bureau have a fairly comprehensive list of pornographers, commercial pornography companies that are in existence? Congressman Istook told us there was an $8 billion a year industry. Do you have a pretty good handle about who they are and where they are?

Mr. WILEY. Not in adult pornography, no, sir. Our efforts are in the child pornography area and we go to predicated sites when we are on the Internet. We don't do surfing. So we will go into predi-

cated sites or sites that are where citizens or other law enforcement agencies tell us we can find child pornography.

Mr. OXLEY. In the case of the situation whereby the so-called adult pornographers put these enticing screens on and entice children to pursue that, then all of a sudden that line between adult and minors becomes very, very blurry; is that correct?

Mr. WILEY. It would for us. It would certainly, if we have indication that it is an adult site, but it is advertising to children to us that would be a key element. We would take a look at that. In fact you have that in adult chat rooms where children might be.

Mr. OXLEY. The effort, our legislation really is in essence to try to segment that, to try to wall off, if you will, the access of children to that kind of material through dealing with the screens that are out there, the enticing screens from a commercial establishment that would be kind of a magnet for young people in many respects. That is why it is set up to do that and, second, to provide for and only deal with commercial people, people who are making money on this stuff.

I am not going to ask you for a legal opinion, but in your work, does it appear that we are on the right track in that regard to try to not only deal with the commercialization of it but also to be very clear that we are attempting to keep minors from doing this and having some ability to identify themselves to the purveyors before they have access to that material?

Mr. WILEY. I think I would defer to the Department of Justice regarding the merits on the bill. However, I would say child pornography is absolutely illegal, yet it is all over the Internet. And there are a number of different doors to access child pornography, and that is true of adult pornography. You don't have commercial sites for child pornography, but if you do for adults, you have other access, other doors to walk into that are not commercial, and that is where you find a lot of child pornography. Whether there are Web sites that are privately owned, private Web sites where they trade pornography, news groups, it serves. There is a lot of private activity on the Internet, and it is all private with the child pornography and the same with adult pornography.

Mr. OXLEY. Well, when you are describing child pornography, you are describing pornography that depicts children; right?

Mr. WILEY. Yes, sir.

Mr. OXLEY. And in that way we are talking about children's access or potential access to that material as well as adult smut, pornography; right?

Mr. WILEY. Yes, sir. What I was trying, the point I was trying to make is that child pornography is absolutely illegal to have, yet it is all over the Internet. And if the bill is addressing commercial entities, there are a lot of private entities out there that are dealing with pornography. So it is hard for me to make a judgment about the merits of the bill and how effective it would be.

Mr. OXLEY. Well, the Communications Decency Act that was upheld said that agencies like yours could still enforce the CDA with respect to obscenity and so what we are trying to do is fill that void as it relates to minors. Your charge is to deal with child pornography, as you described it, as well as, not necessarily FBI,

but obscenity as we have come to understand the definition by the Supreme Court over several numbers of years.

Mr. WILEY. We do work obscenity cases. I can't say that there are a lot of them just because it is a resource issue. But we are charged with the statute that involves interstate transportation of obscene material.

Mr. OXLEY. And that was a popular part of the FBI academy at Quantico, as I recall.

It does not deal specifically with commercial enterprises, does it?

Mr. WILEY. The interstate transportation and, of course, the issue is obscenity and the community standards, which all comes into whether it is a case that could be investigated or prosecuted.

Mr. OXLEY. It could be interstate and not commercial?

Mr. WILEY. Yes, sir.

Mr. OXLEY. We are pleased to have you here, Mr. Wiley. Thank you so much for your testimony and for your patience in waiting for us. Come back again.

Mr. WILEY. Thank you Mr. Chairman.

Mr. OXLEY. I would like to call our third panel. As you are getting set up, I will introduce the rather lengthy and distinguished panel that we have before us. Mr. Jerry Berman, Director of the Center for Democracy and Technology here in Washington; Mr. Laith Paul Alsarraf, President and CEO of Cybernet Ventures, Van Nuys, California; Professor Lawrence Lessig from Harvard Law School in Cambridge, Massachusetts; Mr. Andrew L. Kupser, Chief Executive Officer of Northwest Internet Services, Poulsbo, Washington; Ms. Agnes M. Griffen, Director, Tucson-Pima Public Library, Library Administration, Tucson, Arizona; Mr. Jeffrey J. Douglas, Executive Director, Free Speech Coalition, Santa Monica, California; Dr. Mary Anne Layden, Center for Cognitive Therapy at the University of Pennsylvania; Mr. Peter Nickerson, Chief Executive Officer of N2H2 in Seattle, Washington; and Mr. Bastian, Chief Executive Officer, Security Software Systems Inc.

You run the fate of the last panel, which is sometimes after the last vote and after you have had to sit through opening statements of the members and member panels and the like. The only good thing I can tell you about it is that you followed the FBI and that can't be all bad.

Let me begin with Mr. Berman down here and we will move from left to right.

STATEMENTS OF JERRY BERMAN, DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY; JEFFREY J. DOUGLAS, EXECUTIVE DIRECTOR, FREE SPEECH COALITION; LAITH PAUL ALSARRAF, PRESIDENT AND CEO, CYBERNET VENTURES, INC.; MARY ANNE LAYDEN, CENTER FOR COGNITIVE THERAPY, DEPARTMENT OF PSYCHOLOGY, UNIVERSITY OF PENNSYLVANIA; LAWRENCE LESSIG, PROFESSOR, HARVARD LAW SCHOOL; PETER NICKERSON, CHIEF EXECUTIVE OFFICER, N2H2; ANDREW L. KUPSER, CHIEF EXECUTIVE OFFICER, NORTHWEST Internet SERVICES, LLC; JOHN C. BASTIAN, CHIEF EXECUTIVE OFFICER, SECURITY SOFTWARE SYSTEMS INC.; AND AGNES M. GRIFFEN, DIRECTOR, TUCSON-PIMA PUBLIC LIBRARY

Mr. BERMAN. Mr. Chairman, we appreciate the committee requesting our testimony today. The Center for Democracy and Technology is a civil liberties organization dedicated to achieving the democratic potential of the Internet. That is our focus, and we work with nonprofits who work with the private sector, work with policymakers to try and find solutions that balance conflicting interests. We, since the beginning of the issue of child pornography and pornography on the Internet, have been trying to work for solutions which strike a balance between constitutional liberties and protection of our children.

Because the Communications Decency Act, we think, was far too broad and ineffective and unconstitutional, we led one of the serious challenges to that act and helped and brought a challenge with the American Library Association, America On-Line and many of the on-line companies in order to educate the Court about the nature of the Internet and to say that this is a new medium, it is a world medium, it is a decentralized medium and that any solution that we need to have here has to protect free speech in that new medium and also protect our children. And our argument, which prevailed before the Supreme Court, was that the Communications Decency Act was unconstitutional and ineffective. The Court agreed with us, and one of the most important things they said was that Congress had not really laid a legislative record for the proposal that it had passed.

I think that we are 2 years down the road and we are looking at a very similar situation. The Supreme Court in that 9-0 decision said that there were less restrictive means than a statute which barred adults from receiving material which they are constitutionally permitted to do that could solve the problem and would be more effective in protecting children from pornography. We are here with this statute, and I do not think that the Congress has held the appropriate hearings, I wish they would, to lay the legislative record of why the technology solutions are not less restrictive and I am talking about voluntary solutions that are out on the market and more effective than the statute that is being proposed today, the series of statutes. I think that while the statutes that are being proposed are narrower than the Communications Decency Act, they fall under the same problems, they are ineffective, they raise constitutional issues and they are unnecessary and unworkable.

First of all, the FBI is dealing with child pornography and obscenity on the Internet. That is already illegal. They have a very big enforcement problem. It needs to be carried on, and I think what the FBI witness said is that under this statute they are going to have to divert resources to try and sort it out, whether this statute is protecting children from material which adults are entitled to but which they are not entitled to on the Internet. That is a much broader investigative mandate and may be a diversion. Even if the statute is successful in taking the commercial smut peddler and putting their pictures behind a wall in the United States, as we pointed out in the Supreme Court, over 40 to 50 percent of the material that is on the Internet is coming in from foreign sites. Moreover, rather than putting something in law which is going to help give some certainty to the industry, the statute that you drafted may not be as broad, but I think it has constitutional problems with it, maybe not facially, as the term is; in other words, it is clearly unconstitutional on its face, but in its application.

First of all, we don't know what harmful to minors means in the context of a national standard. Your legislation proposes a national standard and for the FCC to sort this out. The Supreme Court has always held that every local community could decide what was harmful to minors under its statutes. This puts the FCC in the business of regulating the Internet. The statute is supposed to only apply to commercial providers but it also applies to those who may be of benefit from transmitting the material on the Internet which may be harmful to minors. That includes America On-Line, that includes many of the ISPs, and they would be put in the position, which the Supreme Court held was a mistake and unconstitutional, of trying to screen what material is being provided to make sure that adults could get it but that children could not.

Without a national definition of harmful to minors, we don't know what it includes. I, for example, am not clear under your statute whether the Starr report or parts of the Starr report could be published on the Internet under a harmful to minors statute because it may not have redeeming social importance for younger minors. Representative Markey raised that. I think that is a legitimate question. Someone may be prosecuted under this statute for excerpting parts of the report and saying this is the interesting part and clipping it and sending it somewhere else on the Internet. Do they face liability? Under the harmful to minors regime that we have in the United States, the 7-11s of the world, the publishers are a small group of people who can figure out with a lot of lawyers what harmful to minors means under these 50 different State statutes.

Mr. OXLEY. We have to move on.

Mr. BERMAN. The Internet has millions of providers who will have the chilling effect of trying to figure out what harmful to minors means.

My last point is on providing filtering technologies to schools. Schools are trying to find the answer to these problems now. The cost may be prohibitive. They may not, the products on the market may not let them do their own local choice. You were substituting commercial choices for local school boards, which is, I think, con-

trary to our view of how education should be structured in this country.

Third, Mr. Markey and others have recommended having ISPs provide software. That is a potential solution. A lot of them are doing it. More has to be done. More has to be done to make it more simple and accessible to parents. A lot can be done but it will not be done by passing a narrow statute which is ineffective. I think that this committee should start again, get some real information on how the Internet works, and hold a serious set of hearings on how it works. If you want to get some handle power on this, there are proposals for zoning cyberspace into an adult domain zone, providing a one click away solution so that parents can find this stuff easily, figure out whether adult verification systems work, have that studied for the next 6 months, get some real brainpower focused on the legal, technical solutions that are out there and which makes the most sense.

[The prepared statement of Jerry Berman follows:]

PREPARED STATEMENT OF JERRY BERMAN, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

My name is Jerry Berman, Executive Director of the Center for Democracy and Technology. The Center is pleased to participate in this hearing at the request of the Subcommittee. We welcome the opportunity to address a critical issue: how to achieve the goal of protecting children from inappropriate material on the Internet consistent with constitutional values and the growth and health of the Internet.

The Center for Democracy and Technology (CDT) is an independent, non-profit public interest policy organization in Washington, DC. The Center's mission is to develop and implement public policies to protect and advance individual liberty and democratic values in the new digital media. The Center achieves its goals through policy development, public education, and coalition building.

From it inception in January 1995, the Center has played a leading role in policy debates on how to protect children from inappropriate material online. In particular, we view this issue through the experience of the legislative process that resulted in Congress' first attempt to regulate content on the Internet—the unconstitutional Communications Decency Act (CDA). As the coordinator of the Citizens Internet Empowerment Coalition (CEIC), CDT joined with the American Library Association, and others, to rally civil liberties organizations, the library and publishing communities, Internet service providers, and individual users of the Internet to challenge the CDA. In federal district court in Philadelphia, the coalition undertook an educational effort to demonstrate for the judges the unique nature of the Internet—something Congress had failed to consider when it enacted the CDA. We gave the court a tutorial on the Internet. The Supreme Court decision in *Reno v. ACLU*[1] (hereinafter the "CDA decision") striking down the CDA on First Amendment grounds was largely based on the factual findings of the lower court detailing the nature and characteristics of the Internet.

Our message today is simple: The legislative proposals before the Subcommittee today, repeat the mistakes of the CDA. They fail to take into account the special aspects of this potentially powerful medium. They are ineffective, unconstitutional, or unnecessary.

I. THE CDA DECISION

In the CDA decision, the Supreme Court struck down a sweeping attempt by Congress to regulate a broad and undefined category of speech, "indecency," across a wide range of Internet interactions including email, chat groups, and the World Wide Web. As the Supreme Court recognized, the Internet offers new and unique opportunities to maximize the ability of individuals and families to choose the content worthy of their attention. The Court found that users of the Internet are not assaulted by material, and that the risk of encountering unwanted "material by accident is remote because a series of affirmative steps are required to access specific material." The Court concluded that the Internet should not be treated like a broad-

[1] 117 S.Ct. 2329 (1997).

cast medium. As the Court stated, "Unlike the conditions that prevailed when Congress first authorized regulation of the broadcast spectrum, the Internet can hardly be considered scarce expressive commodity. It provides relatively unlimited, low-cost capacity, for communication of all kinds..." The Internet is a global medium and much of the material that would be considered offensive is produced overseas. "Unlike other media, there is no technologically feasible way for an Internet speaker to limit the geographical scope of his speech...or to 'implement [] a system for screening the locale of incoming' requests."

II. THE CURRENT PROPOSALS

Before the Subcommittee today are at least seven well-intentioned but flawed efforts to address the complex problem of protecting children from speech that is considered inappropriate for them. The bills take three distinct approaches, reflecting the complexity of the issue and the diversity of opinions about the role federal legislation can play in solving it. Each of the seven bills before you today is narrower than the CDA and each reveals an effort to more appropriately balance constitutional values in the effort to protect children. Nevertheless, none of the bills succeeds in this effort.

The bills can be placed in three general categories:

- Harmful to minors—The Child Online Protection Act (H.R. 3783) requires entities that sell or transfer information considered "harmful to minors" to restrict access to those under 17. The bill seeks to erect around inappropriate information on the World Wide Web virtual walls that those under 17 cannot climb—in effect zoning the Web.
- Protecting children in the school and library settings—Two bills, the Safe Schools Internet Act (H.R. 3177) and the Child Protection Act adopted by the Labor, Health and Human Services, and Education Appropriations Subcommittee), would condition federal e-rate funding for schools and libraries on the use of filtering technology. A third bill, the E-Rate Policy and Child Protection Act (H.R. 3442), conditions e-rate funding on the adoption of policies outlining "acceptable use" of the Internet.
- Providing parents with access to content selection software—Three bills—the Internet Freedom and Child Protection Act (H.R. 774), the Communications Privacy and Consumer Empowerment Act (H.R. 1964), and the Family-Friendly Internet Access Act (H.R. 1180)—require Internet access providers to make filtering software designed to limit children's access to inappropriate information available to subscribers at the time they sign up for service.

III. BY WHAT STANDARDS SHOULD WE MEASURE THE PROPOSALS?

There are three key factors to consider in weighing proposals to protect children from inappropriate content:

- will a given proposal effectively protect children from the material found inappropriate;
- what is the proposal's impact on constitutionally protected speech, and,
- what liability and burdens would the proposal impose on those who provide Internet access, be they libraries, schools or Internet Service Providers.

Assessing the seven bills in terms of effectiveness, protection of constitutionally protected speech, and burdens on those who provide access to the Internet, CDT concludes that the bills fall short. Some appear unconstitutional on their face while others are likely to be applied in a fashion that violates First Amendment and privacy values. Others, while probably constitutional, are unlikely to substantially address the problem at issue. Several require the private sector, libraries and schools to engage in efforts that are already well underway.

The bills will prove ineffective at meeting the goal of protecting children. In the past, it was assumed that governments could control print or broadcast material within their borders, and that publishers had some ability to control and direct the distribution of their materials. The physical nature of the media by which information and ideas were produced and, disseminated meant that they were controllable.

On the Internet, neither governments nor publishers can control the distribution of material made available over the Web. As the findings in the CDA case state, "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community. Unlike newspaper, broadcast station, or cable system, Internet technology gives a speaker a potential worldwide audience."

The global and decentralized nature of the medium and the fact that it does not allow publishers to easily discern who is seeking and requesting information are barriers to the effective implementation of laws to protect children from information

online. In the CDA decision, the Court found that objectionable information is likely to come from outside the US and be unreachable by US laws. "The district court found that a 'large percentage, perhaps 40% or more, of content on the Internet originates outside the United States'..." "Because of the global nature of the Internet, material posted overseas is just as available as information posted next door." In addition it is difficult to discern, and make access decisions based on, age.

Several of the proposals will limit access to constitutionally protected speech and are not narrowly tailored to meet the government's interest in protecting children from inappropriate information.

Three of the bills—the Online Children's Protection Act, the Safe Schools Internet Act, and the Child Protection Act—will in their application limit adults' and older minors' access to constitutionally protected information. The "harmful to minors" bill attempts to nationalize a standard the Supreme Court has always tied to local community standards. The school filtering bills are likely to result in the filtering of speech far beyond what is considered obscene or harmful to minors. As the Supreme Court restated in the CDA decision, "The level of discourse reaching a mailbox simply can not be limited to that which would be suitable for a sandbox' and this is so '*regardless* of the strength of the government's interest' in protecting children." Despite the more limited scope of these bills, we believe they are not tailored to address the problem at issue.

Several of the proposals will burden those who provide access to the Internet with little benefit to children.

Under four of the bills, Internet access providers are required to take steps to control the content available to minors. While seeking to exercise control over content through ISPs may at first glance seem attractive, making them responsible for information that merely travels through their systems would fundamentally change the nature of the Internet an is practically impossible. ISPs cannot easily monitor the enormous quantity of network traffic to stop the incoming flow of material. Selectively disabling access or limiting transmission to particular users is complicated and in many cases practically impossible. Electronic networks typically do not allow for the identification of particular users or their geographical location. The goal of providing children with enriching experiences on the Web that reflect the norms and values of their parents, and the communities in which they live, is one share by many organizations who oppose these bills, including CDT. CDT believes that as a society we have a responsibility to protect children from information deemed inappropriate, and to provide those responsible for our children's well being with the information, resources tools to accomplish this goal. But we firmly believe that achieving this goal must be accomplished in a manner that is consistent with First Amendment values and respects the diversity of parental and community values across the nation.

IV. ANALYSIS OF PROPOSALS

A. Harmful to minors

The Child Online Protection Act is narrower than the CDA. It requires entities engaged in the business of transferring or selling over the World Wide Web information deemed "harmful to minors" to place it behind a barrier surmountable only by those over 17. Unlike the "indecency" standard of the CDA, the Child Online Protection Act seeks to use a term that has been recognized "harmful to minors." However the bill strays from existing "harmful to minors" law, which is based upon local community standards, seeking to establish a national definition of information that is considered "harmful to minors."

Harmful to minors should be based on community norms, not a national standard. The core of the Child Online Protection Act is to set a single national standard defining speech that cannot be made available to minors over the World Wide Web. The creation of a national "harmful to minors" standard will constrain the ability of communities to determine what information is appropriate for their children. Centralizing content decisions in federal government runs counter to existing "harmful to minors" law as articulated by Supreme Court.

The US Supreme Court has never approved of a single, national obscenity standard, nor has it approved a "harmful to minors" statute based on a national, as opposed to local, standard. The Court's decisions defer to local community standards. As the Court stated in the landmark obscenity decision *Miller v. California,*[2] there cannot be:

> fixed, uniform national standards of precisely what appeals to the "prurient interest" or is "patently offensive." These are essentially questions of fact, and our

[2] 413 U.S. 15 (1973).

> Nation is simply too big and too diverse for this Court to reasonably expect that such standards could be articulated for all 50 states...[3]

Replacing local decision-making with federal standards will have unintended consequences. It may create a "lowest-common denominator" where the community that is least tolerant of speech is able by default to set the national standard. This could greatly reduce the amount of information that children and adults can access in areas with great tolerance for speech. In the alternative, a national standard may limit conservative communities' ability to adopt standards that go beyond a federally-defined base line.

In addition, the novel approach of a *national* "harmful to minors standard" raises vagueness concerns. How can affected entities determine what a cross section of the nation will find harmful to minors? Without clearer guidance—which the bill on its face suggests is necessary—this new and novel national standard provides little information about the activities prescribed by the bill.[4]

Broad scope. While the bill seeks to govern commercial actors, it covers all entities engaged in "the business of selling or transferring" material that is "harmful to minors" by means of the Web. Entities affected by the bill go well beyond commercial pornographers. This definition potentially includes Internet access providers, bookstores, and non-profits that offer items for sale. The bill places in jeopardy not only the creator of the content but also all who may sell or transfer it, whether or not it is their business and regardless of whether money is exchanged, over the Web. ISPs do not know what information is transferred across their system. Many of the entities likely to be affected by the bill are unable to make use of the age verification techniques that comprise the affirmative defenses due to cost and/or availability.[5]

The affirmative defenses found in the bill will spur the collection of personal information about individuals and their First Amendment activities. Under the First Amendment, a barrier to accessing information must be the least restrictive form that the medium supports. Where the barrier conditions access in ways that may chill individuals' exercise of their First Amendment right to read or access information the Court has struck down burdens.[6] Due to the state of current age verification systems, the affirmative defenses found in the bill will push individuals into the position of having to disclose personal information—in some instances including name, address, social security number, in addition to credit card—to the publisher or a third party in order to access information. Current age verification technologies tend to be identity driven.[7] Reliance on such systems will create records of individ-

---

[3] Id. At 30.

[4] While the bill directs the Federal Communications Commission to publish information defining "harmful to minors" on the Web, the Commission's ability to provide guidance is circumscribed by earlier case law. See Bantam Books v. Sullivan, 372 U.S. 58. In Bantam the Court held that the activities and procedures of a commission in notifying distributor; that certain books or magazines distributed by them had been declared objectionable for sale to youths under 18 was a system of informal censorship. Id. at 21. The Court stated that, while the state may regulate obscenity such regulations must "scrupulously embody the most rigorous procedural safe-guards." Id. at 14. It found that the Commission's actions operated as a form of censorship without any of the procedural and substantive safeguards provided by criminal prosecutions, provided no safeguards against the suppression of constitutionally protection information, and created greater hazards to protected speech than reliance upon the criminal law. Id. at 18.

For example, the Court struck down a law that required people who wished to receive "communist literature" to sign-up at the post office. Lamont v. Postmaster General, 381 U.S. 301 (1965). More recently in Denver area Educational Telecommunications Consortium, Inc. v. FCC the Court held that the government may not require adults to affirmatively request controversial but protected material in order to receive it. 116 S. Ct. 2374 (1996).

The FCC's ability to publish examples of information (books and magazines) considered harmful to minors or provide other guidance is questionable because it may be found to fun afoul of the rigorous procedural safe-guards required by obscenity case law.

[5] The federal district court stated in its finding of facts: The burdens imposed by credit card verification and adult password verification systems make them effectively unavailable to a substantial number of Internet content providers. Finding of Fact 107.

[6] For example, the Court struck down a law that required people who wished to receive "communist literature" to sign-up at the post office. Lamont v. Postmaster General, 381 U.S. 301 (1965). More recently in Denver area Educational Telecommunications Consortium, Inc. v. FCC the Court held that the government may not require adults to affirmatively request controversial but protected material in order to receive it. 116 S. Ct. 2374 (1996)

[7] The following are examples of age verification systems being used on the Web: 1) Playboy—pay section charges $60/year via credit card, asks for general personal information; 2) Penthouse—free, asks for credit card and email and country; 3) Hustler—pay section charges $90/year via credit card, asks for general personal information; 4) www.ultravoyeur.com—pay section offers one month free trial, $40/month must give credit card and name on card to choose

Continued

uals' First Amendment activities. Currently there are no rules limiting the private sector use of such information and it is unclear whether law enforcement access to these records would be constrained by existing law. Conditioning adult access to constitutionally protected speech on a disclosure of identity raises troubling First Amendment and privacy issues. The defenses pose a Faustian choice to individuals seeking access to information—protect privacy and lose access or exercise First Amendment freedoms and forego privacy.

The bill does not use the least restrictive means. The CDA decision sent a clear signal to Congress that, when seeking to regulate speech on this new medium, government must use the least restrictive means available. As the Court restated in the CDA decision, 'the level of discourse' "reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox" and this is so "*regardless* of the strength of the government's interest' in protecting children."

While H.R. 3783 seeks to regulate access to a narrower category of speech than the CDA, that does not mean that it will pass the least restrictive means test. The burdens placed on speech by this bill may be found too great in light of the inability of national censorship laws to effect the availability of information from non-domestic sites on the World Wide Web and from a variety of other Internet media such as Usenet newsgroups chat, bulk-email, electronic bulletin boards, not to mention non-electronic media.

The CDA decision, and the findings of fact upon which it is based, identified filtering and blocking technologies as a narrow, media-appropriate means of providing families with the means of protecting their children while meeting the diversity goals of the First Amendment. Congress has not held hearings to determine whether technical tools or this bill could be the least restrictive means of protecting children. There has been no study, no discussion, and no comparison of the effectiveness of various approaches, their likely impact on speech, and their appropriateness for the Internet.

B. Protecting children in the school and library setting

The Safe Schools Internet Act (H.R. 3177) and the Child Protection Act (adopted toy the Labor, Health and Human Services, and Education Appropriations Subcommittee) condition federal e-rate funding for schools and libraries on the use of filtering technology. In contrast, the E-Rate Policy and Child Protection Act (H.R. 3442) conditions e-rate funding on the adoption of an acceptable use policy. While all three are aimed at ensuring that libraries and schools take steps to protect children from inappropriate information when they are outside their parents' eyes, they are likely to have very different impacts on constitutionally protected speech. Of all the bills, the E-Rate Policy and Child Protection Act is likely to be the most respectful of local authority and is least likely to pose constitutional problems.

Requirements to adopt filtering technology will effectively usurp local communities' ability to set standards that reflect their values. While a goal of the Safe Schools Internet Act and the Child Protection Act is to maintain local autonomy, the actual impact of the bills is likely to mirror the Child Online Protection Act's drive toward a national standard. Unlike the national "harmful to minors" standard discussion above, the bills on their face are quite protective of community prerogatives. However, due to several factors the impact of the bills is unlikely to meet this intent:

- Currently available and reasonably priced filtering technologies do not mirror the diversity of local community norms found across the country.
- The budgetary constraints under which libraries and schools operate are likely to limit their ability to custom design filters that meet their community standards.
- The ability of schools and libraries to assess whether commercially available filters meet their needs will be stymied by companies that currently do not disclose the standards under which they filter or the list of filtered sites.
- Some schools and libraries may lack the technical expertise and resources to choose and deploy filters.

The impact of requiring schools and libraries to implement filters is likely to be the replacement of the existing diversity of local community norms with a narrower

---

a PIN, other personal information is optional. If you don't have a credit card you can bill your phone (you are given a server id then you call a 900-number, they give you a temporary "redemption code" then submit redemption code, email address username and password via form. "Discreetly billed as 'WEB ACCESS.'") or pay by check (asks for lots of PII including SSN) or mail in (which you could use check, money order or cash although you still need to give a name—which could be forged—and an email address—which could be a hotmail or other virtual account although most of those ask for PII too); and, 5) www.sensual-photography.com—pay section charges $2/month asks for credit card and personal information or check info, lots of personal information including SSN and/or drivers license.

set of views offered by companies that provide off the shelf filtering and blocking tools. In order to maintain funding libraries and schools may find themselves out of step with their communities' values. This in turn may subject them to litigation;

Similarly, the requirement to install filtering software interferes with decisions by local communities, educators, and librarians to protect children through other means. These institutions are actively pursuing solutions that are responsive and appropriate to their specific missions, goals, and constituencies. Thoughtful local decision-making would be replaced by the decisions made by private companies—many of which are shut off from public scrutiny due to lack of disclosures about the process or guidelines for blocking sites. The prospect of schools and libraries being forced by budgetary constraints to choose between forgoing funding or delegating their traditional power to unchecked private entities raises troubling First Amendment issues.

Restricting speech. While the Supreme Court has upheld the government's right to restrict speech that it funds where the speech reflects government policy,[8] the government may not restrict speech where the purpose of funding is to propagate a diverse range of private views.[9] E-rate funding is explicitly designed to facilitate access to the Internet—a broad range of ideas and views—not to express a specific government policy. Several studies of commercial available filters suggest that they curtail access to information on topics ranging from gay and lesbian issues, women's health, conservative politics, and many others.[10] If libraries and schools are faced with a limited set of options, this approach may force them to censor more than they would choose and in effect discriminate against specific viewpoints.

The bills will alter adults' ability to access constitutionally protected material in ways that will constrain and in some instances violate their First Amendment rights. Currently adults and children are able to access information that falls into the "harmful to minors" category in the same way they access other information online. In schools and libraries with only one terminal the requirement to install and activate filtering software will require adults and older minors to affirmatively request access to constitutionally protected information. As noted above the Court has stated that the government may not require adults to affirmatively request controversial but protected material in order to receive it.[11] Acceptable use policies would avoid this problem.

C. Providing parents with access to content selection software

The Internet Freedom and Child Protection Act (H.R. 774), the Communications Privacy and Consumer Empowerment Act (H.R. 1964), and the Family-Friendly Internet Access Act (H.R. 1180) are aimed at making screening software designed to limit children's access to inappropriate or unsuitable information more readily available to parents in the home. They require Internet access providers to offer subscribers such software at the time the sign up for service. These proposals are unnecessary. Private sector efforts are already well advanced to place technical tools within easy reach of parents. Congress would be wise to let the market continue on its own for a number of reasons:

- Choice—while many ISPs do choose a specific tool to offer subscribers, forcing such a choice may stifle the development of better filters by giving preference to existing products.
- Content control—while filters are an appropriate market-response to the need to address children's safety online, the current lack of transparency about what is being filtered and what criteria underlies it must be addressed before they are truly useful tools for parents to use in guiding their children's online experience. In addition, ISP selection of filters may steer their users access to information.

V. ALTERNATIVES TO LEGISLATION

While the Congress and courts around the country have been debating whether censorship laws can protect children online, companies and non-profit organizations have responded with wide-ranging efforts to create child-friendly content collections, teach children about appropriate online behavior, and develop voluntary, user-con-

[8] See, Rust v. Sullivan, 500 U.S. 173 (1991) (upholding prohibition on abortion counseling at federally funded family planning clinics).

[9] See, Rosenberger v. Rector & Visitors of the Univ. of Virginia, 515 U.S. 819 (1995) (striking down public University's exclusion of religious organizations from access to generally available student activity funds).

[1] See, Access Denied: The Impact of Internet Filtering Software on the Lesbian and Gay Community (GLAAD); Farenheit 451.2: Is Cyberspace Burning (ACLU); and, Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet (EPIC).

[11] Denver, 116 S. Ct. 2374 (1996)

trolled, technology tools that offer parents the ability to protect their own children from inappropriate material. Unlike legislative approaches, these bottom-up solutions are voluntary. They protect children and assist parents and care-takers regardless of whether the material to be avoided is on a US or foreign Web site. They respond to local and family concerns. And they avoid government decisions about content. We would like to describe some of these initiatives to emphasize their diversity, their user-controlled nature, and their responsiveness to parental concerns.

Education, Green Spaces, and Other Initiatives. Many public-private initiatives are underway to help parents and children learn to navigate the Web safely, create kid-friendly content zones, and to work with law enforcement to ensure children's safety. They include:

- sites created by libraries and schools, to lists of useful sites compiled by libraries and educators, such as "Kids Connect Favorite Web Sites"[12] selected by school librarians for K-12 students;
- tools that guide kids while they explore the Internet, such as AOL NetFind Kids Only[13] a search engine that links only to sites that are safe for kids; and,
- hotlines that connect concerned parents and adults to law enforcement resources, such as the National Center for Missing and Exploited Children's Cyber tipline.[14]

In addition to ongoing efforts to develop resources, educational tools and child-friendly materials, the Internet community has sponsored several public events to highlight the issue of children's safety online, including access to inappropriate content, and inform the public of the resources and tools to address it. The Internet Online Summit: Focus On Children[15] was held on December 1st-3rd 1997. More than 650 participants representing over 300 organizations came together to assure that steps were taken to make the Internet online experience safe, educational and entertaining for children. Several major Initiatives emerged from the Summit, including:

- America Links Up A National Education Campaign
- A "Parents Guide to the Internet"
- ISP "Zero Tolerance Policy" on illegal materials online
- "CyberTips Line" a "911" for the Internet
- Law Enforcement and Internet Safety Forum
- Local Law Enforcement Computer Crime Training

Next week, the America Links Up: A Kids online Teach-In,[16] a broad-based public awareness campaign to ensure that every child in America has a safe, educational and rewarding experience online, kicksoff. Based upon the findings, recommendations and commitments made during the December 1997 Summit, the America Links Up coalition has committed to working with the online industry, families, teachers, librarians and other children's advocates to:

- Encourage active involvement of parents, teachers and other caregivers in children's online experiences;
- Educate and empower children to make wise, responsible decisions when active online;
- Heighten awareness of the need for all children to learn the information technology skills necessary for success in their future;
- Promote awareness of the "digital toolbox," technological and non-technological resources that promote safety and access to good content;
- Increase public awareness of safe online behavior, including that required to protect children from harmful and illegal material and conduct;
- Increase public awareness of the law enforcement and other resources available to protect children online; and,
- Encourage communities to get involved with children online and create a dialogue on issues important to the community.

The campaign begins with a National Town Hall meeting in Washington, DC. The teach-in will discuss the importance of the Internet to our children's future, the pitfalls that parents and teachers should be aware of, and how adults can keep children safe when they are online. Participants will include parents and kids, industry leaders, government experts, children's advocates, teachers and librarians. The meeting will also feature the unveiling of:

- "Take the Trip Together" Public Service Announcements;

[12] http://www.ala.org/ICONN/kcfavorites.html
[13] http://www.aol.com/netfind/kids/home.html
[14] http://www.missingkids.com/cybertip/
[15] http://www.kidsonline.org
[16] http:Hwww.americalinksup.org

- A safety video that will be distributed to schools across the country;
- A comprehensive guide to safety tools available to parents;
- A preview of activities going on in communities around the nation; and,
- The official launch of the America Links Up Web site as a resource for parents who want to learn more about the Internet. The Web site already includes tips for kids and their parents and Web pages featuring key Internet terms, Web site resources, and browsers and filters.

Acceptable use policies. Schools; libraries, and other educational and cultural community centers are already seeking ways to provide children with enriching and safe online experiences. A central component of these efforts is protecting children from inappropriate information. Approaches range broadly.

The United States Catholic Conference has developed an "Ethical Internet Use" policy under which each school or diocese adopts a policy detailing the rights and responsibilities of students, parents and teachers in Internet use. The policies are buttressed by contracts signed by students, parents and teachers. For example, Freemont Public Schools in Freemont, Nebraska, like many other public institutions, uses Acceptable Use Policies that educate students on how to access appropriate information and emphasize classroom supervision.

Other schools have chosen to incorporate into their Internet use tools that filter access at the desktop or network level and/or monitor access by students into their Internet strategy. School districts such as the New Haven Unified School District in Union City, California offer schools the ability to choose from filters that help limit access to content and access logs that help teachers monitor classroom use to ensure children's safety. Others such as Macomb County, Michigan, have established a countywide Internet filtering solution but allow individual schools to decide whether to employ it.

Voluntary use of blocking and filtering technology.[17] Blocking and filtering technologies offer parents who voluntarily choose to use them an additional method of addressing children's access to information online. While filters may be considered over—or under—inclusive by various individuals and communities, for some parents they offer a useful tool.

Filtering is widely available today. Every family that brings Internet access into the home for children has the option, often at no cost, to filter out information judged inappropriate for children and invite in that which is appropriate according to that family's own values. In the United States, filtering software is readily available to Internet families:

- All (100%) major national Internet/Online services offer filtering at little or no cost.
- Over 14 million Internet connected households have access to filtering capability.
- ISPs serving 85% of all Internet users offer at least one form of filtering software.
- Over 241 local ISPs in over 35 states offer filtering software for free or at nominal cost.
- Several leading PC manufacturers bundle filtering software with their computers.

Blocking and filtering technologies are easy to use and more effectively shield children from inappropriate material than a law. Filtering software is able to keep up with a proliferation of content from millions of Internet sites around the world and across jurisdictional boundaries. Filtering software can block inappropriate material coming from foreign Web sites.

Filtering software is capable of accommodating a diversity of family values and educational needs. As filtering software and services develop, they enable parents to share their children's Internet experiences as appropriate to the particular child's upbringing and maturity level.

- Over 35 different filtering software products, reflecting a diversity of values.
- 3 PICS-based labeling services have rated over 300,000 sites around the world.
- 90% of web browsers have built-in filtering capability using PICS. These browsers are available at no cost to all Internet users.

However, to ensure that the development of filtering technologies moves forward in service of the free flow of information and the protection of children it is crucial that parents be offered:

- easy access to a diversity of market choices;
- information about the criteria employed by the filtering company; and,

[17] The Technology Inventory: A Catalog of Tools that Support Parents' Ability to Choose Online Content Appropriate for their Children, provides an excellent overview of filtering tools. Lorrie Faith Cranor, AT&T Labs-Research, Paul Resnick, The University of Michigan School of Information, and Danielle Gallo, AT&T Labs-Research. http:Hwww.research.att.conVprojects/tech4kids/

• information about the sites, or kind of sites, blocked.

Parents who choose to use these tools will only be able to choose ones that support their values if information about the products is available.

VI. CONCLUSION: WHAT SHOULD CONGRESS DO NOW?

The infirmities of the proposed legislation ought not to lead to the conclusion that there is nothing to be done about the very real problem of Internet speech that is inappropriate for children. While communities across the country are grappling, with this issue, Congress has yet to provide a forum for sustained, substantive dialogue. For this reason, the Subcommittee attention to this issue is particularly welcome. Increased awareness, generated by local communities, advocates, and the activities described above, has encouraged parents around the country to become more involved in their children's use of the Net and spurred the development of voluntary blocking, filtering, and other content selection tools that assist parents in creating a positive experience for their children. Support from Congress would further and speed these important efforts.

This Subcommittee could provide a needed forum for a serious discussion of this important issue. It could begin the process of examining the alternatives available to achieve the goal of protecting children. Can we zone the Internet, and what are the risks of doing to? Should we seek to verify the age of those seeking certain materials, or in doing so will we create new problems? Should we develop easier to access and use resources and tools for parents and communities? What approach will effectively achieve our shared goals? Such an effort, not continuing cycle of hasty legislation and time-consuming litigation, is the process through which we will ultimately make the Internet a safe place for children and realize our most cherished First Amendment values.

Mr. OXLEY. Mr. Douglas, you are on.

STATEMENT OF JEFFREY J. DOUGLAS

Mr. DOUGLAS. I would like to thank the committee and the subcommittee for the opportunity to address the issues arising from the advent of the Internet's capacity as a distribution medium for commercial pornography, with the concern being access by minors.

In preface, let me introduce myself and the trade association I represent. I am a criminal defense attorney in Santa Monica California and the executive director and chair of the board of the Free Speech Coalition, the trade association of the adult entertainment industry. In most ways, we are a traditional trade association except for the products and services we represent.

As the adult entertainment industry's trade association, we have a twofold mission. Our internal mission is to improve the quality of life for the creators, manufacturers, distributors and retailers of adult entertainment product and services. To that extent we have successfully made available all forms of insurance, most notably health insurance, to an entire group of people previously uninsurable; that is, the actors, actresses, dancers and retail employees who work in adult entertainment. We have established health and testing standards, encouraged the transformation of the movie industry in a safer sex, condom only environment, created industry standards performance contracts and compliance forms for 18 USC 2257 to ensure that only consenting adults perform in adult entertainment. Our second mission is to improve the external environment to make the distribution and availability to those adults who desire our products and services, namely through public education, legislative advocacy and, when required, litigation.

Before I address the issues specifically raised by these bills, I want to clarify, especially in light of the testimony that I have seen about to be provided, the actual products and parties whom I speak

for today. The Free Speech Coalition does not represent anything remotely pertaining to child pornography, only products and services by and for adults. Indeed we offer up to $10,000 annually for information leading to the arrest and conviction of producers and distributors of child pornography. Moreover, since violent and nonconsensual pornography is not part of the commercial market, the Free Speech Coalition has no interest in creators and distribution of such product. This material is regulated by the obscenity laws and outside the arena of my remarks.

The apparent primary concern of everyone here today and the specific reason I am before you is to address the means available to prevent minors from having access to adult entertainment on the World Wide Web and Internet without interfering with the ability of consenting adults to do so. Mechanically the solutions that have been offered are simple and have already been employed by the former so-called CDA. That is requiring a credit card as a screening device without necessarily imposing a fee before adult entertainment is made available. We support this. In this manner only, adults can have access to the material.

The reason that we advocate for such a requirement is simple. The Internet providers have no desire for minors to get access to the material on both moral and financial grounds. Since the mechanics are simple, the question then turns to the definition. The bills pending before the subcommittee have taken three different approaches basically. One is to leave it up to local school boards and librarians to define parameters of what is inappropriate for minors. I will not address this. That is outside my area. A second approach is that access providers make available privately developed screening software to its customers. This puts the definitional responsibility where it belongs, on the adults who should exercise control over what their children consume. The last approach involves governmental determination of content and the access restriction for which I am an advocate.

The concept of harmful matter, however, is a particularly unhelpful one. Harmful matter uses the Miller test for obscenity as applied to minors. This is problematic in two ways. It is not discernible by an average or even an extremely sophisticated person what content is contained within the definition of harmful matter. It is a jury question, a complicated question, and as a trial attorney, I can say it is probably the most complicated trial question you can pose before a jury. Second, there needs to be a very different standard for harmful matter depending on whether you are talking about whether it is harmful matter for a 4-year-old, an 8-year-old, a 12-year-old, or a 16-year-old. Unlike the context of a 7-11 or a retail outlet, because the consumer is invisible to the provider, the difference of what harmful matter is between a 16-year-old and a 4-year-old becomes very serious. Far preferable would be to use an objective approach, similar to those used by communities throughout the United States. The phrase specific anatomical areas and specified sexual acts is commonplace in zoning codes in virtually every community in the United States. Provide a list of what cannot be depicted prior to a credit card screening and everyone's legitimate needs are satisfied.

Providers, the people whom I represent, know what it is they can't put up before they screen for minors. That is what is needed. And also it makes it clear what, as spoken by Congress, what is inappropriate.

Mr. OXLEY. Can you summarize?

Mr. DOUGLAS. Yes, thank you. Adult entertainment, as you noted, is an important source of taxes and jobs. The United States, U.S. News and World Report characterized it as an $8 billion giant.

I have provided the subcommittee with written remarks detailing those aspects. There should be no steps adopted by Congress which would restrict the growth of this market. It is a significant source of creativity, employment, taxes and export.

This is one of the very few occasions that an industry representative has been invited to address Congress regarding pending legislation. On behalf of the Free Speech Coalition and those who have worked tirelessly to establish its credibility, I thank you.

[The prepared statement of Jeffrey J. Douglas follows:]

PREPARED STATEMENT OF JEFFREY J. DOUGLAS, EXECUTIVE DIRECTOR, FREE SPEECH COALITION

Thank you for the opportunity to speak to you as a representative of the adult entertainment industry, as this Subcommittee addresses the issues arising from the availability of pornography on the Internet. I am a criminal defense attorney in Santa Monica, California, and the Executive Director of the Free Speech Coalition, the trade association of the adult entertainment industry.

Established in 1991, the trade association has a two-fold mission. First, to improve the quality of life for the people who create, manufacture, distribute and sell sexually oriented products and services. The second part of our mission is to improve the external environment for the products and services through education, advocacy, and media and public relations.

Our membership base is composed of the actors and actresses, dancers, cinematographers, screenwriters, directors, technicians, producers, manufacturers, distributors, retailers, live entertainment clubs, salespeople, internet providers, audiotext providers and mail order companies and their employees. The Coalition has given our members access to affordable health, vision, dental and life insurance, despite the extreme difficulty of getting insurance for individuals employed in and around a sex industry. The Coalition has been responsible for establishing rigorous testing standards for HIV and other communicable diseases. Further, much credit for the conversion of the major manufacturers of prerecorded materials to adopt a "condom-only" policy belongs to the efforts of the Coalition and its officers and members. The Free Speech Coalition has many educational offerings for its membership, including a wide range of health, substance abuse, relationship and life skills counseling, as well as programs on tax planning and other issues related to small business.

The insurance industry regarded the adult entertainment industry with grave suspicion and outright hostility, even beyond health insurance, until very recently. Due to the efforts of the Coalition, production insurance is newly available specifically for "X-rated" productions, instead of specifically excluding such productions, as was the case up until eighteen months ago. And we are on the verge of offering premises liability insurance to our members at prices unavailable, if available at all, through the regular marketplace.

In pursuit of the second part of our mission, the Free Speech Coalition co-sponsored with the Sex Research Center of the California State University, Northridge, in August of this year a World Pornography Conference. An extraordinary event, the Conference drew hundreds of academics, attorneys, treatment professionals from many disciplines and a broad cross-section of the pornography industry from all over the world.

The Free Speech Coalition has been very successful in overcoming many of the popular misconceptions regarding sexually oriented entertainment. Typically people and groups hostile to sexuality deliberately interchange terms such as "pornography," "hard core pornography," "violent pornography," "child pornography" and "obscenity." These terms are legally and otherwise distinct. Through our efforts, the terms of the debate seem to be changing.

Pornography is *not* a legal term. It is defined by dictionaries as material intended to arouse an erotic response in its audience. That means that an enormous amount of matter, including that which has no sexually explicit content, meets the definition of pornographic, especially including much of the output of Madison Avenue.

"Hard core pornography" or "X-rated" or "Triple X" are also not legal terms. They are marketing terms, either pejorative or complimentary, depending on the intention of the speaker. Each term is intended to convey to some degree the proportion of sexual images in the material.

"Violent pornography" refers to either non-commercially produced material, or the non-sexually explicit material turned out in large quantities by "mainstream" Hollywood. Rape scenes, mutilations and non-consensual sex scenes are virtually exclusively the province of the non-X-rated genre. If you want to see a rape scene, you must go to a regular video store like Blockbuster, or watch television. If you patronize an "adult" videostore for such material, you will leave disappointed. For instance, one of the very few categories of sexually explicit material which will be virtually certain to induce an obscenity prosecution is violent or non-consensual material. Thus such material is essentially unknown in the domestic commercial pornography marketplace.

"Child pornography" and "obscenity" refer to materials which are illegal *per se*. Even as harsh a critic of the adult entertainment industry as Jan La Rue of the California Law Center for Family and Children, a self-styled anti-pornography advocacy group, testified before the California Legislature that the modern adult entertainment industry is not involved in the production or distribution of child pornography. Indeed, the Free Speech Coalition, on behalf of the adult entertainment industry, offers a reward of up to $10,000.00 each year for information leading to the arrest and conviction of producers and/or distributors of child pornography.

Part of the goal of the Coalition's educational mission is to remind consumers and legislators alike that pornography is merely another genre of communication. Pornography can contain any kind of representation or content. Just like genres such as science fiction, romance, mystery and the like, pornography can be demeaning or empowering of women (or men); it can be reductivist or intricate; it can be intellectually complex or crudely raw.

The genre of pornography encompasses the politically and socially conscious materials of Femme Productions (often characterized by their creator Candida Royalle as movies to teach men how to make love to women), to the crudity of the large budget, Hollywood star vehicle *Sliver*. Pornography includes materials which are pedantically educational, as well as purely masturbatory. Use of sexually explicit commercial pornography is now part of the mainstream treatment options in marriage counseling and psychotherapy. Femme Productions and many similar lines regularly receive letters of appreciation from traditional practitioners such as psychologists, social workers and marriage counselors, praising these videotapes for their contribution to the improved sex lives of their patients. Additionally, there are explicit materials aimed specifically at non-traditional audiences, such as lines addressing the difficulties of older gay men coming to terms with an unpopular sexual orientation, heavy with storyline and production values. There are explicit stories designed primarily to teach men and women to use condoms and other safer sex techniques. One can no longer make rigid assumptions about the content of sexually explicit materials.

The term pornography or the term "adult entertainment" encompasses so much material as to make the terms more confusing than enlightening. And therein lies much of the danger when it comes to regulation.

The regulation of sexually explicit material is most often motivated by the assumption that such material is either harmful to some segment of the population, or of little or no social value. Both these assumptions are false. As a nation we long ago rejected the notion that materials should be banned based upon the impact such matter might have upon the most vulnerable or easily influenced or traumatized. And for government to engage in censorship practices is violative of the most basic element of the First Amendment.

Let us assume for a moment that most sexually explicit materials were crude, demeaning of the sacred aspects of human sexuality, advocating values inconsistent with the values central to our society, and simply poor quality communication, *but a small percentage were the opposite.* We dare not censor, control or restrict access to all such materials because of the failings of some or even most. Government is uniquely ill-equipped to make determinations as to what is "good" or "high quality" communication. Governmental decisions about communication necessarily will be biased towards non-controversial material. Furthermore, censorship based upon sexual content will necessarily eliminate the material which makes serious social con-

tributions, especially if the audience for that material is outside the perceived social mainstream.

Imagine trying to establish guidelines for restricting access to violent images, based upon the assumption that violent imagery encourages actual violence among violence-prone teenagers and young adults. How would one distinguish, on an objective, principled basis between *Texas Chainsaw Massacre* and *Saving Private Ryan*? Or between *Clockwork Orange* and *Halloween, Part Whatever*? Or between an imaginary movie called *The Sexual Deviants of Nazi Medical Experiments* and a different imaginary movie, a serious documentary called *The Victims of Nazi Medical Experiments*?

And who should make decisions about restricting access to sexually explicit materials targeted for gay or bi-sexual men and women, people of ethnic backgrounds different from that of the dominant culture, survivors of incest or sexual assaults, to say nothing of materials targeted for non-traditional sexual practitioners, or for people who will never engage in any sexual practices other than the most traditional, but who are curious about divergent sexual practices? Who should hold the power of the censor for all of the heterogenous population which we have celebrated for so many generations as representing the diverse strength of this nation?

We must trust the audience, the people, to distinguish between good and the bad. That is the essence of the notion of the marketplace of ideas which underlies the intellectual structure of the First Amendment.

And when the marketplace is consulted, commercial pornography, the product of the adult entertainment industry, is flourishing. Scores of millions of people, if not the majority of Americans, annually consume the products and services of the members of the Free Speech Coalition. No less a conservative journal as *U.S. News and World Report,* hardly a pornography industry apologist, characterized the adult entertainment industry as an eight billion dollar giant, based upon 1995 domestic figures. That puts adult entertainment in the magnitude of the music recording industry.

There is an audience out there. The audience is watching. And the audience is spending. Those eight billion dollars are taxed. Those eight billion dollars generate jobs. Those eight billions are homegrown American products, generating more dollars, jobs and taxes in a burgeoning export trade.

And it is overwhelmingly true that the area of greatest growth and growth potential is the internet. Through the World Wide Web, people can for the first time get access to any kind of sexually oriented materials, aimed at whatever form of subculture, subgenre or fantasy, privately. No video store clerk, not the mail order warehouse employee, not even the postal deliverer need know what a consumer is watching. If a very traditional "straight" woman wants to watch sexually explicit material, straight or gay, it is between her and her conscience. If an openly gay, radical lesbian separatist enjoys seeing on the privacy of her home computer politically incorrect crude heterosexual pornography which would shock her political activist colleagues, so be it.

Moreover, the availability of pornography on the World Wide Web reduces the intrusion of the marketing of sexually explicit materials into the community. The need for "adult" stores or sections of stores is reduced if an alternative source of access is via computer modem or telephone or cable system. This observation should not be distorted or misunderstood to be the basis for arguing that retail adult marketing can be banned or further restricted. It will be a long time in the future before the Internet provides meaningful access for anyone other than an elite segment of the population. Furthermore, retail outlets provide immediate community access to prophylactic devices, marital aids and other materials otherwise available only via mail order, with the attendant delays.

Therefore regulation of sexually explicit materials through the Internet should be aimed at making the most amount of material available to whomever wants the material, but reducing availability to those who do not wish to consume sexually explicit material, and minors.

As the industry's trade association, it is the position of the Free Speech Coalition that the mechanism required under the former Communications Decency Act to screen for minors is effective and appropriate. Prior to the viewer seeing sexually explicit images, the Website should require that a credit card be provided. No charge need be put on the account. By requiring the credit card, the only mechanism by which minors could gain access to sexually explicit imagery is through the consent or negligence of the parents. That is the case now with the other media for sexually explicit materials.

This mechanism also reduces the exposure of persons who do not wish to view the materials. If the patron must take the conscious, affirmative step of entering

a credit card number to enter a site, the likelihood of inadvertent exposure is insignificantly small.

By virtue of this method, the burden is on the provider of sexually explicit materials to screen for minors, and not exclusively on the household. It bears emphasis that there are numerous screening programs available commercially which seek out sites containing content deemed inappropriate for minors. There are difficulties with such software, however.

Screening software, or so-called "nanny" software, necessarily attempts to encompass a wide range of material, based upon key words, and subjective criteria. Although it does no harm to the commercial providers of sexually explicit material, the clientele which I and the Free Speech Coalition represent, there is measurable social cost in overly protective software.

It must be emphasized that the adult entertainment industry is not at all harmed in any way by restrictions on minors gaining access to "adult only" material. The providers of commercial pornography on the Web want to make money. Even apart from deeply held moral concerns involved in inappropriate exposure of minors to sexual materials, fourteen year olds do not provide an income stream for adult websites. The goal for websites is clear rules and simple compliance, as existed in the late C.D.A. By such clear, straightforward provisions, websites can prevent minors from entering, but still have available material suitable for those adults who wish to consume the product.

It also must be emphasized that I am speaking only of commercially produced material. If the material is child pornography, or is obscene, other laws and enforcement mechanisms are already in place. Further regulation by Congress in this arena is unnecessary. The overwhelming majority of pornography available to the consumer is not merely legal, but fully protected by the First Amendment to the Federal Constitution.

The difficulties arise when the definitions of what materials are encompassed by the regulations are vague. Since the question primarily is what materials could be viewed on the "front porch" of a site, prior to screening, Congress could offer a specific laundry list of visual depictions of "specified anatomical areas" and "specified sexual activities" as is typically found in local zoning regulations that attempt to define "adult" retailers.

Because this would not be aimed at restricting the materials behind the "front porch," Constitutional concerns regarding content regulation would be minimal. However, there must be a concurrent tolerance of purely verbal descriptions to inform the intended consumer of what content and services are available on the site. Currently society tolerates substantial violence, nudity and sexual activity through cable services, relying solely upon the responsibility of the adults in the household. No law or practice prevents a fourteen year old from signing up for a premium channel such as HBO, even though such a subscription brings sexual imagery and violence into the home.

No matter what the system employed, materials will reach those persons inappropriate for the materials when irresponsible persons are in charge of the household. Congress should take no action to prevent such aberrations.

Restrictions on funding for libraries and schools must strike the same balance between reducing the inappropriate exposure of sexually oriented materials to minors as well as those who do not to view the materials. Adult patrons of libraries should not be restricted only to information suitable for children. Well beyond explicit sexuality, under HR 3177, libraries must certify that they employ a system which screens out all material inappropriate for minors. I commend the drafters for requiring only such screening for some, but not all Internet access terminals. Especially since there is such enormous differences between what would be suitable sites for four, eight, twelve, and sixteen year old minors, limiting all adult patrons to the sites "suitable for minors" would interfere enormously into the legitimate and fundamental mission of the library in our society.

I thank the Commerce Committee and the Subcommittee on Telecommunications, Trade and Consumer Protection, and the Chair, the Honorable W.J. "Billy" Tauzin, for the opportunity to speak as an industry representative. I am very proud of the accomplishments of the Free Speech Coalition in its few years of operation, but achieving the credibility of being invited to address a committee of the United States House of Representatives is an extraordinary zenith for the organization. Historically the adult entertainment industry has been regulated without any attempt to enter into dialogue with the industry itself I trust that this appearance before this august group of elected representatives of the citizens of the United States of America will be the beginning of a new tradition of dialogue. On behalf of so many creators, distributors and consumers of adult entertainment, I thank you.

Mr. OXLEY. Mr. Alsarraf.

STATEMENT OF LAITH PAUL ALSARRAF

Mr. ALSARRAF. Thank you, Mr. Chairman. You have to excuse me. My name is Laith Paul Alsarraf, and I am the President and CEO and co-founder of Cybernet Ventures Inc. I am very pleased to have this opportunity to testify before this subcommittee on this important issue. Cybernet Ventures was formed about 3 years ago to develop and implement the age verification service known as Adult Check. Adult Check is recognized as the leader of age verification on the Internet and is also the most widely used age verification service. It enjoys a reputation for integrity, independence, reliability, and technological superiority.

As I have stated in the written testimony submitted to this subcommittee, I am here to support H.R. 3783. I am quite certain that there is widespread consensus on the issue of protecting minors from potentially harmful content on the Internet. I am not quite as certain there is unanimity on the solution to the problem. My position, simply put, is that I would rather see an adult pay access, pay to access content rather than a child or a parent the have to pay to restrict it. Of course, the payment should not be a barrier nor should it prevent or inhibit expression of speech.

Currently a 1-year membership to an age verification service, or more commonly known as an AVS, is less than most consumers pay for 1 month of Internet access. AVSs have become widely accepted as one of the most effective ways to limit children's access to harmful materials on the Internet. When this bill becomes law, more Web sites will utilize this service.

Age verification services generally and Adult Check specifically use passive restriction technology. They require no programming, technical expertise or involvement by parents and require minimal technical expertise of Web site owners in order to implement it. AVS prevents minors from accessing material that may be harmful right at the source. Sites containing material that may be considered harmful would only be able to be accessed by providing a personal identification number. This personal identification number would be issued by an AVS, once it has been verified that the applicant is an adult.

This bill will provide to parents a degree of assurance that their children can surf the net without fear that they will be exposed to harmful or indecent materials. It represents a balanced yet effective approach in our efforts to solve this growing international problem. At Adult Check, we feel strongly that this bill will address parents' concerns about the Net providing children continued access to the largest library in the world. We urge you to pass H.R. 3783 this legislative session.

I would also like to address an issue brought up by Congressman White and Congressman Cox regarding zoning. I have heard zoning. And on its face value, it appears to have some merit, but when you look a little bit deeper into it, it gets a little more difficult, both technologically and practically. On the technological side of it, and I don't purport to be an expert in domain named technology, I do know enough to know that it would be a difficult transition and a separate organization would have to be created to handle a world-

wide extension, which does not exist right now. So transition over to this would be slow at best. On a practical level, it appears to me that you would still need international treaties to force international adult sites to transfer over the dot XXX domain. When we have right now is a service that is being used, our service alone protects close to 29,000 Web sites out there. If we take Congressman Istook's numbers of 100,000 adult sites, that may be conservative, I have heard anywhere from 70 to 120,000, that is a fairly large part of the market and it has been purely on a voluntary basis. There are over 30 other age verification services out there.

What our service does is it places the onus on the Web site, but it does not place a huge burden on them. It is simple to implement. If a person has the expertise to develop a Web site, they can very easily implement an age verification system on that Web site. It is free for them to use and there are incentives as well. It does not involve, I have heard a lot about placing the responsibility on the parents, and that sounds great, but practically we know that parents don't have the time to sit and monitor the child's activities and more often than not the child is more technically savvy than the parent. And that creates a problem. Our service or services like ours require no input from the parents whatsoever. It happens right at the Web site and the parent does not have to spend any money to protect their children.

Mr. OXLEY. Could you summarize?

Mr. ALSARRAF. We have a technology that if we combine this with the bill to give it its effectiveness and the filtering software on the other end, we have technology that exists, that is effective, that is accepted out there and I feel that is the best solution.

[The prepared statement of Laith Paul Alsarraf follows:]

PREPARED STATEMENT OF LAITH PAUL ALSARRAF, PRESIDENT AND CEO, CYBERNET VENTURES, INC.

INTRODUCTION

On behalf of Cybernet Ventures, Inc. I am pleased to have this opportunity to testify before the Subcommittee on Telecommunications, Trade and Consumer Protection. My name is Laith Alsarraf and I am the President, Chief Executive Officer and co-founder of Cybernet Ventures, Inc. By way of background and history, I was born in Ontario Canada in 1969. Both of my parents are doctors and following in the family tradition, I attended UCLA as a premed student. While in college, I also worked as a contract programmer and website designer. The success of these computer oriented ventures pushed my formal education to the sidelines and I formed a company that soon required my full time attention. I now have seven separate corporations each providing technology and development services in a wide variety of areas including an advanced e-commerce package called Power Charge, an internet service provider and a specialized internet marketing group. Our flagship company is Cybernet Ventures, Inc. which provides the age verification service AdultCheck™.

In 1996 the Congress of the United States passed into law the Telecommunications Reform Act ("TRA") which among other things addressed certain issues dealing with access to the internet by minors. The portion of the TRA, which dealt with internet content and access, was the Communications Decency Act ("CDA"). The original CDA created a 'safe harbor' from prosecution for those websites that provide content that might be considered indecent or harmful to minors provided that those websites took reasonable steps to prevent access by minors. In response to the first CDA, Cybernet Ventures, Inc. was formed to provide age verification services ("avs") to websites, which provide content that may be harmful to minors. Cybernet Ventures, Inc. provides avs through AdultCheck.™ Since its inception, Cybernet Ventures, Inc. has experienced unprecedented growth and success, and the

AdultCheck™ age verification service is, by a significant margin, the largest and most widely used avs.

Although portions of the original CDA were subsequently held unconstitutional, the need for protections for minors from accessing content on the internet that may be harmful or indecent is a recurring theme. Specifically, I am here to comment and testify in support of H.R. 3783.

AGE VERIFICATION SERVICES

Age verification software is a script embedded into a webpage which can be implemented by a website owner in minutes. This script is placed at the entrance(s) of a website which may contain material harmful to minors preventing further access or exposure of the website's content by requiring a personal identification number ("PIN"), which is only available to adults. If a consumer does not have a PIN, a link is provided for them to obtain one from the avs associated with that site. Consumers may obtain a PIN instantly by submitting an application to an age verification system. The credit card and other information submitted by a consumer are verified by a proprietary age verification system to determine its validity. If the information is deemed to be valid a working PIN is issued. The process of verifying the information submitted generally takes from 5 to 10 seconds.

Cybernet Ventures, Inc. does not sponsor or display any content. The services provided by Cybernet Ventures, Inc. are limited to age verification and the assignment of personal identification numbers ("PIN"). A consumer applies for a PIN online or by fax. The application is submitted and processed through a proprietary software system that determines the validity of the credit card. The software program is designed to also provide fraud and chargeback control. Once approved, the consumer can use his (or her) PIN to access tens of thousands of websites. The website is assured that any visitor has been 'age verified' by AdultCheck™. The consumer is charged $16.95 for a one year 'membership.'

An avs is not completely foolproof. The two most common criticisms are: 1) once a PIN is issued it can be shared with thousands of potential users, many of whom may be minors by posting it on the internet; and 2) minors have access to credit cards, some with their parents permission, some without.

Cybernet Ventures, Inc. has already developed several proprietary methods to detect password sharing. Velocity checks, relational database management, originating IP address verification and other fraud controls have been designed and are constantly being improved. PINs that have been distributed and are being used by multiple individuals are invalidated within minutes by Cybernet Ventures' proprietary PIN protection software. Significant resources have been and will be dedicated to maintain, develop and implement more effective technologies and to develop new and better methods to prevent fraudulent use of PINs.

Of course a small number of minors will have access to credit card numbers. Some of these minors may have access to their parents' credit cards legitimately; some not. Others may have gotten credit card numbers off of the internet. Because AdultCheck™ does not provide any content, the credit card descriptor is not masked or its meaning obscured by euphemisms, pseudonyms or misleading company names. A minor who obtains a PIN without his or her parents' permission, will only have it for a maximum of thirty days. The illicit transaction will appear on the parents' credit card statement within the current billing cycle and the parents can ascertain the nature of the transaction and question their child as to the circumstances of it. AdultCheck™ provides a high level of customer service accessible via a toll free telephone number or e-mail 24 hours a day, 7 days a week. If a parent contacts AdultCheck™ concerning an unauthorized use of their credit card, a credit is issued to their account, the password is invalidated and the card number is blocked.

Stolen credit cards, bogus card numbers, numbers posted on the internet and other fraudulent credit card transactions are detected by the use of several systems. Each transaction is authorized or declined first by the credit card company (e.g. VISA®, Mastercard®, and American Express®). Even if the credit card is first determined to be valid, it is still subjected to several other checks to determine the validity of the particular transaction. These other checks are proprietary and the systems and programs are protected trade secrets. All of these efforts are brought to bear on the issue of validity to protect consumers and prevent unauthorized use of credit cards. Most importantly, every effort is made to prevent minors from accessing websites that contain content that may not be suitable for them.

Despite our best efforts, no system is perfect and I would not be so presumptuous to claim that avs is 100% foolproof. Other bills are being considered by this subcommittee that specifically mandate filtering software. Filtering software works dif-

ferently than an age verification service and provides a different approach to addressing the issue of minors accessing unsuitable content on the internet. Although my experience and expertise are in the avs arena, I am very familiar with filtering software and its technology. I will defer to those who have been asked to testify on behalf of that industry, however, I must emphatically state that the two technologies are not mutually exclusive and, more importantly, together they can help to form a more effective line of defense to protect children.

As I am certain each of you is aware, the main difference between an avs and filtering software is that an avs stops access at the source, and requires no parental technical expertise or involvement. Unlike filtering software, avs does not place a financial burden on parents who simply wish to restrict access by their children to material that may be harmful. A website restricts access to only those whose age of majority has been verified. Otherwise, an avs is content neutral. Filtering software provides parents a greater opportunity to counsel their children and to screen out content based on words and phrases. Avs prevents access to sites by minors while allowing the internet to be free of prior pattern recognition restraints. By requiring an avs the burden of compliance is placed at the source of the material, the website.

Currently AdultCheck™ is used by a significant percentage of adult content websites on the internet. In addition, AdultCheck™ is also used to restrict access to numerous sites that contain non-sexual content that may also be considered harmful to or inappropriate for minors. Even though the CDA was overturned, most website owners continue to use avs as a responsible approach to content accessibility and AdultCheck™ is free to websites. Avs has been widely accepted among websites owners and consumers because of its effectiveness, ease of implementation and use, and its nominal cost. The consumer pays a nominal fee of $16.95 for access to over 28,000 websites for a year and the website owner pays nothing.

From a consumer standpoint, an avs is superior to direct credit card verification at each site. Because of AdultCheck™ reputation for being responsible, independent and easy to use, consumers have confidence in providing credit card information to us. In addition, AdultCheck™ has no interest in the consumer beyond the service of age verification. We do not contact them, sell them additional services or trade in consumer information. The credit card information is strictly confidential and is not shared, sold or disseminated.

CONCLUSION

Age verification services provide an effective, content neutral method to protect minors from accessing harmful or indecent materials on the internet. An avs, using current technology and credit card merchant banking, allows a free flow of ideas and constitutionally protected speech to course through the internet without censorship and unreasonable intrusion. Although not completely foolproof, the current technology has procedural safeguards to reasonably accomplish the intended goal of protecting children without an overly broad or over-reaching approach. An avs is the least restrictive, least intrusive method of restricting access to content that requires minimal parental technical expertise and intervention. An avs does not judge content, does not inhibit free speech, does not prevent access to any ideas, word, thoughts or expressions. An avs prevents minors from accessing materials not suitable and potentially harmful.

Mr. OXLEY. Dr. Layden?

STATEMENT OF MARY ANNE LAYDEN

Ms. LAYDEN. I would like to give you some examples of the kind of psychological impact this kind of material can have. I am going to give you one example of a patient that I treated, Cathy, who was about 8 years old, when she first came in contact with this kind of material and her brother Frankie, who was about 12. It was at that point that Frankie began to insist on having sex with his sister. Frankie's father thought that he had hidden the pornographic magazines that he had in the home, but Frankie had found them and soon Frankie began to add his own pornographic magazines to the mix. He quickly had a mountain of pornography under his bed. The pornography that Frankie viewed gave him misinformation about sexuality and gave him a pathological view of intimacy. That

pornography told him what females look like, what females do, and the sexual behavior that is acceptable for males. He began his descent into what are called permission giving beliefs, which are the common factors between all the different sexual pathologies and sexual violence. He believed, and this is from Frankie's point of view, that women's bodies were pieces of sexual meat to be consumed for male entertainment.

The pornography that he saw was also hate speech against men. Pornography spreads the myth that male sexuality is visually narcissistic, predatory and out of control. This myth Frankie came to believe. Pornography distortion had begun.

Every night Cathy would get into her bed, roll herself into a fetal position and every night Frankie would come in and peel her open. The demands for sex continued until Cathy was 18 years old. After this experience, Cathy could have gone on to work in the sex industry as a stripper or a prostitute, a Playboy model or a porn video actress. Many people who have been sexually abused do that. The physical invasion and the visual invasion of their bodies that children experience are often reenacted in adult life. The customers now play the role of the perpetrators. These women work in the sex industry because it feels like home. Research indicates that between 60 and 80 percent of the individuals who work in the sex industry are adult survivors of childhood sexual abuse. They work in terrible jobs like stripping and about 40 percent of those strippers are substance abusers, typically cocaine or alcohol; 40 percent are also experiencing multiple personality disorder and are disassociated when they are stripping. Psychologically they are not present during the act. Sixty percent of those individuals become depressed. These numbers are enormous.

Cathy did not take that route. She became a nun and at the age of 40 went into therapy. Frankie went on in his adult life to what is too typical of sex and pornography addicted teens and became an adult sex addict. He married but he continued to act out sexually. His wife would throw away a mountain of pornography each week and each week he would buy more. He sexually and emotionally abused her until she divorced him. His daughters will not talk about what their life with him was like, but they will not have any contact with him either.

He destroyed his career, due to his sexual addiction. He financed his addiction with money that he stole or embezzled. He wheedled money from his mother while she was alive and then misappropriated funds from the estate once she was dead.

Research on adult sexual addiction indicates that there are an enormous host of problems that addicts can anticipate but often the addict does not. Denial is a large part of this problem. Approximately 40 percent of adult sex addicted males will lose their spouse. Severe financial consequences will be suffered by 58 percent of the addicts, some of them losing all or some of their savings and earnings. About 27 percent will lose their jobs or be demoted. Among professionals that are sex addicted, about 40 percent of them will lose their professional careers because of their sexual acting out. High risk sex is frequent among this group. Sexually transmitted diseases range from those who are treatable to those that are deadly. The risk of contacting a disease is compounded by

the risk of transmission. Family lives are disrupted, sometimes there is abandonment of wife and children, arrest is a potential, substance abuse is common. Even suicide is not infrequent. Sex and pornography addiction has become so widespread that in the Philadelphia area alone there are now 80 AA-type 12-step addiction groups for sex and pornography addiction.

There are many, many problems that occur in adults once they have been exposed to this material as children. The limitation of this material is actually vital and the pornographers who spread the material seem to be for the most part willing to reach down and damage our children and reach up and damage the highest members of our society. I think that we need to start by saying this material needs to be controlled, that the pornographers feed on our passivity and our silence, and they need to know that they will not have the comfort of our silence anymore.

[The prepared statement of Mary Anne Layden follows:]

PREPARED STATEMENT OF MARY ANNE LAYDEN, CENTER FOR COGNITIVE THERAPY, DEPARTMENT OF PSYCHIATRY, UNIVERSITY OF PENNSYLVANIA

Thank you, Congressmen, for allowing me to speak to you today.

Congressmen, I would like to tell you a story. I wish I could tell you a lovely story, something that would go with a Norman Rockwell print. But the story I have to tell you is about a terrible thing that has happen. A sad, horrible all too common thing that has happened.

It is a story about a little girl named Cathy and her brother, Frankie. They grew up in a small frame house painted blue in a large midwestern city. Cathy was about 8 when the terrible thing started. Frankie was 12 the first time he asked his sister to have sex with him. Their father thought he had hidden his pornographic magazines well but Frankie found them. Soon he began to buy his own and he quickly had a mountain of magazines under his bed.

The pornography that Frankie viewed as a child mis-educated him about sexuality and gave him a pathological view of intimacy. They told him what females look like, what females do, what sexual behavior is acceptable for males. He began his descent into the permission giving beliefs that are the common factor in different sexual pathologies and sexual violence. He believed that women's bodies were pieces of sexual meat to be consumed for male entertainment.

Pornography is also hate speech about men. Pornography spreads the myth that male sexuality is viciously narcissistic, predatory and out of control. Frankie believed that. Pornography distortion had begun.

Cathy loved her brother but she was also afraid of him. She wanted to please him and she also hated him. Every night she would get into her bed and roll herself into a fetal position and every night he came in and peeled her open. The demands for sex continued until Cathy was 18 years old. After this experience, Cathy could have gone on to work in the sex industry as a stripper or a prostitute, a Playboy model or a porn video actress. Many do. The physical invasion and the visual invasion of their bodies that children experience are often reenacted in adult life. The customers now play the role of the perpetrator. These women work in the sex industry because it feels like home.

Research indicates that 60-80% of sex industry workers are sexual abuse survivors. To work in a terrible job like stripping, 40% abuse substances such as cocaine or alcohol.

Thirty-five percent of strippers have Multiple Personality Disorder and dissociate. Psychologically, they are not present when they are stripping. Is it any wonder that 60% suffer from depression? These numbers are enormous.

Cathy didn't take this route. Instead, Cathy became a nun and at 40 she went into therapy.

Frankie went on to an adult life that is all too typical of sex and pornography addicted teens. He became a sex and pornography addicted adult. He married but continued to act out sexually. His wife threw away a mountain of porn each week. He bought more. He sexually and emotionally abused her until she divorced him. His daughters will not talk about their life with him but they will not have any contact with him either. He destroyed his career due to his sexual addiction. He financed his addiction by money he stole or embezzled. He wheedled money from his

mother when she was still alive and misappropriated money from her estate after her death. He spent time in jail.

Research on the adult sex addict indicates that there are an enormous host of problems that could be anticipated. Often the addict anticipates few of the outcomes. Denial is a large part of the problem. Approximately 40% of sex addicted males will lose their spouse. Severe financial consequences will be suffered by about 58% with some addicts losing all of their savings and earnings. In general, about 27% will either lose their jobs or be demoted. Among professionals who are sex addicted, as many as 40% will lose their professions due to their sexual acting out. High-risk sex is frequent among this group. Sexually transmitted diseases range from those diseases that are readily treatable to those that are deadly. The risk of contracting a disease is compounded by the risk of transmission to others.

Family lives are frequently disrupted. Sometimes there is abandonment of the wife, and children; sometimes there is severe friction even if the family physically stays intact. Arrest is always a threat and this also destabilizes the family. Substance abuse is common with alcohol marijuana and cocaine being the most frequent drugs of choice of the sex addict. Suicide is not infrequent. The consequences and the pain caused by this disorder are severe and yet the addict does not stop. This is an indication of the strength of the pull. The life of the sex addict is filled with pain and shame as the downward spiral takes hold.

Sex and pornography addiction has become such a wide spread problem that, in the Philadelphia area alone, there are now 80 AA-type 12-step groups for sex and pornography addiction. This addiction has some similar dynamics to other addictions. Tolerance develops with more and harder kinds needed to satisfy. Withdrawal symptoms arise with discontinued use. Dishonesty and out of control behavior characterize the secret life.

But this addiction does have some differences. Most traditional addiction treatment starts with detoxification to remove the addictive substance (cocaine, alcohol etc.) from the body. Sex addiction from pornography produces mental imagery that is permanently implanted in the mind of the user and is sealed in by brain chemistry reinforced by the orgasm. These images can be called up in an instant forever. This is the first addictive substance for which there is no hope for detoxification. In my clinical practice I have found this addiction to be less likely to remit than cocaine addiction and more likely to relapse.

Studies have found significant changes in beliefs when subjects have been shown pornography. These belief changes are mental distortions that we call pornography distortion. They come to believe that unusual sexual behaviors, even psychiatrically disordered sexual behaviors, are more common and usual. They come to think of Is common and usual behaviors such as having sex with animals, mixing sex with violence, paying for sex, or having sex in a group. They become more accepting of behaviors that are damaging to others. For example, they reduce their belief that pornography needs to be restricted from children. Showing children pornography is sexual abuse. Seeing pornography makes this form of sexual seem more acceptable.

They become less negative in their attitudes toward rape and believe that rapists should receive lighter prison sentences. In studies in which college males were shown pornography, 50-65% of them then said they would be willing to rape a woman if they thought they wouldn't get caught. College age males who have committed acquaintance rape are more likely to be frequent readers of sex magazines like Playboy and Hustler. The more sex magazines sold within a state the higher the rape rate in that state.

For the last 13 years, I have specialized in the treatment of sexual violence victims and perpetrators. I have treated rapists and rape victims, sexual harassers and sexual harassment victims, incest survivors and pedophiles, prostitutes, strippers, and pornography and sex addicts. In 13 years, I have not treated one case of sexual violence that did not include pornography as a substantial factor. In every case of sibling incest that I have treated, the pornography was nonviolent sex magazines like Playboy, Penthouse, and Hustler, etc.

The kinds of problems I treat are occurring at epidemic, tsunami levels. Among the industrialized nations, we are the most sexually violent nation on the face of the earth. One in eight women are raped; 50% of women are sexually harassed on their jobs in their lifetime. By the time a female in this country is eighteen years old, 38% have been sexually molested. We are in the midst of a sexual holocaust.

I'm happy to report that Cathy is doing well, leading a rich and satisfying life. Regrettably, Frankie is still in denial and despite that has happened to him says that pornography and sexual dysfunction have not caused any problems in his life. In order for Frankie to heal, he must begin by admitting he has a problem and asking for help.

I have seen the terrible damage that sexual addiction can cause. This problem has reached down to damage our children and reached up to the highest levels of society.

Pornography is one of the toxins that spreads this disease and children are the most vulnerable to its infection. However, the toxic impact of pornography distortion effects adults as well. These adults become carriers back into their homes, into their jobs, onto the streets, into the schoolyard.

In order for these terrible things to happen, pornographers depend upon our ignorance and passivity. The pornographers feed on our silence. But silence is complicity. We must all send a clear and strong message to those who would hurt our children with pornography. We must tell them that they will never have the comfort of our silence again.

Mr. OXLEY. Mr. Lessig.

STATEMENT OF LAWRENCE LESSIG

Mr. LESSIG. Thank you. In my written submission, I have addressed three bills that now are before you. H.R. 774, H.R. 3177, and H.R. 3783. H.R. 774, I don't see any constitutional question, and H.R. 3177, I believe you should consider unconstitutional. But I would like to focus my remarks on 3783, the Child On-line Protection Act.

I am a law professor, I teach constitutional law and the law of cyberspace. I cannot help myself. I want to start with two hypotheticals if it is okay. It is clearly, case 1, it is clearly constitutional in real space, that space we are right now in, for the States to pass a law that said, sellers of harmful material must check the age of people before they sell that material to the people. This is a statute, as Justice O'Connor pointed out in her concurring opinion in Reno, which exists in many States and which has clearly been upheld in many State courts, and in Ginsberg the Supreme Court upheld something similar to that.

Case two, it is obviously unconstitutional if a State were to pass a statute that said, before you can sell matter that is harmful to minors you must take an imprint of a credit card so that the purchaser can get access to that material. It is because of case 1 that something like H.R. 3783 strikes me as potentially constitutional. This is exactly what Justice O'Connor was speaking of when she spoke of zoning, not zoning in the Triple X dominion sense but zoning in just the way that Adult Check zones. It is an attempt to create a technological device that helps separate people based on age.

But it is because of case number 2, the case where in real space we take a credit card imprint before we allow people access to speech that they have a constitutional right to, that I would argue I am not sure that H.R. 3783 is yet a bill you should consider constitutional. And the reason is the mode of identification that the bill envisions to distinguish between those who have a right to speech and those that don't. The type of identification that the bill speaks of is essential, too. The one type, the adult verification system which has been spoken of, Adult Check, is a perfect example of that, essentially creates a password system and, as the Supreme Court discussed in Reno, the burden of requiring multiple passwords to get access to this type of speech can be quite significant. That was their concern in Reno about the password system. The credit card is an alternative to the password system also spoken of in this.

There are many people who are obsessed with their fear of putting credit cards on the Internet. I think they are exaggerating things. But, Mr. Chairman, I think the last people in the world that we should require individuals to turn their credit card numbers over to before they get access to speech that is protected are on-line pornographers.

Because, Mr. Chairman, many of these online pornographers are not the sort of people that we should force people to turn their credit card numbers over to to get access to this type of speech. We have just begun to study some of the contracts that they bind people with when they use their credit card numbers to get access, and these are not the types of contracts that are just about making sure that people are adults. These are contracts for bringing people into this online sale of pornography and keeping them there.

Now, if these were the only ways to separate out adults from kids, it might be that the statute would be constitutional, but the point is that it is not. The point is that the architectures of cyberspace are changing so rapidly now that we can see in the future the development of a kind of architecture that would facilitate the identification of adults separate from kids without revealing identity and without the cumbersome nature of password systems. These digital certificate systems hold the promise of being a type of technology that could achieve the objectives that we are discussing today without any of the burden on privacy and anonymity and without any of the potential abuse that the credit card concerns raise.

My concern with the statute is that if you act too soon and entrench a particular technology which is not effective and violates what the Supreme Court identifies as a significant interest, the right to anonymity, you could distort the market and the development of this alternative. And rather than entrenching this inferior technology now by your acting in this bill, this committee should take steps to push these alternatives; and I support Mr. Berman when he suggested that the best way to do it is for this committee to put attention on the development of these alternatives which simultaneously achieve your objective of separating kids from adults while preserving the interests of adults who have a right to get access to this without turning over their financial records to people that you would not want to speak to even in real space.

Thank you very much.

[The prepared statement of Lawrence Lessig follows:]

PREPARED STATEMENT OF LAWRENCE LESSIG, PROFESSOR, HARVARD LAW SCHOOL.

I have reviewed the three legislative proposals presently before this Committee to address the concern about a minor's access to "harmful material" over the Internet. They each present different constitutional and policy questions, and I consider some of those questions in the few pages that follow. In my view, they all represent a careful attempt to deal with what many perceive to be a serious social problem. They each approach the issue in a slightly different way, and they are all more respectful of our free speech tradition than was the Communications Decency Act of 1996.[1]

In my view, however—and even for those who believe most strongly that Congress should act to protect children in this context—it would be a mistake to enact this legislation just now. The architectures of the Internet are changing at a dramatic

[1] 110 Stat. 56.

pace, and, as I explain more carefully below, if Congress were to act now, it would risk entrenching a less efficient or effective technology for dealing with the problem that it seeks to address. Acting now, in other words, risks defeating the very objective that these proposals seek to achieve—namely effective parental control over the material to which their children are exposed.

My argument is not that Congress should do nothing. There are serious questions about the nature of this problem that Congress should, through hearings, seek to resolve. This is an appropriate role for Congress in the midst of the present revolution. But until we know more about how the Internet will develop, we should not pass laws that entrench technologies that may, in a very short time, no longer be necessary or effective.

H.R. 3783—Child Online Protection Act

This proposal is a careful response to the Supreme Court's decision in *Reno v. ACLU*[2] Unlike the Communications Decency Act of 1996, the bill is targeted at commercial speech that is "harmful to minors." The pedigree for state regulation of such speech is well established.[3] As Justice O'Connor indicated in her concurring opinion in Reno, many states rely upon very similar language to regulate the display and distribution of adult material.[4] In light of this authority, my view is that this bill could well be judged constitutional.

There are, however, a number of technical problems with the bill that do raise significant constitutional questions. There is as well a more fundamental problem that in my view makes this legislation unadvisable at the present time. I consider the second point first.

The essence of the bill is a proscription against the distribution to minors of matter that is "harmful to minors," tied to a defense for sites that screen access using a number of adult identification systems, or proxies for adult identification systems (such as credit cards.) The basic structure is zoning, and the constitutionality of such zoning depends upon minimizing the burden that the regulation imposes upon those who have a constitutional right to the speech at issue.[5]

In their present form, however, adult identification systems are significantly burdensome. This burden has three dimensions. First, they all are essentially password systems that are cumbersome to use and relatively expensive to maintain. This feature was most important to the Court in *Reno*. As an adult "surfs" through adult sites, he or she is potentially forced to present a series of different "IDs" to gain access to constitutionally protected speech.

Second, these systems interfere with an individual's ability to access adult material anonymously. All the systems identified in the proposal tie age verification to the identity of an individual, meaning that they all, to some degree, require that individuals give their name as a condition to getting access to constitutionally protected speech. But there is no way that an individual can know how that information will be used by the site, or by an ID company. And the temptation for such organizations subsequently to sell the names of individuals to email spam organizations, or others, is great.

Third, the most common form of identification—the credit card-creates a related and significant risk of abuse itself. Often a site will promise that credit card information will be used only for identification purposes. But because it is so easy for the consumer to lose control over credit card information in cyberspace, the consumer faces a risk that the data he or she provides so as to get access to a site will be used improperly later on. (I have heard of one site, for example, that promises to charge a credit card just $1 to access an adult material, but in the fine print of the agreement, the site claims the right to charge the user $20 a month if the user does not cancel the subscription after 72 hours, and further threatens that canceling at the appointed time is the only way to cancel a subscription.)

If these architectures of identification were the only possible way in which the government's interest in zoning "harmful material" from kids could be accomplished, then these burdens might be permissible under the Court's test in *Reno*.[6] But they are not the only feasible technologies. One alternative—which would be less burdensome to the user, and which could assure anonymity and avoid the risks that credit

[2] 117 S.Ct. 9329 (1997).
[3] Its source is *Ginsberg v. New York*, 390 U.S. 629 (1968).
[4] 117 S.Ct., at 2352 (O'Connor, concurring).
[5] Id., at 2353.
[6] See Eugene Volokh, *Freedom of Speech, Shielding Children, and Transcending Balancing*, 1998 Sup. Ct. Rev. 31, 38-39 (1998).

cards present—would be digital certificate technologies.[7] With such certificates, one in principle could certify one's age without revealing other facts—such as one's name, or credit information—and this certification could be done invisibly, or automatically, when a browser connected with a given site.

The digital certificate industry, however, is just in its infancy. The market is still groping for a model for certificates, and it is unclear now which form makes most sense. At this stage, for Congress to push an outdated identification technology could significantly interfere with the development of these preferable and more protective alternatives. Only when these technologies have matured can Congress make a sensible judgment about the kinds of identification it can, and should, require.

In addition to this general problem with the proposal, there are a number of more specific concerns as well.

- §(e)(1), in §(3) of the proposal, extends the proscription to those "in the business of selling *or transferring*... material that is harmful to minors." It is unclear who is included by the term "transferring." One could well read the proposal to reach any Internet Service Provider that helped facilitate the transfer of such material, whether or not that ISP made such business its primary concern.
- §(e)(2),(3) are both criminal provisions, one directed against those who intentionally violate the proscription paragraph, and the other against those who simply "violate[]" the proscription paragraph. In my view, a criminal penalty in this context creates too great a chill on legitimate speakers. At most the statute should provide a civil remedy.
- §(e)(7)(A) defines the "World Wide Web" to include "hypertext transfer protocol, file transfer protocol, or other similar protocols." It is unclear how far the clause "other similar protocols" is intended to reach. USENET, for example, is a set of protocols for exchanging messages in a public fashion. Its protocols don't now include a way to authenticate on the basis of age.[8] The bill should be clarified to specify how far it is intended to reach.
- §(e)(7)(D) defines "harmful to minors" by a modified statement of the *Ginsberg* test—modified in light of *Miller* v. *California*.[9] But the test as modified does not take account of community standards in setting the test of "harmful," as the standard for obscenity does.[10]
- §3(b) requires that the FCC post "information as is necessary to inform the public of the meaning of the term... harmful to minors." But in light of the Supreme Court's decision in *Bantam Books* v. *Sullivan*,[11] it is clear that the FCC's power here is quite limited. The statute should specify more clearly ' just what kind of information it intends the FCC to post, and indicate clearly that these postings are not to become the equivalent of a "blacklist" of material.

H.R. 3177—Safe Schools Internet Act of 1998

This proposal requires, as a condition of receiving federal funding, that "elementary or secondary school[s and] librar[ies]" certify that they have a "system" to "filter or block matter deemed to be inappropriate for minors." "Inappropriate" is to be determined, under the bill, by local school or library officials, and the bill would not allow the judgment of these local officials to be second-guessed by any agency of the federal government. Presumably, so long as the local officials have made a selection, certification would be assured.

The problem with this proposal, however, is similar to the problem with H.R. 3783. For the bill seems to presume that technology exists that would allow local officials to make subtle choices about the kinds of material the software will filter. But in fact, the technology of filtering is not now so well developed. Given the present array of blocking and filtering software, the local official in effect would be forced to delegate this decision about the kinds of material to be blocked to software companies that are now independently marketing the material to parents.

This technologically forced delegation raises significant constitutional concerns. For the scope of material that is presently blocked by blocking software typically extends far beyond the speech that governments can constitutionally restrict. The speech blocked by such programs reaches far beyond the narrow scope of "harmful to minors," and, in some cases, well beyond the reach of the Communications De-

[7] See the description in A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 Or. L. Rev. 49 (1996).

[8] Though there are proposals that the protocol be changed to enable such authentication. See Stan Barber, *Internet Draft, Network News Transfer Protocol* (March 1998), available at ftp://ftp.ietf.org/internet-drafts/draft-igtf-nntpext-base-04.txt.

[9] 413 U.S. 15 (1973).

[10] Id.

[11] 372 U.S. 58 (1963).

cency Act of 1996. Congress would then be indirectly forcing (through the spending power) local governments to impose conditions on speech access inconsistent with First Amendment principles.[12]

Once again, the better solution would be to allow the technologies of filtering to develop, before Congress in effect mandates their use. There is a wide range of new technologies for rating and filtering speech now being developed in the market. Congress again would be better advised to let those technologies mature before pushing localities to use them.

H.R. 774—Internet Freedom and Child Protection Act of 1997

This proposal would require "access providers" to offer—either for a fee or at no charge—"screening software that is designed to permit the customer to limit access to material that is unsuitable for children." In my view, there is nothing constitutionally troubling about this provision, though I can't see what problem it is meant to solve.

There are many kinds of access providers—some focused on families, others on business. Presumably, these providers have a sufficient incentive to provide services that their customers demand. To satisfy the requirements of this bill, all providers would have to provide child protection software—whether the customer was Citibank or the family next door. But it not clear what advantage is gained by giving Citibank the option to buy child protection software, and it is unclear why a family access provider won't do so on its own.

Indeed, the major access providers already comply with the requirements of this bill. America Online has an extensive system of protection that it offers its customers; presumably, any other access provider could comply by simply providing a link on its web page to vendors that sold child protection software. Given the ease with which suppliers now meet market demand, it is uncertain what positive function the regulation would have.

Mr. OXLEY. Thank you.

Mr. Nickerson.

STATEMENT OF PETER NICKERSON

Mr. NICKERSON. Thank you, Mr. Chairman.

N2H2 provides server-based Internet filtering to about 8,000 schools around the United States. We also provide filtering to about 200 Internet service providers. We provide filtering overseas to businesses and some libraries. Those are our principal markets.

In some States, including your own State, we filter about 50 percent of the access made by children in schools. We are at the end of this month going to start filtering Department of Defense schools in Europe. We have a very broad base in terms of what we are doing, how we are doing filtering. It is widely accepted.

What I want to do is run through quickly to explain to the committee the changes that have occurred over time in filtering and what we see on the horizon and then touch on a few of the issues which have been brought up in this hearing.

We are now providing filtering on a server-based level which is much different than what most committee members are aware of. We put a server on a school district site, and there are 32 servers in the State of Ohio in various locations. Those school networks, which may be individual schools, they may be school districts, in the State of Ohio they happen to be multiple districts, send all of their Internet traffic through this filtering servers.

Children make a request. The request goes through the filtering server, and it is checked to see if it is okay. If it is not okay, it goes

[12] Given the Supreme Court's standard of review in spending clause cases, see, e.g., *South Dakota* v. *Dole*, 483 U.S. 203 (1987), my claim is not that this provision would necessarily be struck by the Court. But Congress has an independent duty to consider constitutional norms in the spending clause context, and these norms of federalism should be more robust than those considered by the Supreme Court.

out and gets it; and if it is not okay, it tells them to go someplace else.

We now have about a hundred million web pages per month going through our servers around the country. And so one thing I think the committee needs to know is that schools are using the Internet, and the growth is significant. During the school year last year we saw 15 percent growth per month on the use of the Internet, and so it was substantial.

There is a general perception out there that Internet filtering technology is seriously flawed. I think a lot of that comes from early programs that use keyword blocking to block anything that is on the Internet that has a particular word. The Middlesex example that you used earlier is a good example of that.

Those technologies have changed a lot. I want to run through and give you the sorts of features that are on our systems now. All of the filtering is customizable. We designed our systems to be usable based on a community's own standards. So when we install a server on a location, the administrators in that community go and pick among categories that they want to block, and they are able to unblock sites. There is a feature that is an adult override which, if a school district chooses, the adults in that district have a user name and password, they can go around the filtering whenever they need to.

It is notable that a number of school districts choose not to use that option. They decide that if adults want to go to the stuff that is blocked, they can do that somewhere else besides the school, so that is not a mandatory piece that is in there.

There are ways to set up filtering schemes within our system so that after certain hours there is a different filtering scheme in place. We update the lists of sites that are blocked daily. It is all automatic. The school does not do anything administratively. We have a system that 24 hours a day is finding sites. Those sites are added to lists and lists are updated and all of the downloads are automatic, and then they have technical support 24 hours a day to go through that system.

Mr. OXLEY. Would you summarize, Mr. Nickerson?

Mr. NICKERSON. I will.

I think there are a few things that are important to note. A lot of the issues dealing with what is going on in this committee are dealing with, A, commercial sites; B, things that are classified as obscene. What we see in schools is a much broader interest in blocking other forms of sites that are objectionable to kids. Graphic violence is an example.

I would estimate that over half of the sites that we block that show graphic sexual acts of one sort or another are not commercially—they are not commercial sites. They may be on some student's Web site at a university. Focusing on commercial sites is not going to take care of this problem. It is a much broader problem than that.

I do want to make one last comment in terms of the XXX zone sort of thing. If you try to zone this, you are going to leave out most of what is out there. Most of the material is legal, and kids put it up themselves, and it exists all over the world. The XXX zone will get a small category of sites only.

Last, in terms of E-rate, I think this has the potential to slow down adoption of the Internet in schools. Internet filtering can be expensive. It is not a cheap process to go through this. A lot of poorer schools don't have the money for very much. I think some of the legislation is redundant to the increase in market demand that has occurred over the last few years for this. Most schools are looking at filtering in a positive way. I think if the committee and the Congress wants to accelerate the adoption of filtering, they may consider putting filtering in one of the categories of the E-rating that schools can purchase. I think that would accelerate it faster than anything else.

[The prepared statement of Peter Nickerson follows:]

PREPARED STATEMENT OF PETER NICKERSON, CEO, N2H2

Introduction

My name is Peter Nickerson. I am CEO and President of N2H2, Inc. in Seattle, Washington. Since 1995 N2H2 has provided server-based (network) Internet filtering services to schools, libraries, businesses and ISPs in the United States, Canada, the UK and Australia. In the U.S. over 8,000 schools use *Bess* SM, its school filtering service, in order to allow students access to the Internet with minimal supervision. By the end of September, as many as 50 percent or more of K-12 students using the Internet in schools in Texas, Ohio, Washington, Maine, Oklahoma and Tennessee will be going through N2H2's filters. Within a month, 50 schools in the Department of Defense's European school system will also being using N2H2's *Bess* filtering. In addition to these school services, N2H2 provides filtering to dozens of public libraries, businesses and almost 200 Internet Service Providers who provide the service to their dial-up customers. While N2H2 services have historically been provided on a network-wide basis, these relationships with ISPs and recent partnerships with companies like Netwave, Fortress, and Winstar now allow individual computer users to utilize N2H2 services even when they are not connected to a network with an installed N2H2 server.

In addition to filtering services, N2H2, in partnership with Inktomi, will soon be providing the Internet community free access to a search engine designed specifically for schools. It is free of references and links to adult sites yet still provides access to a catalogue of over 100 million web pages. Later this fall, N2H2 will also provide e-mail services to schools which will allow school administrators to control how and with whom students communicate over the Internet using e-mail. N2H2's objective is to provide schools with a suite of Internet services that allow them to fully utilize the educational opportunity of the Internet, without fear of exposing students to inappropriate material.

A general perception exists that Internet filtering is seriously flawed and in many situations unusable. It is also perceived that schools and libraries don't want filtering. These notions are naïve and based largely on problems associated with early versions of client-based software that were admittedly crude and ineffective. Though some poor filtering products now exist, filtering has gone through an extensive evolution and is not only good at protecting children but also well-received and in high demand. This evolution has been caused by normal market forces. Customers have requested and demanded changes to filtering products and asked for new features. Most filtering firms have responded by improving their offerings and adding new products. More firms have entered the industry. As N2H2's record can attest, demand for these newer and improved filtering systems is strong. Customer satisfaction, at least for N2H2's products, is very high with N2H2's school customer attrition at virtually zero.

Though N2H2 provides filtering to businesses, ISPs, and libraries, its principal market focus has been the K-12 school environment. Our experience there provides some unique insights.

Changes in the Demand for Internet Filtering:

When N2H2 started marketing Internet filtering to schools in 1995 it met with, at best, a lukewarm reception. For the most part administrators did not want filtering and did not see the need. Many told us that they thought Acceptable Use Policies (AUP) would suffice. That perception has changed. Schools now, with rare exceptions, understand the need for filtering and actively seek solutions to the problems associated with open Internet access. Exceptions to this are rare. This change

seems due to the publicity about pornography on the Internet, public pressure, and a good understanding of how simple it is for children to be exposed to adult Internet material when filtering is not in place.

It appears that school officials have also found that AUPs, by themselves, do not work. They are long, often written in legalese, not read (nor necessarily understandable) by students, and often too easy to ignore. In reviewing one school district's Internet use, where the district had a well-conceived and well-written AUP, N2H2 found that almost five percent of the Internet requests were for sites that contained adult content, mostly pornography. It would not surprise us to find similar results anywhere you had normal, curious children. (In contrast, we have found that in schools with filtering, students soon stop looking for this material and the number of sites being blocked is approximately one and one-half percent. These include blocks of chat, free-email, sites that request personal information, and sites that contain adult-oriented advertising.)

While the K-12 environment is readily adopting Internet filtering without the added pressure of a legislative mandate, the same is not true of libraries. Some libraries do have various forms of Internet filtering on their computers. Our observation is that most do not. Filtering in the library environment is more complicated and much more tied to legitimate free-speech issues than in schools. Some librarians are adamantly opposed to filtering on First Amendment grounds. Those who are not are worried about litigation or the threat of litigation and have resisted the urge to filter. The demand for filtering in libraries is relatively low and will probably remain so until the courts resolve the extent to which librarians can filter.

Filtering Attributes, Characteristics and Flexibility:

The demand for N2H2's filtering in the schools has been stimulated by an array of features that are part of the service. N2H2 sells Internet filtering in the K-12 environment under the trade name of Bess. It is a service rather than a software product. N2H2 provides its schools a filtering and caching server (or for small schools, access to one) and completely maintains and services the filtering functions for the customer. This approach has proved invaluable to many schools who are short-handed in the technical area and may not have the resources to learn and maintain new hardware and software systems.

The services are adaptable to the customer's needs and community standards regarding filtering. The following is a partial list of the features and options that schools receive when they decide to use filtering. It is important to note that this is the array of options that schools have asked to see and which make the filtering service attractive and functional for them.

- The service is turnkey—All hardware, software, maintenance, and updates are included.
- Filtering is fully customizable—Customers choose the categories of sites they want blocked on their system. Choices include pornography, drug use, graphic violence, and bomb-making. (See the attached list for a complete description of the categories). Customers can also invoke exceptions for educational sites and choose whether or not to block free e-mail, chat or simply allow moderated chat.
- Customers can further customize the filters by adding or subtracting sites from the block lists.
- Different filtering schemes can be set up for different times of day.
- Over 4.5 million web pages are contained in the block-site categories.
- All sites that are blocked are reviewed by N2H2 staff before being added to the block lists.
- When users think that a site should not be blocked (or should be blocked), they can easily notify N2H2 staff and a review usually takes place within a day.
- Updates to the block lists occur daily, automatically.
- Technical support and system monitoring is available 24 hours a day.
- Adults can override the filters using passwords.
- Administrators get complete statistics on their network's Internet use on demand.
- Upgrades to the software are automatic.

These features allow communities to customize their filtering to fit their needs. It is probable that none of our customers configure their systems the same. It is notable for the legislation being considered that some schools choose not to install the filter override option. Adults who want to access filtered sites need to do so off of the school's network.

"Obscene" versus "Adult"

The legislation before Congress deals with the filtering of sites that are "obscene". The vast majority of sites that are adult-oriented or may otherwise not be appropriate for children do not fit the legal definition of obscene. They are legal. While laws will not cover the filtering of these sites, most filtering systems will block these

legal, adult sites. While some anti-filtering advocates argue that this is improper, we think it is more appropriate to treat the filtering of these sites the same way as adult entertainment. Communities have long held, and the courts have agreed, that adult entertainment can be "zoned" out of certain parts of the community in order to protect other legitimate (but competing) interests. Internet filtering seems to fit this standard. It essentially sets up Internet zones where adult material is not allowed (schools and public libraries) in the interest of protecting children. Access to adult sites is still allowed on those public and private computers on which the risk to children is negligible, and where the community has no obligation to protect them.

Attached to this written testimony is a copy of the system N2H2 uses to categorize sites. It gives some flavor of the types of perfectly legal sites which might be inappropriate for children.

Legislative Effects

Lastly, Congress needs to be aware that the different forms of legislation appearing before them may not have a significant impact on promoting filtering. Most school and library administrators understand the need for some protection for children and are trying to deal with the problem, even without legislation. Because filtering is not free (list prices can range from $0.50 to $3.00 per workstation per month) this legislation could slowdown the adoption of Internet use in schools. If Congress wants to accelerate adoption of filtering, the e-rate funding program might be changed to include filtering.

Mr. OXLEY. Thank you.

Mr. Kupser.

STATEMENT OF ANDREW L. KUPSER

Mr. KUPSER. I would like to summarize for the committee some of my concerns.

My name is Andrew Kupser. I work as the CEO for one organization, and I manage several other Internet providers.

I have three areas of concerns here today. One of the areas is that we are dealing with a highly charged, emotional issue. Second is, we are lumping some perfectly legal, while you may find them objectionable, business enterprises into a category that is illegal, the distinction between obscene and those that are detrimental to minors. There is absolutely no question that child pornography is illegal, but there are adult entertainment sites that are legal.

As an Internet provider, I operate in four States and two countries. I operate in Washington State two services, Michigan one service, California one service, and Mexico City. I have to deal with across-border issues. If the intention of this committee is to simplify some of those across-border issues and try to legislate some of the common grounds for what is acceptable and not acceptable, I think you are started in the right direction.

One of the things that we need to be aware of and that I am very aware in my corporations is cultural diversity. Actually, 84 percent of my stock is owned by one individual and a first generation American-Chinese woman. So when we talk about legislation, you are going across several different issues, not only cultural but business and emotional issues.

The legislation that is before us is actually very timely. Unfortunately, I think there is a cautionary note that needs to go with this. Several months ago—and I am not nearly as wise as the Federal Reserve Board—but there was a term or a phrase coined, "irrational exuberance." We all agree and we would like to help everybody reach these goals. I don't think that we can do it individually. I think it needs to be a cooperative effort among everybody here.

One of my concerns with filtering is that it is not a complete solution. It is a good solution. I think as you go up the different levels of filtering that are available you can arrive at an optimal solution if you use a combination of hardware vendors who are integrating filtering software into their new product lines, current software providers that are out there, and the cooperation of the ISPs.

One thing I would like to caution this committee against is requiring an ISP to monitor or surveil their subscribers. There are currently laws in place that prohibit me from reading other people's e-mails. That is an illegal activity for me. If it is a criminal investigation, it would be different. So Mr. Hastert, I believe, made the suggestion that maybe we can monitor activities. It is possible, but technologically it is impractical and, legally, it is probably illegal.

One thing that I am concerned about here is we are dealing with two media that are very similar. One is the print media, which we have all drawn reference to, and the electronic media. I would not want to see this committee galvanize a cooperative effort between the print media and the electronic media. We would see the same or similar legal issues arise that this country has dealt with in the past.

Mr. OXLEY. Would you summarize?

Mr. KUPSER. I will.

The technology exists and the software exists to help curb some of these issues that we are dealing with. Unfortunately, there are ways to fool or spoof that technology. Filtering software can be circumvented in 3 to 10 days. So a software solution is not going to be the only solution. It is going to take real people real time filtering the sites as they come up, as one of the other witnesses testified to, roughly 200 a day.

[The prepared statement of Andrew L. Kupser follows:]

PREPARED STATEMENT OF ANDREW L. KUPSER, MANAGING MEMBER, KUPSER COMMUNICATIONS

I would like to thank this body for the opportunity and time to express my concerns before you. The time that you have allocated to me is extremely important and valuable.

I operate several Internet access services including two service providers in Seattle Washington, Los Angeles California, Upper Peninsula of Michigan State, and Mexico.

My largest venture currently has over 350,000 subscribers. The smaller ventures are just starting to break even. The companies that I represent include Kupser Communications a Delaware Corporation, Northwest Internet Service, LLC a Washington State Company, and Connection Global a Nevada Corporation.

Eighty four percent of the outstanding stock is owned by a first generation American-Chinese woman.

Several months ago, when this legislation was in its infancy the Federal Reserve chairman coined a phrase that I would like to borrow... Irrational Exuberance. At the time few people heeded the caution.

While the legislation before us is well intended, I ask that the legislative body consider the exuberance in which we are pursuing this important legislation. Are these rational avenues of enforcement and regulation or are there better solutions.

The rates of which technology advances may shortly render these proposed laws obsolete. Today, you have before you representatives from the software industry, the access provider industry and conspicuously missing are the hardware manufacturers. Currently, the more progressive hardware manufacturers are fielding their equipment with filtering abilities built in. This posses a threat to filtering software companies and pornographic purveyors. As technology advances these hardware

manufacturers and software manufacturers will converge on similar solutions to a common problem.

We can all site individual circumstances that could have been prevented had a particular safety net been in place. My concern is this body is contemplating and action that is a benefit for the few at the cost of many.

I will not argue the point of whether protecting our children is impertinent or not. It is obviously very important. How that protection is implemented is of importance.

These issues encompass the defense of transmissions of these materials to minors. It would appear that an access provider is being held to a higher standard than their counter part of the print media—United States Postal Service, Federal Express, United Parcel Service. Would it be reasonable for this body to legislate and propose enforcement of a search of each document that passes through these services? Would it be as reasonable to ask that these similar services be held accountable for the documents that pass these through these services. Is this body unintentionally setting up a discriminatory policy between printed media standards of transmission and electronic media of transmission? Please keep in mind there are current laws in place that actually prohibit this activity. It is my opinion that this legislation as drafted could require access providers conduct such "snooping" or "surveillance".

Can the legislative body reasonable expect the Internet Industry to surveil each piece of mail, transmission or conveyance of material? Prior legislation by this body preclude myself or other businesses from doing exactly this.

This legislation draws a distinct difference between electronic media and print media. In this distinction, the electronic media purveyors will rise through similar legal challenges that the print media has already prevailed.

This proposed bill provided criminal liability relief but not civil relief.

This bill provides for "software" prevention. Should there be a concern for those access providers that attempt hardware solutions.

Global Implications

The legislation that is proposed will have the effect of (attempt of) projecting US Law onto foreign soil. What we find objectionable in the US is an issue that this bill should deal with. I believe that there will be an inability to enforce this in other countries. This un-enforceability may occur for several differences—cultural, religious or traditional values. How does this body plan to enforce these issues to businesses, content providers or organizations outside the recognized boarders of the US?

As a company that provides or is required to provide filtering, even though located on foreign soil has a major impact on my ability to compete internationally. Although I may filter sites that foreign government find objectionable and those the US legislation requires could position my business in a "limited information" provider. I would not be able to provide information objectionable to the foreign government and I cannot provide information that the US legislation prohibits. It may be easier to direct what information I can provide.

Enforceability

Trying to legislate this filtering software appears to be feasible. In reality, unscrupulous content providers can spoof Internet protocol addresses, change I.P. addresses and locate outside legal boundaries of the US Department of Justice. The ability of the filtering or preclusion of gaming sites outside the jurisdiction of the US can dramatize this. Many of these gaming laws would be unenforceable outside the US just as many of these well-intentioned protection laws will be reduced.

American society is very mobile this also includes the society on the Worldwide Web. As legislation may require my business to filter a site. The site owner may choose to relocate or even spoof an Interned address. Within three to seven days many well-intentioned filters become obsolete. Furthermore, as more sights continue to germinate in our society, these sites will need to be added to filtering software.

We are proposing an issue similar to "there is one bad student in the school, so let's close the school". As we start closing schools the well-mannered, well-intended students and teachers are penalized as the few are punished. Are the needs of the few sacrificed for the good of the many?

The burden that this think could place on the access providers will devastate the industry as a whole. I believe we need to look at the demographics of the access providers. The majority of these companies are small entrepreneurial companies who struggle to keep pace with the technology the additional burden of requiring filtering will eventually drive these businesses out of the market.

As a small business, I provide employment for an average of five employees per location. These opportunities are provided to aspiring young technologically capable

individuals. The opportunity for a young man or woman to leave high school with no secondary training and secure a job who's average pay in the Seattle area according to 1996 statistics is over $112,000 per year is unheard of. In my position as a small business, I provide opportunities for our youth to excel. Through formal training with large manufacturers such as Cisco, Lucent and Microsoft courses. Currently, I provide these opportunities at a cost to my business. If this legislation is passed, these opportunities will need to be reconsidered. I will be forced to re-allocate funds from one area—salaries and education to hardware and software filtering, related expenses.

Mr. OXLEY. Thank you.

Mr. Bastian.

STATEMENT OF JOHN C. BASTIAN

Mr. BASTIAN. Thank you, Mr. Chairman and honorable members.

My name is John Bastian. I am from Sugar Grove, Illinois; and I am the Chief Executive Officer of Security Software Systems. Our company provides computer software solutions designed to protect children online and when properly implemented are effective yet not restrictive. The real goal in our industry is providing a safe online environment for children.

Congress now has a responsibility to draft new legislation that will not restrict online free speech principles yet prevent minors from accessing web-based material intended for an adult audience.

The Internet has experienced an incredible growth rate of almost 100 percent per year since 1988. It is estimated that as of January, 1998, 102 million people use the Internet worldwide. Projecting this rapid growth out to the year 2001, over 700 million people will be online. This explosive growth in popularity has made the Internet an indispensable vehicle for information, communication and commerce. With such a vast interactive audience, a wide diversity of content is available to the average Internet user. Unrestricted access provides the ultimate diversity in information, culture, art, music and sex.

Sexually explicit material is also a large, diverse part of the Internet. Thousands of explicit web sites exist with millions of pages of pornographic material. Most are easily accessed by a few clicks of a mouse. But sites are only a portion of the sexually explicit areas. E-mail, chat rooms, news groups and Instant messaging can be a virtual playground for sexual predators and pedophiles and also contain pornographic materials.

When I was growing up, mom always told me, don't talk to strangers; and when a child is in a chat room the room is full of strangers. The Internet provides a form of anonymity that allows opportunity for people to say and do things they probably would not face to face. It also provides an almost endless supply of those types of opportunities. For adults, these high-risk areas are more a matter of personal choice, but for children the danger is real.

Technology is available to satisfy a wide array of the requirements schools, libraries, business, government and parents will demand for their specific needs. Whether it is simply reminding users of an acceptable use policy or expressly denying access to sexually explicit or highly vulgar material, solutions exist which are inexpensive, effective and versatile. Care must be taken not to restrict the vast amount of information available online, and we are all re-

sponsible as legislators, educators and parents to protect our children.

Thank you very much for the opportunity to testify.

[The prepared statement of John C. Bastian follows:]

PREPARED STATEMENT OF JOHN C. BASTIAN, CHIEF EXECUTIVE OFFICER, SECURITY SOFTWARE SYSTEMS INC.

Mr. Chairman, Honorable Members of the House Committee on Commerce. Thank you for this opportunity to testify before your Committee. My name is John Bastian. I am from Sugar Grove, Illinois, and am the Chief Executive Officer of Security Software Systems, Incorporated. Our company provides computer software solutions designed to protect children on-line and when properly implemented are effective yet not restrictive. The goal of our industry is to provide a safe on-line environment for children.

Congress now has a responsibility to draft new legislation that will not restrict on-line free speech principles, yet prevent minors from accessing Web based material intended for an adult audience.

The Internet has experienced an incredible growth rate of almost 100% per year since 1988. It is estimated that as of Jan. 1998, 102 million people use the Internet worldwide. Projecting this rapid growth out to the year 2001, over 700 million people will be on-line. This explosive growth and popularity has made the Internet an indispensable vehicle for information, communication and commerce. With such a vast interactive audience, a wide diversity of content is available to the average Internet user. Unrestricted access provides the ultimate diversity in information, culture, art, music and sex.

Sexually explicit material is also a large, diverse part of the Internet. Thousands of explicit web sites exist with millions of pages of pornographic material. Most are easily accessed by a few clicks of a mouse. But sites are only a portion of the sexually explicit areas. E-mail, chat rooms, newsgroups and Instant messaging can be virtual playground for the sexual predators and pedophiles.

When I was growing up, mom always told me "don't talk to strangers". When a child is in a chat room, the room is full of strangers. The Internet provides a form of anonymity that allows opportunity for people to say and do things they probably would not face to face. It also provides an almost endless supply of those types opportunities. For adults, these "high risk" areas are more a matter of personal choice, but for children the danger is real.

Early attempts at protecting children on-line took a rather draconian approach to the problem. Block off huge sections of the Internet, allow only certain search engines to operate, allow only certain sites to be accessed or provide remedial blocking of "unapproved" sites. From an end user standpoint it was difficult, expensive, restrictive and not effective. Site blocking technology has improved greatly with a wide array of excellent solutions.

The real-time nature of the Internet allows site content to be changed at anytime. Our company, Security Software Systems, took a different approach to the problem because we felt a more interactive solution was needed. We first looked at how pornographic sites were prioritized within the search engine hierarchy and found some interesting parallels. To attract visitors, a web site will register certain keywords or phrases associated with their site orientation. The more exact or repetitive match returned will put a site higher in the pecking order. Thus if someone is searching "XXX" the sites having xxx registered with the search engine will appear as a result of the search. The more xxx's they have, the higher they rise in the search result. We applied this logic to our base technology and developed a basic content model that used these words and phrases to identify pornographic sites.

In early 1997, after a year of testing and refining, we developed a new child protection application "Cyber Sentinel". It proved to be exceptional at blocking explicit web based material and was unique because of its total reliance on a content model. Part of the technology developed was the ability of our program to gather all the text being transferred to the computer, including hidden or non-visible text. After a solid content "engine" had been built, we created the functionality. Providing different operating modes, provisions for users to put in personal information and the ability to capture visual records of "violations". We made the product easy to use, versatile and very effective.

Even though we started out to filter web sites, law enforcement found our creation worked especially well in chat rooms and e-mail where conversations can turn sexually explicit or predatory very quickly. Children can fall victim to predators by giving out their phone number, home address or other personal information. Many

Internet related criminal investigations relate directly to predators contacting children in chat rooms or by e-mail. Chat rooms are very popular with children and widely used part of the on-line experience. E-mail is the most widely used feature of the Internet and has become an indispensable communication tool. We turned our development to encompass all facets of on-line communications.

Acceptable Use Policies (AUP) are being implemented in many institutions that have unrestricted on-line access. Products like ours can be used to monitor or help reinforce these policies. On detection of an AUP violation the software can display a warning screen reminding the user of the policy. The software can also record and save these warnings for later review.

Technology is available to satisfy a wide array of the requirements schools, libraries, business Government and parents will demand for their specific needs. Whether it is simply reminding users of an acceptable use policy or expressly denying access to sexually explicit or highly vulgar material, solutions exist that are inexpensive, versatile and effective.

Care has to be taken not to restrict the vast amount of Information available on-line and we are all responsible as legislators, educators and parents to protect our children.

Thank you for the opportunity to testify.

Mr. OXLEY. Thank you.

And our final witness, Ms. Griffen.

STATEMENT OF AGNES M. GRIFFEN

Ms. GRIFFEN. Thank you, Mr. Chairman. I appreciate the opportunity to participate in this hearing today.

My name is Agnes Griffen, and I am the Director of the Tucson-Pima Public Library, which serves a population of more than 800,000 residents in both urban and rural county. I am here today not as a representative of the city of Tucson, since they have not taken an official position on these bills, but representing the American Library Association and speaking as a member of its legislative committee.

I would like to comment briefly on legislation H.R. 3177 and Representative Istook's amendment on H.R. 4274.

As a working librarian in a system that is large and has 19 branches and about 250 folks to help serve the public and about half of the population is registered as library card holders, I want to share with you some of the practical problems related to mandated filtering that would face libraries today as well just briefly our philosophical and policy reservations about these proposals.

I think it is commendable that this committee is taking a broad look at these issues, especially in exercising responsibility to monitor and ensure that child pornography and obscenity is cutoff at the source. Librarians do support approaches that focus on industry, and we do work with local law enforcement agencies when necessary, so I want to acknowledge that these issues are serious. As new technologies proliferate in libraries, it is critical that we balance the extraordinary values of these new communications and learning tools with responsible use and careful guidance.

Librarians around the country are on the front line in providing the training, support and guidance for parents and children and all library users what they need to become responsible Internet users. We are one of the few places in the country that is doing this now for the general public, something that I think is important to remember. How we provide that guidance varies depending on the community that we serve.

Nationally, only 15 percent of public libraries are currently using blocking software. In Arizona, neither Tucson or Phoenix are using filtering, but a number of other smaller public libraries are and a number of school systems.

Seventy-five percent of public libraries in the country have made the decision on how to handle this tough issue locally with guidance from community library boards and often from elected officials, and most have adopted acceptable use policies which do spell out appropriate behavior in the library. This has been an important process for communities that have gone through it because it can help parents to become aware of the issues and of some of the options available to them to help them work with their kids to express the values that those parents are trying to teach them.

We think that local decisionmaking is working, and we are very concerned that a legislative mandate to use blocking and filtering software will intrude unnecessarily into the prerogatives of local community-based institutions as well as into the professional decisionmaking of public and school librarians.

In Arizona, the State legislature considered a bill like this last year, and we all argued that using filters should be a local decision and that we did not think that proposed legislation was one that we could live with because it would bestow on us a local parental role which we are neither staffed for nor prepared to deal with.

Mr. OXLEY. Would you summarize?

Ms. GRIFFEN. Yes. Most public libraries do not use chat rooms and e-mail. We don't have the resources to do that. I am not familiar with any cases where—I understand the FBI man said there was one, where a person lured a person to a library, but I have never heard of any instance of someone reaching out through a terminal to reach a child in a public library at least.

What I want to point out is the actual physical, logistical implementation of these requirements would require us to hire people to card people at the door by age and to, in some cases, perhaps even follow them around to make sure, if there was a filtered terminal and an unfiltered terminal, that the kids who are under 18, and I have a hard time telling the difference between a 15- and 18-year-old, to make sure that they don't access the wrong terminal.

What I want to conclude with, though, is that it doesn't make a lot of sense to me to mandate in order to get Federal funds or discount the telecommunications services to require school and public libraries to spend their already limited resources of mostly local money, or any of their minimal State funds, or any of their even more scarce Federal dollars that trickle-down to us to purchase software that cannot do the job that this bill requires us to do. This is not the time.

Thank you.

[The prepared statement of Agnes M. Griffen follows:]

PREPARED STATEMENT OF AGNES M. GRIFFEN, DIRECTOR, TUCSON-PIMA PUBLIC LIBRARY ON BEHALF OF THE AMERICAN LIBRARY ASSOCIATION

I want to thank you for the opportunity to participate in this hearing today. My name is Agnes Griffen. I am a member of the ALA Committee on Legislation and the Director of the Tucson-Pima Public Library in Tucson, Arizona. I have been a librarian for over 30 years. I have previously served as the Director of the Montgomery County, Maryland, Public Library System for 16 years. In addition, I have

served in numerous positions in the American Library Association, including on the Executive Board, and as a past President of the Public Library Association.

I am here today as a member of the American Library Association's Committee on Legislation to comment on legislation, especially H.R. 3177, the Safe Schools Internet Act of 1998 sponsored by Rep. Rob Franks (R-NJ), and an amendment sponsored by Rep. Ernest Istook, Jr. (R-OK) and included in the Labor, HHS Appropriations bill, H.R. 4274. Each of these measures would create a federal mandate for schools and libraries to install filtering and blocking software on computers with Internet access as a condition of participating in universal service telecommunication discounts (H.R. 3177) or receiving other federal funds ("Istook").

The American Library Association (ALA) is the nation's oldest and largest association of librarians and trustees with approximately 56,000 members, including members of the American Association of School Librarians (AASL), the Association of Library Services to Children (ALSC), the Young Adult Library Services Association (YALSA) and the Public Library Association (PLA).

As a working librarian with over 30 years of experience and presently in a system that serves over 800,000 residents, I want to share with members of the subcommittee some of the practical problems related to mandated filtering facing libraries today as well as some of our philosophical and policy reservations about these proposals.

It is commendable for this Committee to take a broad look at these issues, especially exercising responsibility to monitor and ensure that child pornography and obscenity is cut off at the source. Librarians support an approach that focuses on the industry itself, rather than placing the burden on libraries and schools at the public access level. As new technologies proliferate, it is critical that we balance the extraordinary value they bring to communications and learning with responsible use and careful guidance.

In my library system and in libraries around the country, librarians are on the front line in providing the training, support, and guidance that children, parents and all library users need to become responsible Internet users. In fact, libraries are one of the few institutions doing this for the general public. How we provide that guidance varies somewhat depending on the community we serve. Nationally, very few, only 15% of public libraries, use blocking and filtering software on some or all of their terminals. In Arizona neither Tucson or Phoenix city libraries employ filtering, but a number of other smaller public libraries in the state do. Most of us (75%) have made the decision on how to handle this tough issue *locally*, with guidance from our community library boards and often elected officials. The process of developing acceptable use policies has been important for communities. It can help parents and other caregivers to become more aware of the issues and the options they have to control or limit their own children's access through home computers.

We think that local decision making is working and are very concerned that a federal blocking and filtering software mandate will intrude unnecessarily into the prerogatives of local community-based institutions as well as into the professional decision making and judgment of public and school librarians. In my own state of Arizona, the state legislature defeated a bill last session that would have imposed similar blocking and filtering requirements on schools and libraries. During consideration of that bill, librarians in Arizona made clear that the decision whether to use filters should be a local decision, made by Library Boards and/or City Councils or County Boards of Supervisors. We argued that the state should not set local policies for local libraries and that their proposed legislation would bestow on public libraries a role that most have neither sought nor accepted, that is, an "In loco parentis" role that would require library staff to take on full responsibility for what minors read, see or hear through their public library (and in the case of the law proposed in Arizona, to face criminal prosecution if they do not do so.) Legislators in Arizona carefully considered our concerns and defeated the bill. It would be unfortunate indeed if Congress were to step in now and override such judgments made at the state level.

It is worth noting here that most public libraries do not have the resources to provide general access for the public to E-mail or chat rooms. The image of the sexual predator stalking children through libraries is largely a myth, as I am not aware of any such incidents in public libraries.

It has been my experience that the use of filtering software is not a particularly effective way to guide children away from "questionable" material on the Internet nor is it a well-suited "solution" for libraries. Libraries serve as a community's principal source of information. For many, the public library provides the only access to the vast resources of the Internet. Many of those libraries (43%), including many in Arizona, have only one terminal with graphical access to the World Wide Web. To mandate that one computer be filtered would block access for library users of

all ages, not just for children and youth. Moreover, blocking software does not just target "Illegal material." It deprives the community of access to many sites that provide valuable as well as constitutionally protected information for both adults and children on subjects ranging from AIDS and breast cancer to religion and politics. At the same time such software also fails to provide "protection" from materials that others may find "objectionable," however defined.

When this issue was considered in Arizona, Betty Marcoux, a local school librarian (speaking as a parent and citizen), told the Arizona Senate Education Committee: "presently I work in a school district that uses a filter on every instructional computer for students and faculty. Not only has it prevented students and teachers from accessing important and valid information, such as the Web sites of the National Rifle Association and the ACLU, but it has allowed students to access clearly pornographic sites that are not blocked by the filter system." Or, as high school student Graham Allen said in testimony before the Committee, "I can disable any filter with five keystrokes." (He also noted that he was already 18 at the beginning of his senior year, a point that should be raised in this debate.)

More recently, Marcoux expressed concern that blocking and filtering in the school setting undermines efforts to educate students to be responsible users of information. The K-12 school setting is the ONLY setting where we may have the opportunity to do this for all kids—our future generations. If we use filters and abdicate our teaching responsibilities to instead teach the kids how to be discerning users, when will this occur?

"My students have been locked out from issues on breast cancer, AIDS, CityNet, the ACLU, the NRA, and presently are finding access hard to obtain through our filtered computers for the Democratic and Republican party sites, Rollcall.com, and other political websites. All of these searches stem from curricular lessons and issues." Another point made by both Marcoux and Allen is that IF they do gain access, the filtering system slows the entire process down and may actually time them out. Many students become discouraged and will no longer use the school library.

Furthermore, a blocking and filtering mandate brings with it substantial administrative and staff costs. The Istook amendment, for example, would require that filters be operational whenever a minor accesses the Internet. To obtain access to constitutionally protected information, the theory is that filters may be turned off for a minor under the direct supervision of an adult designated by the library or school. Filters may also be turned off by adults for their use under the Istook proposal.

But, many filters cannot be easily turned off and on for each individual user or computer. Even where this is possible, library staff would have to be responsible for that task in order to assure compliance with the law and to limit inadvertent damage or purposeful vandalism of both hardware and software. This would require constant monitoring and intervention by staff already often fully occupied with helping users find good sites as well as with other public services at the circulation or information desks.

Further, to comply with these proposals library personnel would have to check the age of library patrons before Internet access would be permitted. In a public library setting, it is almost impossible to distinguish between a 17 and an 18 year old. How many of you can tell the difference between a 15 year old and a 20 year old? At least at the busiest libraries, libraries would require additional staff, and perhaps security guards to check ID at the point of entry to the public access computers for those patrons who look as though they may be under 18. Staff or guards would also have to monitor Internet use in order to make sure that computer savvy minors did not manage to get around the filters. For some similar requirements in the Arizona legislative proposal, we estimated a cost for our library system of about $500,000 per year to hire such security guards and additional costs just at the larger branches.

While blocking and filtering products can be useful tools for parents to use at home, as public institutions supported primarily by local public tax monies, libraries are obligated to meet the information needs of the entire community or school population, while upholding the basic principles of the First Amendment as well as maintaining privacy and confidentiality of users. Within the same community, within the same school district or library system, indeed, even within the same library or school building, users have vastly different needs. Federally mandated blocking software cannot responsibly anticipate the information and curricular needs of a diverse community or determine the best sources of information for any particular public or school library user. This is the responsibility of library and school boards who reflect the values and standards of their constituencies and who are in the best position to know how to responsibly guide childrens' Internet access within these institutions.

When a library installs commercial filters or blocking software, it transfers the professional judgment about the information needs of the community from the local governing officials and the community librarians and teachers to anonymous third parties—often part time workers with no credentials and no ties to the community—who evaluate sites for the software filter manufacturer. But it is librarians, not the software manufacturers, who have professional skills to serve the community's information needs, and the responsibility to work with governing boards to help develop policies to assure appropriate Internet use. It is also librarians who must respond to community complaints and potential legal action over improper or inadequate blocking.

Librarians are also very concerned about "quick fixes" that fall to teach children how to best use the Internet. Our children are growing up in a global information society. They need to learn critical viewing and information skills that will help them make good judgments about the information they encounter. Students of all ages must be able to assess as well as access information—i.e., be able to distinguish between information that is useful and valuable and that which is not, to handle and reject content that may be offensive to their values and to adhere to online safety rules when confronted with uncomfortable situations. Simply blocking offensive and unwanted content will not teach students those critical skills.

Librarians believe that there are many other ways that can be employed to help children make wise and responsible use of the Internet. Librarians provide training for children, parents and teachers on appropriate Internet use. Almost all employ local Internet use policies for children and other library users which establish the rules for appropriate behavior in libraries or schools when using online resources. Librarians provide guidance on how to assess the value and reliability of Internet resources. The American Library Association, for example, has developed Families Connect, which provides on line classes developed by the American Association of School Librarians that teach Internet basics, safety, and other recommendations for making the most of Internet resources. In Tucson, several libraries provide Internet classes for the public on a weekly or monthly basis.

Most important, librarians assure safe and positive online experiences for children through guidance to sites that are educational, entertaining and valuable based upon each child's needs. In addition to providing direct advice and guidance to children seeking to research particular topics or find certain information, many individual libraries as well as the American Library Association have developed children's web sites and home pages that lead children directly to the best the Internet has to offer. Last year, the ALA developed a list of 700 great sites for kids to guide parents and children to sites that are safe, educational and entertaining, www.ala.org/parentspage/greatsites. This year a new site, Teen Hoopla, www.ala.org/teenhoopla/ was added which includes homework sites, chat and opportunities for online publication for teenagers.

Notwithstanding the many concerns about the use of filtering, some communities have made the judgment to install blocking software in libraries. Others have tried blocking and eventually removed the software because it proved to be ineffective, overly broad and difficult to maintain. Still others have carefully studied the costs and benefits of filtering with their library or school boards and decided to use other methods to guide children's Internet use. But all in the library community who have looked at children's Internet access have made their decisions based on local community circumstances and norms and trained professional judgement, not on the basis of federal mandates.

Conclusion

Librarians understand that increased access to the Internet in schools and libraries has heightened concerns about children's access to inappropriate and illegal material. Those concerns are serious, but they are not new. Communities have been developing many different and effective ways to guide children's access that are informed by professional research and judgment and local norms and values. Congress should not Interfere with local control and decision making by mandating a single approach to a multifaceted problem. There is no one right solution; there are many.

Finally, it makes no rational sense that, in order to get federal funds or discounted telecommunications sources, school and public libraries should be required by Congress to spend their already limited resources of mostly local tax dollars, or any of their minimal state funds, or any of their even more scarce federal dollars to purchase software filters that cannot do what these amendments would require they do! Filters will not and cannot solve the problems of obscenity and child pornography on the Internet. That is the purview of the Justice Department and other law enforcement agencies. Libraries cannot and should not be asked to do the impossible.

Mr. OXLEY. Thank you.

We will begin a round of questions.

All of you were here when Senator Coats testified and read a poignant letter from a school in Indiana signed by a number of teachers; and one of the things that we gleaned from that letter was their frustration that, indeed, the screening software was not effective for what they felt was necessary to protect minors against that kind of material.

So I am going to ask each one of you, A, whether you think in your experience whether that software is or can be effective; and, second, whether indeed that kind of software should be mandated in some form for public schools.

Mr. Berman, let us begin with you.

Mr. BERMAN. There is a great diversity of tools on the market, some effective and some ineffective, depending on what you are trying to accomplish and what your own values are. What we don't have, I think, is a resource made available in this country which would bring those different tools together so that consumers, including schools and libraries, would know what their choices are, how many choices they can pick from, and what the filtering criteria of those companies are.

I know that industry spokespeople are talking about creating such a resource that you can access on the Internet from anywhere and so the consumers would know what they are getting, schools would know what works. You could critique them and you could be interactive and it is well within the technology to require a national dialog. It requires work by the industry and prodding by public policy people to get that to happen.

Mr. DOUGLAS. I concur with Mr. Berman's remarks.

Mr. OXLEY. Good.

Mr. ALSARRAF. I would like to say, with filtering software, I am vaguely familiar with it, and in combination with other services it can be very beneficial.

Ms. LAYDEN. I have no comment on the issue.

Mr. LESSIG. I don't think that there is sufficiently settled filtering software there now, and I think it is certainly unconstitutional for you to mandate that it be installed. It is a harder question in the particular bill that we have here, which is a spending clause bill, but to mandate it I don't think——

Mr. OXLEY. Even under the auspices of the E-rate system, where the schools would be taking advantage of the E-rate?

Mr. LESSIG. That is a spending clause. For the court, it is a harder constitutional question. But I think you, as Congresspeople, ought to have a more robust question than the Supreme Court; and I think you ought to consider it for the same reasons, to be constitutionally problematic.

Mr. OXLEY. Thank you.

Mr. Nickerson.

Mr. NICKERSON. I don't want to go on a marketing binge here for filtering companies.

Mr. OXLEY. It is your best shot.

Mr. NICKERSON. I think there are now 43 companies doing filtering in the United States of some sort or another, and the quality of them varies significantly.

I think we have been successful, and I will tell you that the attrition rate of our customers in the school space is zero. Everyone that we have installed, we have re-upped their subscription as time goes on.

Mr. OXLEY. So the Indiana school didn't buy from you?

Mr. NICKERSON. They did not buy from us.

Mr. OXLEY. Okay.

Mr. Kupser.

Mr. KUPSER. I think several of the points have been made before. I think it is a combination of the filtering software, placing the burden squarely on the purveyors of the adult material on the web to verify ages, and part of the responsibility falls to the ISP.

In my case, I offer the parents not only the software but the option to use a proxy server or unfiltered service. I think it is a combination of all of those.

Mr. OXLEY. Mr. Bastian?

Mr. BASTIAN. I believe that there are very effective solutions that are available not only for the home market but also from server or service-based technology for not only site blocking but monitoring chat rooms, e-mail and, really, addressing the real-time nature of the Internet.

The Internet is constantly in motion. It is a hard thing to really get a target on. But our products are content based, a very advanced content model, and we feel that it is a very good product. We are targeted more toward the home market, but we do have libraries in schools that are installing our systems now.

Mr. OXLEY. Ms. Griffen?

Ms. GRIFFEN. Even assuming that Congress could clarify the difference between what is legal and illegal on the Internet, and that is a tough one, as you well know, I question that with 320 million web pages as of last April and exponentially increasing, that any filtering company, no disrespect meant, but that any filtering company will ever be able to accomplish this.

Mr. OXLEY. Thank you.

The Chair's time has expired. The gentleman from Washington, Mr. White.

Mr. WHITE. I would like to welcome Mr. Kupser and Mr. Nickerson. They took the same airplane ride as I frequently take to be here, and I appreciate that very much.

Mr. Nickerson, you came into my office it must have been 6 months ago and made to me a very effective presentation about how your particular software works, and I would like to go through that so everyone on the committee understands that. As I understand it, when you say that you have a server, this is not software on anybody's computer, this is offsite?

Mr. NICKERSON. That is correct.

Mr. WHITE. They cannot even have access to your computer which is on some other site away from the school?

Mr. NICKERSON. It is at their network hub. So there is nothing on the school computers that the children use.

Mr. WHITE. Basically, you provide a service to these people? It is not as though you sell them the software and then disappear. You monitor and update it on a daily basis?

Mr. NICKERSON. We do not sell software. It is a service that we provide.

Mr. WHITE. Can you tell us just how much error rate you have experienced, and please be as candid and explicit as you can be. How many cases are you aware of in your work across the country, how many errors are you aware of where people have gotten stuff that they should not have gotten?

Mr. NICKERSON. We have a system in place that allows all of the users to both inform us if they think that we have missed a site. They click a button, and it sends us that, and we review that right away. Also, if they think that we have blocked something that we should not have blocked, they click on that, and we immediately review it. That is an ongoing process.

The whole idea of being able to do this 100 percent is not rational. This is an ongoing process. We recently went through a test that was done independently by a western State, and they had us at the 99 percent level of what they were looking at.

Again, it is very subjective. We are in a situation where what gets blocked in one community may be perfectly okay in another community, and they are going to make that judgment. It is community based. We have some school districts in one particular university that has a huge list that they have added to. We have other libraries that use only a list that contains commercial graphic pornography.

Mr. WHITE. Under a system like yours which charges a fee and it may not be right for every particular user, wouldn't you have a pretty high degree of confidence that you know what you are going to get under a system that is administered under your schedule, recognizing that nothing is going to be perfect? It is not perfect if you walk into the bookstore and pick up the wrong book in a bookstore, but don't we have at least as much confidence using your sort of software as we would really in that sort of situation, or am I overly optimistic?

Mr. NICKERSON. I think our customers have confidence that they have a safe Internet. We are seeing a hundred million sites a month through our servers, and administrators, once the system is in place, let the kids go places.

In places where we have gone in and tested where they do not have filtering but they have acceptable use policies, in the one instance we went in and did a large-scale check, 4 to 8 percent of those sites would have been blocked. So these administrators are using filtering because acceptable use policies don't give them that confidence level.

Mr. WHITE. Mr. Lessig, you raised the concern that we are going to get off on the wrong track, and it is so easy for us in Congress to recognize a real problem like this one but come up with a solution that is yesterday's technology or yesterday's solution or that locks us into something that doesn't work with something that might be right around the corner.

I would like to ask you to expand on whether that is a real danger or—we are never going to have perfect information. Is now the time to act or are we running the risk of making a mistake by talking about this here today?

Mr. LESSIG. I think you are running the risk of making a mistake if you want a constitutional bill, because I think the court has already identified——

Mr. WHITE. We don't worry about that.

Mr. LESSIG. That is what I was told. If you want a constitutional bill, the court is already worried about the password-type identification, and I think the court will be quite sensitive to identification which forces people to give up their financial information in order to get access to this type of speech.

Now, around the corner I think with—who is to say, but in a couple of years let's say an alternative model develops which does permit a kind of identification that doesn't present either of these two risks and this committee or the Congress can push to get that type of identification as the identification model that is used. But the identification system that exists right now I think risks this statute being unconstitutional and also presents serious issues of privacy that you ought to be concerned about.

Mr. OXLEY. The gentleman's time has expired.

The gentleman from Illinois.

Mr. HASTERT. I thank the chairman. I came in at the end of the testimony. Unfortunately, I was in another meeting.

I thought I heard—Ms. Griffen, I thought you said that you do not know that any youngster has ever gotten illicit material in a public library.

Ms. GRIFFEN. No, I did not say that. What I said was I am not aware of children being solicited by child pornographers through a public library terminal site.

Mr. HASTERT. Thank you. I thought we needed to have a clarification.

Mr. Bastian, I visited your company out in Sugar Grove, Illinois, a couple of months ago because something happened in my district. We had a predator who actually put a child's name and address on the Internet to be solicited. So all of a sudden this family was getting all of these phones calls and people showing up at the person's door, and it happened through the Internet, and it was a dirty trick that happened, and these people had to deal with it.

You have done a lot of work with screening and being able to screen out and give parents control, and some of your materials are used in the public centers as well. Five years ago this was not a problem in the Congress. We never thought about this happening. We do not know what is going to happen 5 years from now. Companies like yours and other people here today have been able to do the technical stuff so that you can start to get a handle on this.

If you looked into the future, for instance, is it applicable, is it feasible to have something that would go into the system and see who is sending that material? How do you see this happening? What is the future?

Mr. BASTIAN. First of all, the basis of our product is a content model. We looked at the problem a little more globally. We looked at it from people that are online are going to get information from many different areas, not just sites. So we looked at how we can take a content model, apply the context rules to it, see how it is applied related to predatory or pornographic information.

Mr. HASTERT. So it works in a chat room as well as on a web site?

Mr. BASTIAN. Right. Our product we found works on—e-mail predators have been attaching word documents to the e-mail so somebody can open it offline where there is no protection whatsoever. So we took a little different approach to how site blocking works. We do not work off of a set of URL addresses, we work off a content model.

We worked with law enforcement for the past couple of years. We developed our child predator library based off of over a hundred ongoing investigations of sexual predators, and they have tasked us to come up with technology that is more advanced of what is called the ping. You can go out and ping and find a server. They want us to integrate trace routing technology that, online in chat rooms with a keyword or phrasing, that matches the model for online predators. We can save that information and conversation, and we can reach out and find out where that particular person in that chat room is actually talking from. So this is future development, but it is in process.

Mr. HASTERT. So, basically, the license for these people to be predators on children is that there is an anonymity there until they make personal contact with the child, and we can actually reach out and start to spot these people. So the anonymity is not there, and that would be a detraction from people doing it, wouldn't it?

Mr. BASTIAN. I would think if law enforcement has the proper tools, it would be easy to enforce. They would be able to get warrants and have accurate information to get warrants on.

Mr. HASTERT. My time has expired. I thank the gentleman.

Mr. OXLEY. Thank you.

The gentleman from Pennsylvania, Mr. Greenwood.

Mr. GREENWOOD. Thank you, Mr. Chairman.

Mr. Lessig, with regard to the adult identification systems and their burdensome nature as observed by the courts in Reno, the comparison that we make frequently with this legislation is that, clearly, the courts hold that you can have triple-X-rated movie theaters, but also the community can say you cannot show clips of those films visible from the sidewalk. So you have to buy a ticket and go to the movie to view that material.

The Internet is, by its nature and structure, significantly different from that. So my question is: How do the courts measure burden or burdensomeness, given these very, very difficult structures? The fact that it is burdensome to prove that you are an adult through the Internet is a function of the Internet. You can't just go in and hand the man a $5 bill and see the show if you are not an adult.

Does the court not recognize at all when you have a medium that by its nature makes it burdensome to prove your adulthood, that a legal structure that we might create in the Congress that is not intended to be burdensome, not intended to make access to free speech more difficult but is just a reflection of the media we are working with, does the court not recognize that?

Mr. LESSIG. I think the court does recognize that quite explicitly. The question that the court asks, though, is: Is there a less restrictive way of achieving the very same end?

Mr. GREENWOOD. On whom does the burden of proof fall?

Mr. LESSIG. To answer the question whether there is——

Mr. GREENWOOD. In other words, if the court is concerned to know whether this is the least restrictive burden we can impose, would it be up to the plaintiff who challenges the law that we might pass to prove that there is, in fact, an equally effective and less burdensome way to achieve adult identification?

Mr. LESSIG. In the Supreme Court case of Reno v. ACLU, the suggestion which was litigated in both that court below and also in a New York court that there were these developing technologies that would be better protective of the very same interests was enough for the court to believe that it should wait before it endorsed a system and for helping to separating out parents from kids, adults from kids.

That is my suggestion of the very same problem that you are going to face here. But in addition to that problem, the problem that somebody else is going to come along and say here is another technology that won't compromise privacy, that will not make people put their financial records out on the system, in addition to that problem, I am saying by endorsing this technology you might be interfering with the development of this other, more effective, more efficient protective technology.

Mr. GREENWOOD. I am not a lawyer, but does sunsetting legislation in the world of rapidly changing technology have any impact on the court's view?

Mr. LESSIG. Well, there is—it is an excellent question. There is a debate about whether once you strike a statute down it can become constitutional later because of changes in technology.

Mr. GREENWOOD. Or does the fact that the law will go out of existence in 3 years and then need to be reconsidered or repassed and considered by the courts in light of the technology that exists then, does that impact the court?

Mr. LESSIG. That is an excellent question. I don't think that we have a clear answer on that. In Reno, the court could see in the horizon better technologies privately implemented, and that is one of its reasons for saying that it should stop.

Mr. GREENWOOD. My time has expired. I will leave it to your discretion whether you would like Mr. Berman to respond.

Mr. OXLEY. Yes, of course.

Mr. BERMAN. My answer is that the burden be on the government to show less restrictive means. That is why I made the request respectfully to the committee and the Congress again that the burden is really on the Congress as representing the government to make the public policy findings about what is the least restrictive means, and that was not done in the Reno case. There was absolutely a zero, zilch record that Congress put together. And I think we are heading into the same thing here again.

Even if the harmful to minors standard or any of these bills are narrower, Congress has not wrestled with the technology, authorized a study, compared apples and oranges and apples and apples to find out and really give the court a best-shot judgment about how this medium is best regulated. And I think the problem with sunsetting is that you put in a technology and it is there and what it does is it freezes or may freeze investment, and companies that

may want to put $100 million into B won't do it because they think that you have bet on A.

So you would have a more fluid study or process, a study which is really spotlighting the technology, spotlighting developments and looking at it from a series of criteria: constitutional effectiveness, protecting the kids on different parts of the Internet, and have that as an ongoing thing so you can be advised. We don't need a regulatory solution. We need some thinking focused on resolving these issues.

Mr. OXLEY. The gentleman's time has expired.

Professor Lessig, in the dial-a-porn case, the key in terms of the customer is that they rely on credit card verification. What is any different in the case of online pornography in terms of, first, identifying whether or not that individual can pay for it, which is important from the purveyors' side, and, second, for determining who is an adult and who is not? What is wrong with that scenario?

Mr. LESSIG. In the Internet context, the credit card creates a greater danger.

Mr. OXLEY. How so?

Mr. LESSIG. The ability to use the credit card in a larger commercial context exists.

Second, and significant constitutionally, there are less restrictive alternatives than the credit cards that can be used here. It is the fact that there is a less restrictive alternative on the horizon in the Internet context that makes credit cards not a solution, whereas they might be a solution in the context of dial-a-porn.

Mr. OXLEY. Well, I would just point out our legislation, if you will look, does not rely on credit card verification exclusively.

Mr. LESSIG. Yes.

Mr. OXLEY. We are sensitive to that issue in terms of trying to be forward looking in terms of allowing the technology in the least invasive area to ultimately prevail.

Mr. LESSIG. If I may, Mr. Chairman, what the legislation doesn't do, however, is guarantee a structure that can preserve some kind of anonymity here. The German government, when they went through the very same legislative process, put an explicit right in that there would be services that would guarantee anonymous access which would answer part of the problem, I think, but this legislation doesn't yet do that, and that is at least one way in which it creates more of a burden than in the context of dial-a-porn.

Mr. OXLEY. Mr. Alsarraf.

Mr. ALSARRAF. When those parts of the CDA were struck down, that was 2 years ago, and if they were expecting technology to come out, nothing has come out beyond filtering and age verification systems, and age verification systems have come a long way in the 2 years, and we continually spend a lot of resources on research and development, improving it. We have great things on our horizon. And if we keep thinking 2 years away there is a better technology, we will always be take chasing technology 2 years in the future and never take care of anything in the present. We are not yesterday's technology because there is nothing here better. We are continually trying to improve our product and putting a lot of money and resources into it.

Mr. OXLEY. Mr. Berman.

Mr. BERMAN. Where is the legislative record that compares these technologies so you can make that finding? It may be true that is the best thing possible, but when the court looks at the statute again, they are going to say, when did Congress wrestle with that issue and establish a factual basis for it?

Mr. OXLEY. You are doing a pretty good tag team right now.

Mr. BERMAN. We are talking about the issue, but we are not talking about the facts.

Mr. OXLEY. I don't know, did anybody not bring us any facts today? We had facts from the FBI and facts from the members and everybody here. That is what this committee deals with. The dial-a-porn issue, if you recall——

Mr. BERMAN. There is opinion whether one technology here might be better than another and whether filtering is effective or not effective, but that is opinion without any empirical study that I know of that might have some credibility with a court or as a matter of making public policy that would help to resolve this issue.

Mr. OXLEY. We do have some background on this. We went through the dial-a-porn issue.

Mr. BERMAN. It took 10 years for the court to sort that out. And if you want to have 10 years of litigation, that is where we are headed.

Mr. OXLEY. I am prepared to say that we will have litigation no matter what we do.

Mr. ALSARRAF. In terms of burdensome, I think credit card verification is, in fact, extremely simple. Once you put your information, and when they gave their information to us we return it and do all of the verification in about 5 to 10 seconds.

Digital certificates, these other future things, those would be much more burdensome. As anyone knows who has dealt with digital certificates on secured servers, that takes weeks, and it is a headache.

But I would like to say we don't disclose our information to any of our web sites. Our customer is given a PIN and that PIN never—that PIN is never given to the web sites. It comes straight to us to verify, and we return them back into the web sites' content area.

Mr. OXLEY. Have you had any complaints from your customers about lack of verification or giving information?

Mr. ALSARRAF. No. Everything we do is encrypted. We keep our information extremely secure. We have a great reputation on the Internet for that, and we have become known to be reliable in that sense.

Mr. OXLEY. Mr. Lessig, there was some talk about the zoning concept, and it has some attractions. Let's say that we went to a zoning concept, that you really have to have effective filtering devices to make that effective at all?

Mr. LESSIG. Again, I think there are two types of zoning being discussed here. When the Supreme Court was talking about zoning, they were talking about the type of zoning that 3783 would enact.

The different type of zoning discussed here is creating another domain like .xxx. I agree that it would require some kind of filtering to make that effective.

Second, it is not clear how you would deal with the full range of cases that you are trying to deal with in a .xxx area, because pure commercial porn sites would have to go to .xxx. Bookstores that had a mix of material, some pornographic, some not, would be opposed to being forced off into a .xxx domain. So I am not sure that is a solution to the problem that you are looking at, but I also don't think that it would be difficult, and the existing domain name situation could handle it quite easily, which is to add another domain which would be .xxx, and people voluntarily could associate themselves with .xxx if they wanted without any legislation requirement from Congress at all.

Mr. OXLEY. We were told that the cost for filtering is excessive. How much are we talking about in terms of—let's go to Mr. Nickerson—in terms of if I wanted to get a filtering device for my home computer or school, how much money are we talking about?

Mr. NICKERSON. Software programs that sell in the marketplace sell for $29 to $50, and then there is a subscription base associated with that.

Our charges to schools are subscription based. The list prices depend on the number of workstations, but they vary between 50 cents to $3 per month per workstation depending on the size and the sort of system and how much service we have to put into them.

Mr. OXLEY. Is it upgraded on a regular basis?

Mr. NICKERSON. The actual system is upgraded every night so that there is a fresh list in it every night. Because we sell services rather than software, we up the filtering system for efficiency reasons about every 2 months. So that is included as part of that.

Mr. OXLEY. Do any other members of the panel wish to question?

Mr. WHITE. I have one question. Thank you very much.

Mr. Lessig, we talked about how long it would take to come up with the next generation software. Two years is too long. That is the message that Senator Lieberman and I were trying to send to the Internet community when we said—we had this wonderful meeting at the White House a year ago, and nothing has happened since except the problem has gotten worse.

I am sympathetic to the idea that we can do a better job working with you, but it has to be something that is going to be developed within the next year. So I would ask you and Mr. Berman, if we are going to have an all-out effort where industry realizes this is their last chance to solve this problem, and recognizing that Congress has limited resources, how long would it really take us to put together a group of people to focus on this problem and come up with a solution that is more effective than what we are thinking about right now?

I ask you and Mr. Berman, and if anybody else has a thought, I would be happy to hear it.

Mr. LESSIG. In the last 2 years there has been quite significant development in the type of architectures that I am describing that could make this possible in the future. This is the digital certificate architectures.

There is no clear model yet, and I think it would be a mistake because digital certificate architectures implicate commerce much more broadly than they implicate this particular issue for you to rush that. I mean, 2 years sounds like a long time, but it is an ex-

tremely significant feature of the architecture of Internet commerce. So it has been developing.

Now, again, I believe Mr. Berman is right. What I think this committee can do is to bring this type of architecture, people developing this type of architecture in and push them on the question of how to develop your relatively limited interest in respect to what this architecture generally can do and how quickly can it be done. I am not a software developer, but my sense is that it can be done and done more effectively. And if you push something else, you will interfere with its integration into your objective here of an effective and efficient and privacy protective regime.

Mr. WHITE. Mr. Berman?

Mr. BERMAN. I think the answer is the kind of Internet technology commission that is looking at this. You can't do it on a daily basis, but which has to report back to you. You take some of the proposals and look at them in terms of effectiveness, constitutionality, technology, what is on the horizon. If this is an important issue and I think it is, it may cost a little money, but a credible commission that can come back to you and to the administration with public policy and say here are the options that are out there and this is what can be done by the private sector. This is what zoning will do for you if you create .xxx. This is what will happen under different scenarios. I would think that they would respond to that.

The Internet industry is a growing, amorphous thing. They ought to regulate itself, but no one quite knows who it is. It needs a form and a process.

Mr. WHITE. Thank you, Mr. Chairman. A new Mr. Chairman, not even on this committee.

Mr. GREENWOOD [presiding]. Mr. Hastert has a number of questions. I was just musing to myself about the access to the second amendment under the Brady bill can involve a complete background check, no anonymity, all kinds of burden, but we can't find a way to get any restrictions on our First Amendment rights.

I want to get back to the danger of pornography, and I want to ask a question of Dr. Laden, and there is a case, the famous Reno case or Nevada case I think you mentioned—or someone mentioned anyway. We had a case across the river in New Jersey where a young boy, a very young boy, 7 years of age, was going door to door selling things for his school; and in the house of a door he knocked on was a teenager who had been very involved in child pornography and took that little boy in and sexually molested him and killed him.

Is there something about the Internet that you find—the anonymity that the Internet provides that you find particularly damaging or risky or the impact that it has on the individual compared to other outlets and forms of pornography?

Ms. LAYDEN. Clearly, the pornography itself is damaging, but the Internet gives it a particularly virulent form. And that is, in the past, we have had inhibitions to go into porn shops. People would not go in them. Some men wouldn't go in there because they didn't want their minister or next-door neighbor to see them go in there.

As soon as you have the anonymity of having it piped into your own home, the research on anonymity indicates that psychologically it loosens up the inhibitions to antisocial behavior so that

anonymity produces an increase in antisocial behavior. Children particularly are affected by that. But of course my point of view is that the anonymity mixed with the pornography affects adults tremendously as well.

We are at an inundated level of dealing with Internet addicts at our center. We cannot treat all of the addicts who are coming in, not just sex addicts but Internet addicts who are in there, and the level is epidemic. We are at a tsunami level at sexual violence as well as Internet addiction.

Mr. GREENWOOD. Is it clear that you can make a fixated pedophile not simply through trauma that happens to the individual as a victim of a sex crime but through exposure to material?

Ms. LAYDEN. We know that it is relatively easy to produce certain kinds of sexual fetishes, and the research indicates that it is not particularly hard, partly because of the tremendous impact of pornographic imagery on the mind, on brain chemistry reinforced by orgasms. It is relatively easy to seal in sexual pathology.

One of the difficulties with this addiction, unlike all the other addictions we have had ever to treat, is that when you start treating cocaine addicts, let us say you start with detoxification, you want to remove the addictive substance from the body before you can treat them. With pornography, there is not a hope of detoxification. This material is permanently implanted in the brain, producing permanent brain chemistry and brain anatomy shifts, so that we have a kind of addiction that we have never been asked to treat before.

We are seeing that the imagery in itself is dramatic, but this particular kind of imagery is producing outcomes that we did not expect. It is producing all the same outcomes as well. We are having tolerance. We need more and more of it and harder and harder kinds. You get withdrawal, so that pornography addicts go through withdrawal when you remove it.

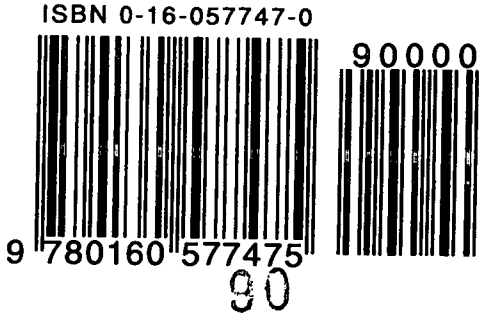
My own clinical experience has been that it is easier to get a cocaine addict into remission than it is to get a pornography addict into remission. The pornography addict is more likely to relapse than the cocaine addict, so that those of us who are treating are having better success with cocaine than we are with pornography. Those of us who are treating the cross-addicted individual are finding that relapse into cocaine is happening through the sex addiction. We will not get the cocaine problem in the country under control until we control sex addiction.

Mr. GREENWOOD. I think it is important to remember the seriousness of the problem as we search for solutions. I want to thank all of the members of the panel for their attendance and their contribution and their patience, and I would ask unanimous consent that the record be kept open for 14 days. Without objection, that shall be the case. Unless there are further questions, this hearing is adjourned.

[Whereupon, at 2:03 p.m., the subcommittee was adjourned.]

[Additional material for the record was submitted by: Enough Is Enough; the National Law Center for Children and Families; BASCOM; and the American Civil Liberties Union, and are retained in subcommittee files.]

ISBN 0-16-057747-0



U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
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").